

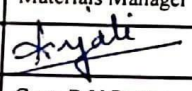
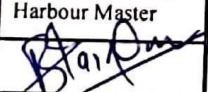
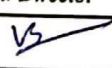
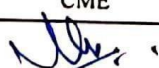
 MUMBAI PORT TRUST	Title	IMS APEX MANUAL	Page No.	1
	Department	MANAGEMENT	Date	03-02-2020
	SECTION 1	GENERAL	Revision	00

MUMBAI PORT TRUST

APEX MANUAL



- 1) ISO 9001: 2015 QUALITY MANAGEMENT SYSTEM (QMS)
- 2) ISO 14001: 2015 ENVIRONMENT MANAGEMENT SYSTEM (EMS)
- 3) ISO 27001:2013 INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

Prepared by		Reviewed by	Approved by
Name	A R Hazarnis, Materials Manager	Manas Mandal, CME	 Chairman
Signature			
Name	Capt. B V Pawar, Harbour Master	Bhabatosh Chand, Dy. Conservator	
Signature			
Name	VBSV Rao, Jt. Director	Manas Mandal, CME	
Signature			

 MUMBAI PORT AUTHORITY	Title	IMS APEX MANUAL	Page No.	2
	Department	MANAGEMENT	Date	03-02-2020
	SECTION 1	GENERAL	Revision	00

Table of Contents

S. No.	Content	Authority		
		Review Control	Approval Control	Issue Control
Section -1 General				
1.	Top Page	CME	Chairman	Pdf copy uploaded on Intranet and KMS of E-Office
2.	Table of Content			
3.	Apex Manual Document Control			
4.	Brief about Mumbai Port			
5.	High Level Organization Chart			
6.	Scope of MbPT			
7.	Processes of Mumbai Port Activities			
Section 2 Common Procedures				
1.	Procedure for identification of internal & external issues	Joint Review by Departmental HODs	Chairman	Pdf copy uploaded on Intranet and KMS of E-Office
2.	Procedure for identification of needs & expectations of stakeholders			
3.	Procedure for risk & opportunity assessment			
4.	Procedure for resource provisions			
5.	Procedure for control of Documented Information			
6.	Procedure for Internal Auditing			
7.	Procedure for Management Review			
8.	Procedure for Non-Conformity investigation and corrective action			
Section - 3 Quality Specific Policies & Procedures				
1.	Definitions	CME	Chairman	Pdf copy uploaded on Intranet and KMS of E-Office
2.	QMS Processes of Mumbai Port Activities			
3.	MbPT Quality Policy			
4.	MbPT Quality Objectives			
Section -4 Environment Specific Policies & Procedures				
1.	Definitions	Harbour Master and Dy. Conservator	Chairman	Pdf copy uploaded on Intranet and KMS of E-Office
2.	EMS Processes of Mumbai Port			
3.	MbPT Environmental Policy			
4.	MbPT Environmental Objectives			
5.	Procedure to determine aspects & impacts			
6.	Procedure to determine compliance obligations			
7.	Communication Policy regarding environment			
8.	Environmental Emergency preparedness & response			
Section -5 Information Security Specific Policies & Procedures				
1.	Definitions	Jt. Director (P&R) and CME	Chairman	Pdf copy uploaded on Intranet
2.	Organization of ISMS Processes			
3.	Information Security Org structure, Roles and responsibilities			
4.	ISMS policies			
5.	MbPT Information Security Policy			
6.	MbPT Information Security Objectives			

 MUMBAI PORT AUTHORITY	Title	IMS APEX MANUAL	Page No.	3
	Department	MANAGEMENT	Date	03-02-2020
	SECTION 1	GENERAL	Revision	00

7.	ISMS scope of application			and KMS of E-Office
8.	Procedure for Information security risk assessment & treatment			
9.	Statement of Applicability (SOA)			
10.	ISMS control procedures Information Security polices Organization of information security Segregation of duties Mobile and teleworking Human resources security Asset management Access control Cryptographic controls Physical and environment controls Ops security Communications Security System acquisitions development and maintenance Supplier relationship Information Security Incident management Information security Aspects of business continuity management Compliance			
11.	User Policies and procedures Acceptable usage policy Reporting Incidents Password policy Virus protection policy Physical security Handling confidential information Use of office equipment Inappropriate Internet use Review by Management Restrictions on posting MbPT information on social media Violations Execution responsibilities			
12.	Social Media Policy			
13.	Policy on Governance of cloud security			
14.	Procedure for Information Security Incident Management			

 MUMBAI PORT AUTHORITY	Title	IMS APEX MANUAL	Page No.	4
	Department	MANAGEMENT	Date	03-02-2020
	SECTION 1	GENERAL	Revision	00

Apex Manual Document Control

The Management Representatives of QMS, EMS and ISMS have collectively prepared this IMS (Integrated Management System) manual which is overall approved by the Chairman. Respective ISO Management Representative will perform the enactment, revision, and abolition of relevant sections assigned for their review after obtaining the approval from the designated authority, as above.

Revision to IMS Manual

The revision to the IMS manual could happen in following situations:

- Revision in the ISO 9001, ISO 14001 & ISO 27001 standard
- Revision in the scope statement of MbPT
- Revision in policy and objectives of QMS, EMS & ISMS
- Revision requested by any user or perceived by respective ISO Management Representative, requiring necessary change in the IMS Manual
- Revision arising out of a closure of a Non Conformity during the audit process.

It shall be the responsibility of the respective ISO Management Representative to review the changes, requested or perceived, and make revision in the current version of IMS manual, making previous version OBSOLETE and the newer version as CURRENT. All the changes in the IMS Manual shall be re-approved by authorised person, prior to issue. The overall issue control of the apex manual shall be controlled by the respective Management Representatives.

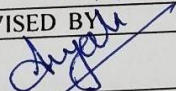
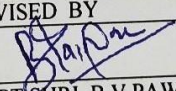
Distribution of IMS Manual

Respective ISO Management Representative shall ensure that the current pdf version of the IMS manual is uploaded on the MbPT Intranet and KMS of E-office

MUMBAI PORT TRUST	Title	IMS APEX MANUAL	Page No.	6
	Department	MANAGEMENT	Date	03-02-2020
	SECTION 1	GENERAL	Revision	00

Details of Revision carried out in the Apex Manual

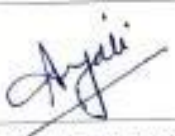
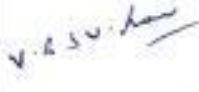
Sr. No.	Date of Revision	Details of revision	Rev. No.	Approved By & Date/ Reference
01	09.8.2021	The MBPT Corporate Quality Objectives for 2021-21 revised.	01	25.7.2021 by Chairman.

	REVISED BY	REVISED BY	REVISED BY
SIGNATURE			
NAME	SMT. A.R. HAZARNIS	CAPT. SHRI. B.V. PAWAR	SHRI. V.B.S.V. RAO
DESIGNATION	MATERIALS MANAGER	HARBOUR MASTER	JOINT DIRECTOR

MUMBAI PORT AUTHORITY	Title	IMS APEX MANUAL	Page No.	6
	Department	MANAGEMENT	Date	13.02.2023
	Section 1	GENERAL	Revision	02

Details of Revision carried out in the Apex Manual

Sr. No.	Date of Revision	Details of revision	Rev. No.	Approved By & Date/ Reference
01	09.08.2021	The MBPT Corporate Quality Objectives For 2021-21 revised	01	25.07.2021 by Chairman
02	13.02.2023	The MBPT Corporate Quality Objectives For 2023 revised	02	06.02.2023 by Chairman

	REVISED BY	REVISED BY	REVISED BY
SIGNATURE			
NAME	SMT. A.R. HAZARNIS	CAPT. R. L. SHINDE	SHRI. V.B.S.V. RAO
DESIGNATION	MATERIALS MANAGER	HARBOUR MASTER	JOINT DIRECTOR

	Title	IMS APEX MANUAL	Page No.	5
	Department	MANAGEMENT	Date	03-02-2020
	SECTION 1	GENERAL	Revision	00

About Mumbai Port

Mumbai Port has long been the principal gateway to India and has played a pivotal role in the development of the national economy, trade & commerce and prosperity of Mumbai city in particular. The port has achieved this position through continuous endeavor to serve the changing needs of maritime trade. Though traditionally designed to handle general cargo, over the years, the port has adapted to changing shipping trends and cargo packaging from break bulk to unitization / palletization and containerization. Besides, it has also developed specialized berths for handling POL and chemicals. For decades, Mumbai Port was India's premier port.

Having weathered and survived many a changes in maritime trade in its long history, Mumbai Port is today facing challenges posed by competition from adjoining ports and private ports, changing traffic patterns, inherent physical constraints and continuing labour intensive operations, etc. However, Mumbai Port is taking various measures to render cost effective and quality services to the trade.

MbPT Location and Salient Features:

The Port of Mumbai is situated almost midway on the West coast of India and is gifted with a natural deep water Harbour of about 400 square kilometers protected by the mainland of Konkan on its East and Island of Mumbai on its West. The deep waters in the Harbour provide ample shelter for shipping throughout the year. The approaches to the Harbour are well lighted, with the Prongs Lighthouse to the North, visible 27 kilometers and the Kennery Light House to the south visible 29 kms. The entrance of the Harbour which has approaches from the South-west is between Prongs Reef and the Thull Reef lying off the mainland to the South-east, a distance of about 9 kilometers.

The main navigational Harbour Channel is, for the great part, a natural deep-water fairway. The channel has been deepened to 11 meters. With a mean high water neap tide of 3.3 meters, the channel is adequate to meet the requirement of a large number of cargo vessels, passenger ships and deep drafted tankers. With good lighting arrangements navigation is allowed at the port round the clock.

Dry Cargo Handling:

There is an enclosed wet dock namely Indira Dock having a total water area of 24.04 hectares and a quayage of about 4000 meters. The Indira Dock, has an Entrance Lock 228.6 meters long and 30.5 meters wide through which vessels can enter or leave the docks at any state of tide. There are 21 berths inside the basin and 5 berths along the Harbour wall, with a designed depth of 9.14 meters and 7.5 meters respectively. The depth of berths inside the basin can be increased by 1.20 meters by impounding water by electric pumps. There are two berths on the Southward extension of East arm of the Indira Dock, namely Ballard Pier Station and Ballard Pier Extension. The Ballard Pier Extension berth, is 244 meters long and has a modern passenger Terminal Building. It has a designed depth of 9.75 meters CD. The Ballard Pier Station berth caters to container vessels and has a designed depth of 9.1 meters CD.

 MUMBAI PORT AUTHORITY	Title	IMS APEX MANUAL	Page No.	6
	Department	MANAGEMENT	Date	03-02-2020
	SECTION 1	GENERAL	Revision	00

Marine Oil Terminals:

For handling Crude oil and Petroleum products, there are four jetties at Jawahar Dweep. One of the jetties at Jawahar Dweep, which was commissioned in 1984 can handle tankers with the maximum loaded draft of 12.7 meters corresponding to 125,000 Displacement tons. Two of the jetties can accommodate tankers up to 70,000 Displacement Tons and 228.6 m length and the third one can take tankers of 213.4 m length and up to 48,000 Displacement Tons. Chemical and POL products are handled at two jetties at Pir Pau. Old Pir Pau jetty can accommodate tankers of 170.7 m length while the new one commissioned in December 1996 can handle tankers with a length of 197 m and a draft of 10.5 m. All the jetties are connected to Oil Refineries by a network of pipelines.

Bunders:

Besides the wet docks, there are along the Harbour front a number of bunders and open wharves where the traffic carried by barges/sailing vessels are handled.

Dry Dock:

The port has one dry dock, inside the Indira Dock, viz. Hughes Dry Dock which is 304 meters long.

Storage:

There are transit sheds at most of the berths and a number of warehouses in the Port area for storage of un-cleared cargo and pre-shipment storage of export cargo.

 MUMBAI PORT AUTHORITY	Title	IMS APEX MANUAL	Page No.	7
	Department	MANAGEMENT	Date	03-02-2020
	SECTION 1	GENERAL	Revision	00

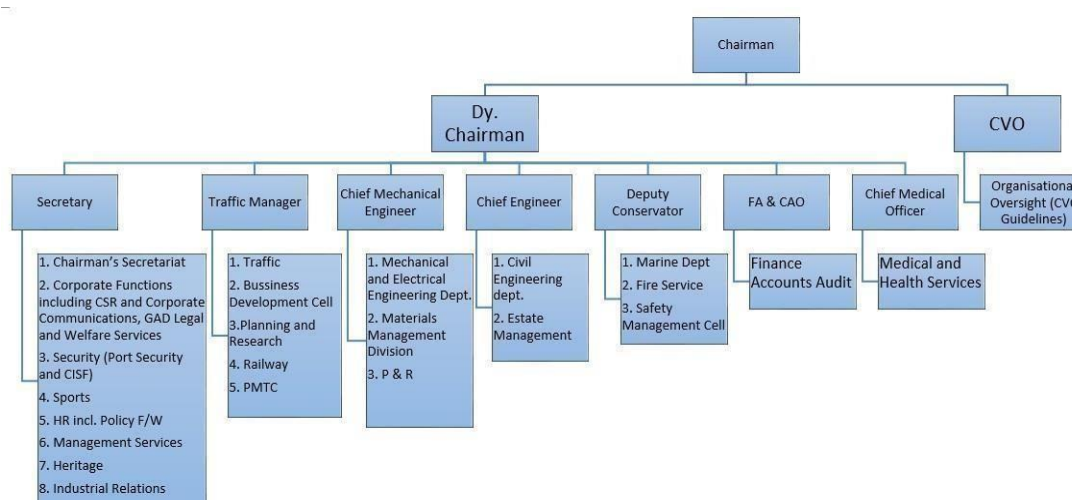
High Level Organization Chart

For each process, MbPT has named a process owner with defined responsibilities and authorities in the departmental (Section wise) manual to establish, maintain, control and improve the process and its interaction with other processes.

Leadership team will ensure that the responsibilities, authorities and roles of process owners are recognized throughout MbPT, and that the people associated with the individual processes have the competences needed for the tasks and activities involved.

For effective planning and implementing the Integrated Management System and taking the corrective and preventive actions, the top management team consisting of Chairman, Dy. Chairman, head of departments, Core group members from each department and Management representative is responsible.

Following is the organization's high level organization chart.



 MUMBAI PORT AUTHORITY	Title	IMS APEX MANUAL	Page No.	8
	Department	MANAGEMENT	Date	03-02-2020
	SECTION 1	GENERAL	Revision	00

Scope of MbPT

The scope of IMS at MbPT is defined as below:

Scope:

“To provide integrated sea-port facilities for safe handling, storage and delivery of cargo / container to the requirements of our customers and promote domestic and international cruise shipping.”

Boundaries:

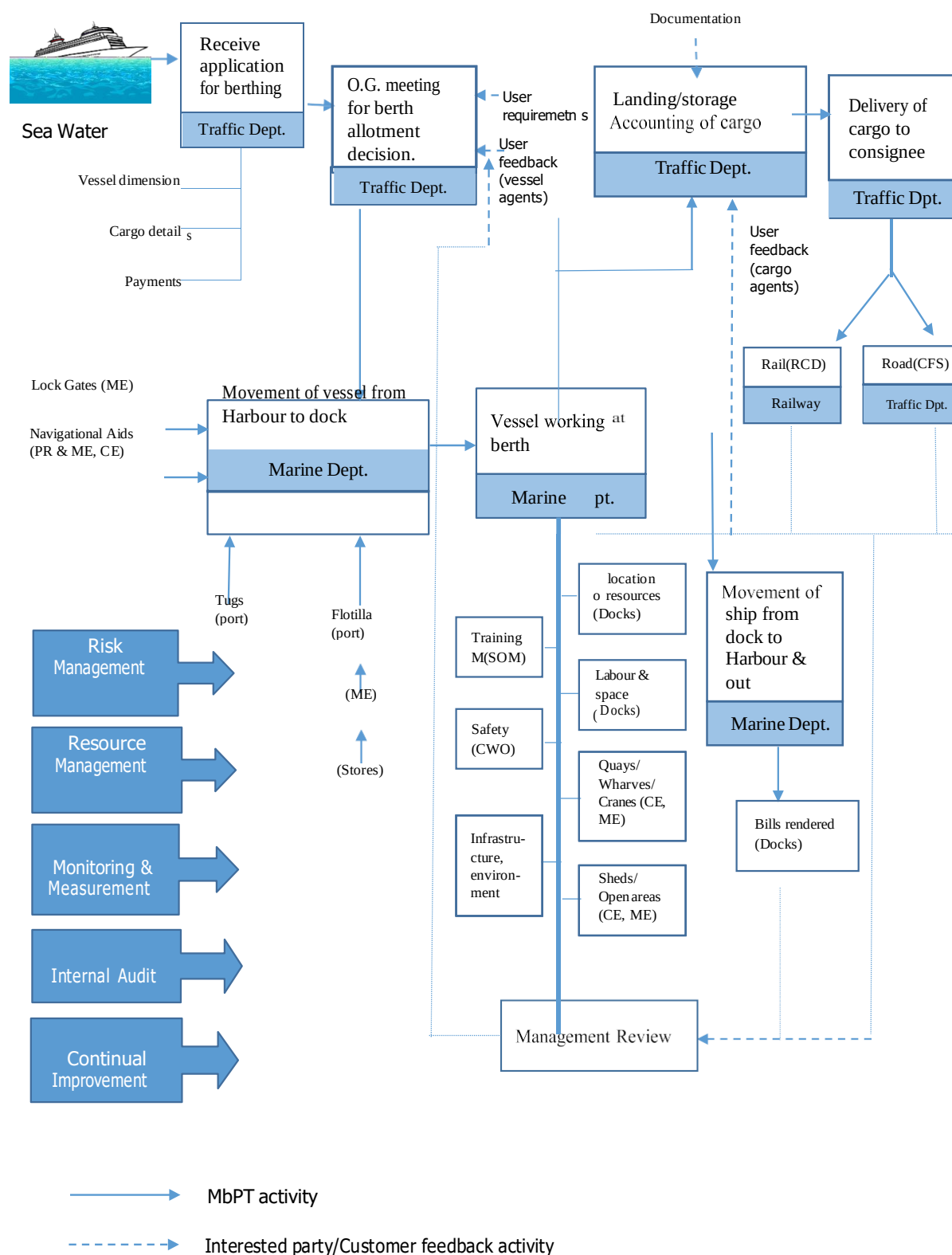
The area covered under IMS is as follow:

- a) MUMBAI PORT AUTHORITY administrative office building including:
 - I. Port House
 - II. Vijay Deep
 - III. Nirman Bhavan
 - IV. Bhandar Bhavan
 - V. Ambedkar Bhavan
 - VI. Hamallage
 - VII. Yantra Bhavan
 - VIII. Seva Bhavan
 - IX. OPL Wadala office
- b) Jawahar Dweep including berths (JD1, JD2, JD3 and fourth oil berth).
- c) Pir Pau including berths (Old Pir Pau, First Chemical Birth and Second Chemical Birth), combined bldg., Wadala.
- d) Indira Dock including Dry Dock, OCT and offices in Indira Dock premises including passenger terminal building at BPX.
- e) Sassoon Dock
- f) Ferry Wharf
- g) Passenger terminal at Ferry Wharf

APPLICABILITY (Exclusion) : Clause nos. 8.3 and 8.5.1 (f) are not applicable for MUMBAI PORT AUTHORITY for the scope of ISO 9001:2015, ISO 14001:2015 and ISO 27001:2013 frameworks.

 MUMBAI PORT AUTHORITY	Title	IMS APEX MANUAL	Page No.	9
	Department	MANAGEMENT	Date	03-02-2020
	SECTION 1	GENERAL	Revision	00

Processes of Mumbai Port Activities



 MUMBAI PORT AUTHORITY	Title	IMS APEX MANUAL	Page No.	10
	Department	MANAGEMENT	Date	03-02-2020
	SECTION 1	GENERAL	Revision	00

Every department has planned and documented the works carried out in their respective department. Following contents and the approach adopted by respective department shall be available with the departments.

- Current context of the department
- Issues & Risks assessed by the way of SWOT analysis
- Stakeholder needs & expectations and risks thereof
- Scope of the work carried out by their respective department
- Departmental organization chart
- Roles & responsibility towards all the 3 ISO frameworks
- Departmental objectives w.r.t. the 3 ISO frameworks
- Action Plans to achieve the departmental objectives
- Standard operating procedures & working instructions to control the department's activities
- Templates & formats that facilitate data collection and evidences in support of the activities that have been carried out

	Department	MANAGEMENT	Page No.	1
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 2	COMMON PROCEDURES	Revision	00

Section 2

Common Procedures

	Department	MANAGEMENT	Page No.	2
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 2	COMMON PROCEDURES	Revision	00

Procedure for identification of internal & external issues

Intent of the requirement:

To determine the issues (internal & external) that are relevant to MbPT's purpose and strategic direction and that affect its ability to achieve the intended result(s) of its integrated management system.

Scope:

Applicable to all processes at MUMBAI PORT AUTHORITY

Responsibilities:

Chairman in consultation with department head(s) shall determine internal and external issues relevant to MbPT's strategy and intended outcome of IMS

All department head(s) along with respective nodal officers of the department shall be responsible for determining internal and external issues relevant to their department.

Definitions:

Internal issues: Issues that are internal to MbPT and impact its approach in achieving its objectives/goals. These are facilitated by considering issues related to values, culture, knowledge and performance of the organization.

External issues: Issues that are external to MbPT and can impact its approach in achieving its objectives/goals. These are facilitated by considering issues arising from legal, technological, competitive, market, cultural, social and economic environments, whether international, national, regional or local.

Procedure:

- Each Department shall identify internal and external issues that can affect quality, environment and information security performance of MbPT.
- The departments may determine issues (Internal & external) using SWOT (Strength, Weakness, Opportunities, Threats) as a tool.
- List down Strength & Weakness as internal issues & Opportunities and Threats as external issues of the MbPT.
- After consolidating Internal & External issues, get them reviewed by the respective Head of Department.
- Respective HOD's shall monitor information related to the issues that are identified for their department. Any change in issues shall be discussed during Management review meeting.

Document: Identified internal & external issues.

	Department	MANAGEMENT	Page No.	3
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 2	COMMON PROCEDURES	Revision	00

Procedure for identification of needs & expectations of stakeholders

Intent of the requirement:

To determine interested parties and their needs & expectations that effect or potential effect on the MbPT's ability to consistently provide products and services that meet customer and applicable statutory and regulatory requirements.

Scope:

Applicable to all processes at MUMBAI PORT AUTHORITY

Responsibilities:

All department head(s) along with respective nodal officers of the department shall be responsible for determining needs and expectations of interested parties relevant to their department & MbPT.

Definitions:

Interested parties (Stakeholders): Person or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity. Interested parties can be both external and internal e.g. Customers, owners, employees, providers, bankers, regulators, unions, partners, society, competitors or opposing pressure groups.

Procedure:

- Each Department shall identify interested parties and their needs & expectations with respect to quality, environment and information security performance of MbPT.
- Define the relevant interested parties and their needs & expectations related to MbPT or its department's in context to QMS, EMS and ISMS.
- List down interested parties and their needs & expectations with respect to QMS, EMS and ISMS as tabulated below.

Sr No	Stake Holders / Interested Parties	Needs & Expectations from Organization

- After consolidating interested parties and their needs & expectations, get them reviewed by department head, as appropriate.
- Respective HOD's shall monitor information related to the interested parties needs & expectations that are identified for their department. Any change in needs & expectations of interested parties shall be discussed during Management review meeting.

Document:

Identified interested parties and their needs & expectations.

	Department	MANAGEMENT	Page No.	4
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 2	COMMON PROCEDURES	Revision	00

Procedure for risk & opportunity assessment

Intent of Requirement:

To identify potential problems before they occur so that risk-handling activities may be planned and invoked as needed across the life of the service/product or project to mitigate adverse impacts on achieving objectives. Also to build and improve capabilities to respond effectively to low probability, critical, catastrophic risks for achieving cost savings through better management of internal resources.

Scope:

Applicable to all operations/processes/activities and products/services at MUMBAI PORT AUTHORITY. It also includes risks applicable to the activities carried out by the suppliers /in house contractors.

Responsibilities:

Department heads along with their nodal officers shall be responsible for identification and management of IMS risks in all the sections under their departmental control. Risk and controls will be reviewed from time to time, at least once in six months.

PROCEDURE:

- Risk factors identification by considering processes, past incidents, work areas, potential emergency situations and compliances with respect to Quality, Environment & Information security to see what happened and whether the same could occur again.
- Assess the process risk and interested party risk by evaluating their needs and expectations as cited in departmental manuals.
- Assess the likelihood and the severity or consequences of each risk and to give it a “risk rating” by preparing risk matrix (Ref. Departmental Manuals, Risk table)

	Department	MANAGEMENT	Page No.	5
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 2	COMMON PROCEDURES	Revision	00

- Categorize the risk by establishing impact criteria and its impact in context to Quality, Environment & Information security
- Make a decision on available risk, whether to avoid, share, transfer, accept or mitigate the risk
- Periodically monitor or change the criteria as required
- Review your risk assessment and update biennially.

Risk Control:

Risk control must address the following questions:

- Is the risk acceptable without further action?
- What can be done to reduce, control or eliminate risks?
- What is the appropriate balance among benefits, risks and resources?
- Are new risks introduced as a result of the identified risks being controlled?

Risk Reduction

Risk Reduction emphasizes on processes for vindication or avoidance of risk when the risk surpasses an acceptable level. Risk reduction includes:

- Actions taken to alleviate the severity and probability of risk; or
- Processes or methods that improve the ability to sense risk Implementation of risk reduction measures may introduce new risks into the system or increase the significance of other existing risks. Therefore, the risk assessment must be repeated to recognize and evaluate any likely change in the risk table.

Risk Acceptance

Risk Acceptance is a decision to accept risk. The risk acceptance decision shall be:

- A decision to accept known, residual risk;
- A decision to accept residual risks, which are partially assessed, based upon limited information;
- or
- An amalgamation of these circumstances

	Department	MANAGEMENT	Page No.	6
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 2	COMMON PROCEDURES	Revision	00

Risk Table – Risk and Impact Analysis (Aspect-Impact Analysis) is included in the Individual departmental Manuals

LIKELIHOOD OF OCCURRENCE	CERTAIN (Constantly in normal conditions)	4	4	8	12	16
	LIKELY (Intermittent in normal conditions, weekly or monthly)	3	3	6	9	12
	OCCASIONAL (Possibly may occur, annually, may be due to staff or equipment failure)	2	2	4	6	8
	UNLIKELY (To occur ,no evidence of occurring, extreme situation only)	1	1	2	3	4
SEVERITY OF CONSEQUENCES			A	B	C	D
			MINIMAL IMPACT (Environmental impact reversible in 1 month)	MINOR IMPACT (short term localized impact reversible in 1 year)	MODERATE IMPACT (Medium term localized impact not reversible in 1 year)	MAJOR IMPACT (Long term impacts irreversible)
		LEGAL/ POLICY/ OTHERS		Effecting policy and procedures	Potential breach of regulations	Actual breach of regulations.
		REPUTATION		Potential for internal complaint	Potential for external complaint	Because of breach actual serious complaint/PR issue
		Carbon Emissions	Reduction in carbon emissions	No increase or decrease in carbon emission	Minor increase in carbon emission.	Major increase in carbon emission

	Department	MANAGEMENT	Page No.	7
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 2	COMMON PROCEDURES	Revision	00

Procedure for resource provisions

Intent of the requirement: To provide resources needed for implementing & maintaining the effectiveness of QMS and enhancement of customer satisfaction level.

Scope: This procedure shall apply to the operations and control of MbPT activities

Responsibility: All HoD(s) under the direction & approval of the Chairman, MUMBAI PORT

AUTHORITY. Interpretations w.r.t. MBPT:

Resources are those minimum fundamental needs which facilitate the process to become effective & efficiency.

Resources could be classified as

- ✓ Human Resources
- ✓ Machines & Equipment
- ✓ Space
- ✓ IT Hardware/ Software
- ✓ Work Environment related equipment
- ✓ Transport
- ✓ Financial Resources
- ✓ Material Resources

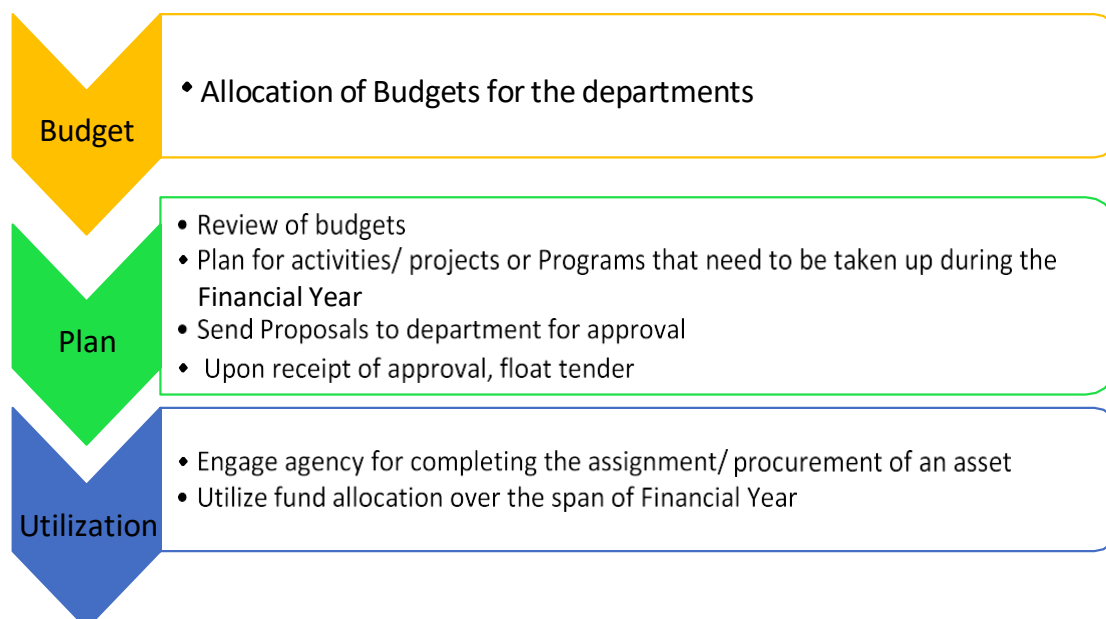
Resources are provided to implement and maintain the IMS and continually improve its effectiveness and to enhance the stakeholder satisfaction by not only meeting stakeholder requirements but also exceeding their expectation.

All the departments have identified the internal and external resources that are needed for the achievement of the MbPT's objectives. MbPT's policies and methods for resource management are consistent with its objectives.

Respective department head at MbPT shall periodically review the availability and suitability of the identified resources, including outsourced resources, and take action as necessary so as to achieve the objectives.

MUMBAI PORT AUTHORITY, through the Chairman, allocates budgets at the start of the financial year, based on past use & utilization of budgets and funds. During periodic review within the department the financial needs are addressed from time to time.

	Department	MANAGEMENT	Page No.	8
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 2	COMMON PROCEDURES	Revision	00



Finance department has already established and maintained processes for monitoring, controlling and reporting the effective allocation and efficient usage of financial resources related to MbPT's objectives.

All HoD(s) will be responsible for the IMS, providing the essential resources including competent Human resource, through GAD, for the implementation, control and improvement. The job responsibilities for all functions to comply with the policies have been defined, communicated and understood by the concerned personnel.

Every department will be responsible for provisioning and providing the resources, including its sourcing through established procurement rules under GFR. Records shall be maintained by respective department and finance department.

	Department	MANAGEMENT	Page No.	9
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 2	COMMON PROCEDURES	Revision	00

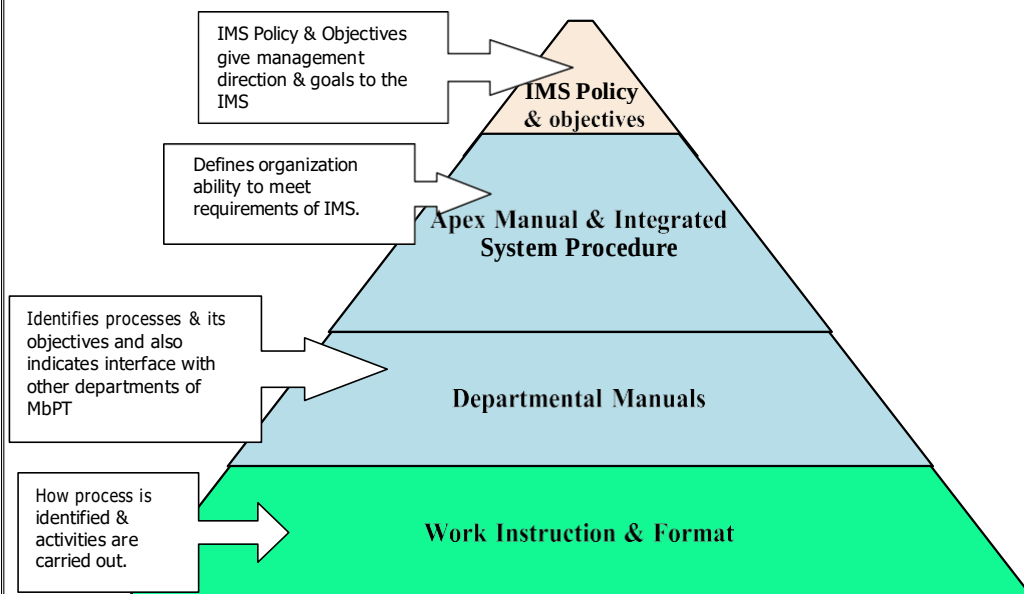
Procedure for control of Documented Information

A document communicates to the officials of MUMBAI PORT AUTHORITY, things such as: what is to be done, how it is to be done, and the required standard that must be met. Documents are the company's plan for how it is going to operate its day to day work. Control of documents is the way company makes sure that the correct information is available to the relevant people.

This means documents must be approved by the appropriate authorities, up to date, and be available to the people who need the necessary information. The information may be continually revised and improved as MbPT makes changes in the way it operates.

Documentation Structure

MUMBAI PORT AUTHORITY has made elaborate documentation to describe its processes, systems. The hierarchy of documentation structure is as depicted in the image, here.



The IMS documentation includes both documents and records. The documentation for MbPT has been done based on the following:

- The functionality of departments of MbPT
- Risks and opportunities
- Roles and Responsibilities of it's people.

	Department	MANAGEMENT	Page No.	10
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 2	COMMON PROCEDURES	Revision	00

Intent of Requirement:

To provide a system for controlling documentation in the form of documents and records, in order to have a better traceability and retrieval.

Scope:

Applicable to all documents and records originated from MUMBAI PORT AUTHORITY. Also all the external origin document in control of various departments.

Document identification:

The documentation numbering nomenclature shall be as follows:

DEPARTMENT/ DOCUMENT TYPE/ SERIAL NO.

Example:

MGT/APX/01 represents; Apex manual number 01, owned by Management function

ME/QSP/01 represents, Quality system procedure for mechanical department with serial no. 01.

Abbreviations:

Following abbreviations that will apply across the organization:

Nomenclature of Organizational Departments / Divisions:

Nomenclature	Department / Division
Traffic	Traffic department
MEED	Mechanical and Electrical Engineering
GAD	General Administration Department
MMD	Materials Management Division
Marine	Marine department
FA	Finance (Accounts Department)
CE	Civil Engineering
PMTTC	Port Management Training Centre
P&R	Planning and Research division
MGT	Management

Nomenclature of Document Types (DOC):

Name	Description
APX	Apex Manual
DM	Departmental Manual
WI	Work Instruction
FO	Format

Issue control

MbPT has ensured that all the documented information related to IMS, regarding the distribution, access, retrieval and use along with the storage preservation, retention control and disposition is taken care with the help issue control matrix given below.

	Department	MANAGEMENT	Page No.	11
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 2	COMMON PROCEDURES	Revision	00

Document Type	Prepared by	Approved by	Issue Control
Apex Manual	As defined in document control of apex manual	Chairman	Respective Management Representative
Departmental/ Sectional Documentation Context/ Risk/ QSP/WI/Guidelines/Aspects-Impacts/ SOA/ CAPA and others	Respective nodal officer	Respective head of the department	Respective nodal officer
Environmental emergency Preparedness Plan	Harbour Master	DC	Harbour Master
External Origin document eg., IS Codes, Acts & rules, etc	-	-	Respective nodal officer

Revision of Documents

The revision to the documents could happen in following situations:

- Revision arising out of change in Policy, Objectives
- Revision arising out of any changed conditions
- Revisions arising out of any change in any process step or procedure
- Revision arising out of a closure of a Non Conformity during the audit process

It is the responsibility of the preparing & approving authority to review the changes, requested or perceived, and make revision in the current version of the document, making previous version OBSOLETE and the newer version as CONTROLLED COPY. All the changes in the document will be re-approved by respective approving authority, prior to issue.

The list of these documents is maintained in Departmental Manual. Also, the storage location and retention period of these documents is provided there for easy traceability of these documents and the outdated records are disposed as per the record retention and disposition. (Refer Departmental Manuals)

Records:

Records are to be maintained by respective departments.

	Department	MANAGEMENT	Page No.	12
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 2	COMMON PROCEDURES	Revision	00

Procedure for Internal Auditing

Internal audit is used as an effective tool for determining the levels of compliance of company's IMS implementation and provide valuable information for understanding, analysing and continually improving the organization's performance. Internal Audits of each department are conducted by trained Auditors of other departments.

MbPT performs internal audits for checking the compliance of the quality objectives and failure (if any) and identifying problems, risks and nonconformities, as well as for monitoring progress in closing previously identified nonconformities. Verification that the actions taken have been effective can be determined through an assessment of the improved ability of company to fulfil its objectives.

Objective

The objective of this procedure is to carry out internal audit in MbPT to ensure to check if it

- ▶ Conforms to the respective requirements of these International Standard(s) (ISO 9001:2015, ISO 14001:2015 & ISO 27001:2013, independently) and relevant legislation or regulations.
- ▶ Is effectively implemented and maintained.

IMS internal audit responsibility

The respective ISO Management Representative have the responsibility to ensure that IMS internal audit programs are planned and executed, and audit report is prepared. It is the responsibility of Nodal Officers along with their Auditees to ensure closure of audit observations identified as an outcome of these audits.

The high level responsibility matrix for IMS Internal Audit activities is as follows:

Sr. No	IMS Internal audit task list	Responsibility
2.1.1	Establish, plan, monitor, review the IMS Audit Program	Respective ISO Management Representative for their respective domain
2.1.2	Responsibility to provide audit support to the QMS, EMS & ISMS function for IMS Internal Audits	Respective Nodal Officers
2.1.3	Approval on IMS Internal Audit Program	Respective ISO Management Representative
2.1.4	To maintain the list of Employees undergone ISO 9001:2015, ISO 14001:2015 and ISO 27001:2013 internal auditor training.	Respective ISO Management Representative
2.1.5	Conducting IMS Internal Audit	Assigned auditor

	Department	MANAGEMENT	Page No.	13
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 2	COMMON PROCEDURES	Revision	00

2.1.6	Release of final IMS internal audit report to auditee.	Internal Audit Team
2.1.7	Accountability to ensure Non-conformities and corrective actions generated out of execution of IMS Internal Audit are monitored and action items are closed	Relevant Departmental HOD's
2.1.8	Compiling and Publishing the IMS Internal Audit report, including major or minor non-conformity, observations to the relevant department heads & chairman.	Respective ISO Management Representative

IMS internal audit program

IMS internal audit program shall be planned and conducted by the Internal Audit Team with support from the top management, considering the IMS policy, clearly highlighting the Scope of Audit which may include achievement of the objectives, risk assessment, control and mitigation measures and the results of previous audits. The Audit program shall consider the determination of audit criteria, scope, frequency of audits and methods.

Audit schedule

- a. The Management Representative of respective ISO shall ensure that internal audits of the IMS are conducted as per defined frequency (every six Month) based on internal audit schedule.
- b. While preparing Internal Audit schedule the following details may be considered:
 - ▶ Sections / locations to be included under the scope of audit
 - ▶ ISO 9001, ISO 14001, ISO 27001 standard(s) clauses to be examined.
 - ▶ Timelines for verifying the effectiveness of controls. (every 6 months).
 - ▶ Results of previous audits; timely closure of action items

Elements of audit schedule

- a. The elements of IMS Internal Audit schedule may include:

- ▶ Location of the audit
- ▶ Purpose and scope
- ▶ Date
- ▶ Time of audit
- ▶ Program of conducting audit
- ▶ Name(s) of Auditor
- ▶ Name(s) of Auditee

	Department	MANAGEMENT	Page No.	14
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 2	COMMON PROCEDURES	Revision	00

Audit team

Auditors

- a. The Internal Audit Team should conduct the audits and shall ensure objectivity and the impartiality of the audited process. It is suggested that the internal auditor has undergone or met any one of the below mentioned trainings:
 - ▶ Lead/ Internal auditor's course in ISO 9001, ISO 14001, ISO 27001.

Selection of auditors

- a. The concerned ISO Management Representative must nominate the team of auditors to conduct the IMS Internal Audits of business functions.
- b. The auditors who would be performing the internal audit for IMS shall be responsible for following:
 - ▶ Conducting the Audit within the scheduled time and as per the scope
 - ▶ Document and supporting objective evidences for all findings
 - ▶ Keep the auditee informed about the audit procedures
 - ▶ Safety and security of all documents
 - ▶ Maintaining independence and the confidentiality irrespective of the nature of their job

Audit methodology

- a. The Internal Audit Team should undertake a review of the processes, assets, facilities and the current practices against ISO 9001, ISO 14001, ISO 27001 standard and MBPT's internal documented system.
- b. The following methodology is recommended:
 - ▶ Interview key personnel
 - ▶ Review records and documentation
 - ▶ Take notes of findings
 - ▶ Submit an audit report
- c. The audit team should perform a systematic, independent audit, check documented process for obtaining evidence and evaluate it objectively to determine the extent to which audit criteria are fulfilled.

Internal audit execution

Audit meeting

- a. The agenda of the audit meeting may consist of:
 - ▶ Scope of the Audit
 - ▶ Audit Schedule
 - ▶ A brief overview of how the audit will be conducted
 - ▶ Corrective/ preventive actions and action plan
 - ▶ Closure of non-conformity from previous audits

	Department	MANAGEMENT	Page No.	15
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 2	COMMON PROCEDURES	Revision	00

- ▶ Any other clarifications from auditors/ auditees are provided and conflicts resolved specifically with respect to schedule.

IMS internal audit for entire IMS arrangements

- a. The Audit Team shall also perform review of IMS for the overall IMS arrangements. A review of IMS documentation:
 - ▶ Should be conducted as per the standard followed for implementation of IMS
 - ▶ Review may include relevant IMS documents and records and previous audit reports
- b. The following points may be considered when performing a review of the IMS arrangement at the function:
 - ▶ Are all the mandatory requirements of ISO 9001, ISO 14001, ISO 27001 standard addressed?
 - ▶ Does documentation match the audit scope?

Audit reporting

- a. The auditor should document the audit findings as per the given scope of audit. Auditors should record non conformity findings / opportunities for improvement along with the supporting evidences. They should conduct meeting with auditee and obtain acknowledgement of non-conformities for accuracy and understanding. Respective internal auditors of the IMS internal audit team shall complete the audit report duly signed and hand over the original report indicating response date to the Auditee within 2 working days from the closure of audit. The following points may be considered in the audit report:
 - ▶ Audit report must be dated, signed and shall be covering the given scope of audit.
 - ▶ Audit report should be distributed only to recipients designated by the respective ISO Management Representative at MbPT. Recipients and audit team must respect the confidentiality of the report.
 - ▶ Nominated IMS internal auditors shall share the duly filled audit report with the respective ISO Management Representatives.
 - ▶ The Auditee shall complete the corrective action / preventive action as per the audit observations within the response time and hand over the original Audit report to the respective ISO Management Representatives, keeping a copy of the report in their record.
 - ▶ Respective ISO Management Representative shall collate the final audit report and shall share it with the following:
 - Nodal Officer
 - Department Heads
 - Top Management/Chairman
- b. IMS Internal Audit Report comprises of the following: -

Audit summary

- ▶ The Audit related details are filled
- ▶ The scope of the audit
- ▶ Observations, root cause and recommendations

	Department	MANAGEMENT	Page No.	16
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 2	COMMON PROCEDURES	Revision	00

Non-Conformances

- ▶ Non-Conformance (NC) is a gap against the IMS requirement or which may have an adverse effect to the interests of MbPT. For a major NC, the adverse effect is immediate and for a minor NC the effect may take place in long run. An observation may arise out of opportunity for improvement.
- ▶ The Non-conformity description is given.
- ▶ The related clause of IMS (ISO 9001, ISO 14001 & ISO 27001) or its related procedures will be specified.
- ▶ Corrective Actions to be taken, responsibility and target closure date will be provided by the auditee.

Previous IMS internal audit review

- ▶ Previous IMS internal audit findings should be reviewed and status should be updated.
- ▶ All observations and NC's which are not closed, should be again documented in report.
- ▶ The IMS Auditor(s) is required to seek concurrence from the auditee on the audit findings. Once the audit findings have been agreed upon, the IMS Internal Audit and Non-conformance reports are finalized.

End of Audit meeting

IMS Audit team should hold an end of audit meeting with the Auditees to present audit findings and conclusion. Auditor shall provide recommendations for improvement where specified by audit objectives. The summarization may be done as follows:

- ▶ General information about audit conducted
- ▶ Function / Process / Facility covered
- ▶ Total NCs / Observations

Retaining audit records

The evidences and facts collected and collated as part of the IMS internal audit are to be shared with Top management. Respective ISO Management Representative should retain the audit records with them in secure manner.

	Department	MANAGEMENT	Page No.	17
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 2	COMMON PROCEDURES	Revision	00

Procedure for Management Review

MbPT uses a systematic approach to review available information and decisions are made based on this gathered information. Data is collected from many sources, such as:

- Monitoring of the MbPT's environment
- Measurements of the MbPT's performance
- Assessments of the integrity and validity of measurement processes
- Results of internal audit
- Risk assessment
- Feedback from customers and other interested parties

At organization, Management review meetings are planned, and conducted periodically. The frequency of the meeting is as follow:

Frequency of MRM	Who will attend MRM
Half yearly (Twice in a year)	Chairman – ISO Management Representative – Heads of the Departments & core group members.
Quarterly (Four Times in a year)	ISO Management Representatives & core group members meeting.
Monthly	Nodal Officers of the respective Departments – Nodal task force members

During MRM the progress of department(s) towards achieving its objectives are evaluated; including opportunities for improvement and learning. Reviews address the assessment and evaluation of improvement activities performed previously, including aspects of adaptability, flexibility and responsiveness in relation to the company's vision and objectives.

The procedure for carrying out the management review is as described below.

Intent of Requirement:

Management review is an imperative requirement to review the organization IMS management system, at scheduled intervals to ensure its continuing suitability, adequacy and effectiveness. Reviews shall include assessing opportunities for improvement and the want for changes to the IMS management system, including the IMS policy and objectives. Records of the management reviews shall be retained.

Scope:

A management review is to focus on the overall performance of the IMS management system. Management review is required to be carried out by top management on a regular basis and required to be carried out by meetings of other communications means also.

	Department	MANAGEMENT	Page No.	18
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 2	COMMON PROCEDURES	Revision	00

Responsibility:

Chairman, respective ISO Management Representatives, Head of departments, Core group members and nodal task force members review the IMS management system at three different levels as per defined planned intervals to ensure continuity suitability, adequacy and effectiveness.

Harmonization of Reviews with functional managers:

In advance, the agenda for the review meeting shall be informed to the managers of the functions that the review is organized on a scheduled date and time. All findings shall be deliberated including the corrective actions taken with the managers responsible for the functions.

PROCEDURE

Management Review:

The Chairman, respective ISO Management Representatives, Head of departments, Core group members and nodal task force members shall conduct Management Reviews as per above defined frequency. All elements of the IMS shall be audited.

The review shall scan the organization's Integrated Management System to ensure its ongoing correctness, adequacy and effectiveness.

Inputs:

The “inputs” into the management review shall comprise information on:

- ✓ The status of actions from previous management reviews.
- ✓ Changes in external and internal issues that are relevant to the integrated management system or respective ISO framework.
- ✓ Customer satisfaction and feedback from relevant interested parties relevant to IMS
- ✓ The extent to which IMS policy & IMS objectives have been met
- ✓ Process performance and conformity in context to quality, environment & information security
- ✓ Information on the IMS performance, including trends in Monitoring and measurement results
- ✓ Information on the IMS performance, including trends in audit results
- ✓ The performance of external providers
- ✓ The adequacy of resources for effective implementation of IMS
- ✓ The effectiveness of actions taken to address risks and opportunities in context to IMS
- ✓ Opportunities for continual improvement of IMS
- ✓ Legal requirements and other requirements in context to IMS
- ✓ Information on the IMS performance, including trends in results of evaluation of compliance with legal requirements and other requirements
- ✓ Relevant communication(s) with interested parties, including complaints
- ✓ The needs and expectations of interested parties, including compliance obligations

	Department	MANAGEMENT	Page No.	19
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 2	COMMON PROCEDURES	Revision	00

- ✓ Fulfilment of its compliance obligations

Output:

The “output” from the management review shall include any decisions and actions related to:

- a. Improvement of the effectiveness of the Integrated Management System and its processes,
 - Record evidence of continuous improvements
- b. Any need for changes to the IMS
 - Record product/service improvements being made and/or implemented
- c. Resource needs

Acceptance:

Closing Reviews

Management Review Meeting Action Items shall be considered closed only after all corrective actions have been accomplished, and follow-up by respective ISO Management Representatives has been done to authenticate the effectiveness of the corrective action.

Rejection:

Corrective Action

Integrated Management System non-conformances as per IMS requirements shall have corrective action initiated in accordance with the corrective action systems.

Reporting of Minutes of Meeting:

All the minutes of the management/functional review meeting shall be maintained by respective levels of ISO Management Representatives

Additional follow up meetings and reviews:

Respective ISO Management Representatives is empowered by Chairman to call for any extraordinary meetings with functional Teams or as and when required.

Records:

Minutes of Meeting Report

	Department	MANAGEMENT	Page No.	20
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 2	COMMON PROCEDURES	Revision	00

Procedure for Non-Conformity investigation and corrective action

If any Non-conformity arises, then it will be updated describing the nonconformity and subsequent action taken.

The procedure for problem solving or carrying out the corrective actions and preventive actions (CAPA) is as described below:

Intent of Requirement

To establish a system that defines the criteria and methodology for taking corrective and preventive action on identified problems or negative trends identified through analysis of records related to IMS.

Scope:

This procedure applies to internal or external concerns relating to quality, environment, information security, reliability, or performance of any service offered by MUMBAI PORT AUTHORITY. Specifically, the procedure encompasses the action taken regarding nonconforming service, customer complaints, audits findings, and negative trends identified from analysis of IMS.

Responsibilities:

Department Heads are responsible for establishing, implementing, and maintaining the ongoing effectiveness of the corrective action/ preventive action .

All employees have the responsibility to initiate corrective/preventive action requests relating to their job function.

Events of Initiating and terminating:

A CAPA shall address the following:

- Non-conformances within process, service or system
- IMS audit Findings
- Subcontractor control
- Management review findings

Terminating of a CAPA:

The CAPA must contain a thorough investigation and documentation for all sections. All data and analysis should be put in measurable terms to support the corrective action and future verifications.

Time Spells for CAPAs:

A proposed due date will be agreed upon between the Management and the assignee charged with collecting the problem analysis data. A single time postponement of the proposed due date can be requested, and must be approved by the Management.

PROCEDURE:

When there is a shortfall in the achievement of objectives or deviation from procedure Corrective Action /Preventive Action (CAPA) analysis is undertaken.

The systematic problem solving methodology contains following steps:

	Department	MANAGEMENT	Page No.	21
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 2	COMMON PROCEDURES	Revision	00

- Deviations / Failure
- Description of Problem
- Root Cause Analysis and Root Cause Identification
- Corrective Action / Preventive Action(s) Closure

Guiding Rules:

The CAPA will be officially closed after review in the Management Review Meeting. The verification will be within the next 90 days after corrective actions had been implemented.

Management will review the status of all CAPAs and the effectiveness of the corrective action program while the management review.

Records:

Corrective Action report

	Department	MANAGEMENT	Page No.	1
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 3	QUALITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Section 3: Quality Specific Policies & Procedures

	Department	MANAGEMENT	Page No.	2
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 3	QUALITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Definitions

Term	Definition
A	
Association	Organization consisting of member Organizations or persons
Audit	Systematic, independent and documented process for obtaining objective evidence and evaluating it objectively to determine the extent to which audit criteria are fulfilled
Audit Client	Organization or Person requesting an audit
Audit Conclusion	Outcome of an audit, after consideration of the audit objectives and all audit findings
Audit Criteria	Set of policies, procedures or requirements used as a reference against which objective evidence is compared
Audit Evidence	Records, statements of fact or other information which are relevant to the audit criteria and verifiable
Audit Findings	Results of the evaluation of the collected audit evidence against audit criteria
Audit Plan	Description of the activities and arrangements for an audit
Audit Program	Set of one or more audits planned for a specific time frame and directed towards a specific purpose
Audit Scope	Extent and boundaries of an audit
Audit Team	One or more auditors conducting an audit, supported if needed by technical experts
Auditee	Organization being audited
Auditor	Person who conducts an audit
Acceptance inspection	Inspection done when accepting the purchase goods.
B	
C	
Capability	Ability of an object to realize an output that will fulfil the requirements for that output
Characteristic	Distinguishing feature
Change Control	Activities for control of the output after formal approval of its product configuration information
Competence	Ability to apply knowledge and skills to achieve intended results
Competence Acquisition	Process of attaining competence
Complainant	person, Organization or its representative, making a complaint

	Department	MANAGEMENT	Page No.	3
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 3	QUALITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Complaint	Expression of dissatisfaction made to an Organization, related to its product or service, or the complaints-handling process itself, where a response or resolution is explicitly or implicitly expected
Compliance Obligations	Legal and other requirements
Concession	Permission to use or release a product/ Service that does not conform to specified requirements
Conformity	Fulfilment of a requirement
Configuration	Interrelated functional and physical characteristics of a product or service defined in product configuration information
Configuration Authority	Configuration control board, dispositioning authority, person or a group of persons with assigned responsibility and authority to make decisions on the configurations
Configuration Baseline	Approved product configuration information that establishes the characteristics of a product or service at a point in time that serves as reference for activities throughout the life cycle of the product or service
Configuration Management	Coordinated activities to direct and control configuration
Continual Improvement	Recurring activity to enhance performance
Context of The Organization	Combination of internal and external issues that can have an effect on an Organization's approach to developing and achieving its objectives
Correction	Action to eliminate a detected nonconformity
Corrective Action	Action to eliminate the cause of a nonconformity and to prevent recurrence
Customer	People or Organization that could or does receive a product or a service that is intended for or required by this person or Organization
Customer Satisfaction	Customer's perception of the degree to which the customer's requirements have been fulfilled
Customer Service	interaction of the Organization with the customer throughout the life cycle of a product or a service
D	
Data	Facts about an object
Defect	Nonconformity related to an intended or specified use
Dependability	Ability to perform as and when required
Dispute	Disagreement, arising from a complaint, submitted to a DRP-provider
Document	Information and the medium on which it is contained
Documented Information	Information required to be controlled and maintained by an Organization and the medium on which it is contained
Distributor	All distributors that trade out our MbPT product.
E	
Effectiveness	Extent to which planned activities are realized and planned results achieved

	Department	MANAGEMENT	Page No.	4
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 3	QUALITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Efficiency	Relationship between the result achieved and the resources used
Engagement	Involvement in, and contribution to, activities to achieve shared objectives
External Provider	Provider that is not part of the Organization
F	
Feedback	Opinions, comments and expressions of interest in a product, a service or a complaints-handling process
G	
Grade	Category or rank given to different requirements for an object having the same functional use
Guide	Person appointed by the auditee to assist the audit team
H	
I	
Improvement	Activity to enhance performance
Information	Meaningful data
Information System	Network of communication channels used within an Organization
Infrastructure	(Organization) system of facilities, equipment and services needed for the operation of an Organization
Innovation	New or changed object realizing or redistributing value
Inspection	Determination of conformity to specified requirements
Involvement	Taking part in an activity, event or situation
Interested Party	Person or Organization that can affect, be affected by, or perceive itself to be affected by a decision or activity
J	
Joint Audit	Audit carried out at a single auditee by two or more auditing Organization
K	
L	
M	
Management	Coordinated activities to direct and control an Organization
Management System	Set of interrelated or interacting elements of an Organization to establish policies and objectives, and processes to achieve those objectives
Measurement	Process to determine a value

	Department	MANAGEMENT	Page No.	5
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 3	QUALITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Measurement Management System	Set of interrelated or interacting elements necessary to achieve metrological confirmation and control of measurement processes
Measurement Process	Set of operations to determine the value of a quantity
Measuring Equipment	Measuring instrument, software, measurement standard, reference material or auxiliary apparatus or combination thereof necessary to realize a measurement process
Metrological Characteristics	Characteristics which can influence the results of measurement
Metrological Function	Function unit with administrative and technical responsibility for defining and implementing the measurement management system
Metrological Confirmation	Set of operations required to ensure that measuring equipment conforms to the requirements for its intended use
Mission	Organization's purpose for existing as expressed by top management
Monitoring	Determining the status of a system, a process, a product, a service, or an activity
Management people	Engineer, Manager, Operations department staffs.
N	
Nonconformity	Non-fulfilment of a requirement
O	
Objective	Result to be achieved
Objective Evidence	Data supporting the existence or verity of something
Observer	Person who accompanies the audit team but does not act as an auditor
Organization	Person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives
Output	Result of a process
Outsource	Make an arrangement where an external Organization performs part of an Organization's function or process
P	
Performance	Measurable result

	Department	MANAGEMENT	Page No.	6
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 3	QUALITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Policy	Intensions and directions of an Organization as formally expressed by its top management
Preventive Action	Action to eliminate the cause of a potential nonconformity or other potential undesirable situation
Procedure	Specified way to carry out an activity or a process
Process	Set of interrelated or interacting activities that use inputs to deliver an intended result
Product	Output of an Organization that can be produced without any transaction taking place between the Organization and the customer
Product Configuration Requirement	Requirement or other information for product design, realization, verification, operation and support
Progress Evaluation	Assessment of progress made on achievement of the project
Provider	Organization that provides a product or a service.
Project	Unique process, consisting of a set of coordinated and controlled activities with start and finish dates, undertaken to achieve an objective conforming to specific requirements, including the constraints of time, cost and resources
Project Management	Planning, organizing, monitoring, controlling and reporting of all aspects of a project
Project Management Plan	Document specifying what is necessary to meet the objectives of the project
Process inspection	Inspection performed during the stage of the process of manufacturing.
Product inspection	The final inspection done before the shipping at the stage where the product was completed.
Process in charge personnel	Person in charge of administration for each process appointed by the responsible section manager of the department who is responsible for the manufacturing of the standard product.
Q	
Quality	Degree to which a set of inherent characteristics of an object fulfills requirements
Quality Assurance	Part of quality management focused on providing confidence that quality requirements will be fulfilled

	Department	MANAGEMENT	Page No.	7
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 3	QUALITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Quality Characteristic	Inherent characteristics of an object related to a requirement
Quality Control	Part of quality management focused on fulfilling quality requirements
Quality Improvement	Part of quality management focused on increasing the ability to fulfill quality requirements
Quality Management	Management with regard to quality
Quality Management System	Part of management system with regard to quality
Quality Manual	specification for the quality management system of an Organization
Quality Objective	Objective related to quality
Quality Plan	Specification of the procedures and associated resources to be applied when and by whom to a specific object
Quality Planning	Part of quality management focused on setting quality objectives and specifying necessary operational processes and related resources to achieve the quality objectives
Quality Policy	Policy related to quality
Quality Requirement	Requirement related to quality
R	
Record	Document stating results achieved or providing evidence of activities performed.
Regulatory Requirement	Obligatory requirement specified by an authority mandated by a legislative body
Release	Permission to proceed to the next stage of a process or the next process
Repair	Action on a nonconforming product or service to make it acceptable for the intended use
Requirement	Need or expectation that is stated, generally implied or obligatory
Review	Determination of the suitability, adequacy or effectiveness of an object to achieve established objectives
Rework	Action on a nonconforming product or service to make it conform to the requirements

	Department	MANAGEMENT	Page No.	8
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 3	QUALITY SPECIFIC POLICIES & PROCEDURES	Revision	00

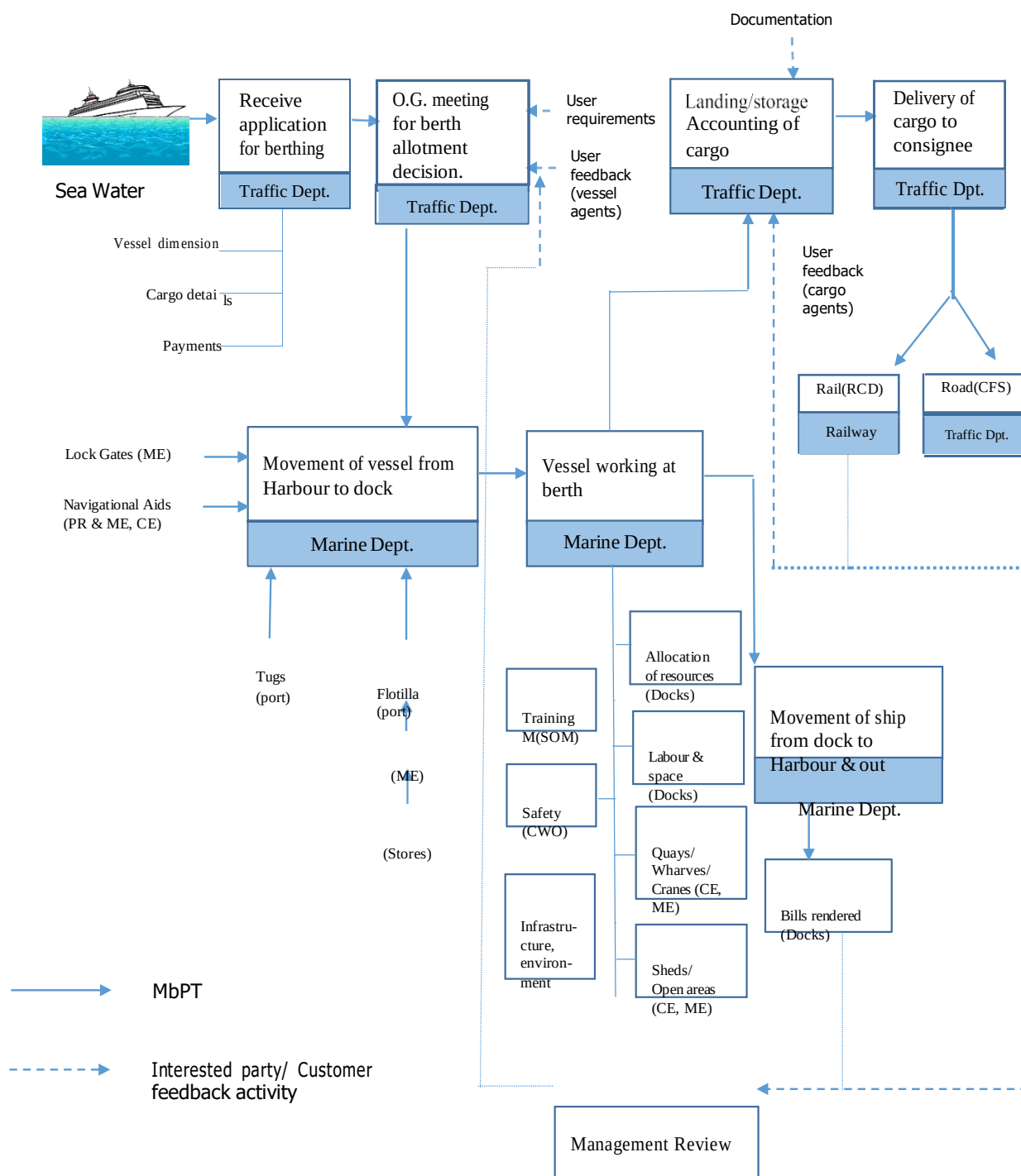
Risk	Effect of uncertainty
S	
Service	Output of an Organization with at least one activity necessarily performed between the Organization and the customer
Specification	Document stating requirements
Strategy	Plan to achieve long-term or overall objective
Supplier	Organization that provides a product or a service
Statutory Requirement	Obligatory requirement specified by a legislative body
System	Set of interrelated or interacting elements
Standard product	Establish the specification as a product, it is called the product that possess the Instrumentation control described clearly in catalogue and explanatory material.
T	
Technical Expert	Person who provides specific knowledge or expertise to the audit team
Test	Determination according to requirements for a specific intended use or application
Top Management	Person or group of people who directs and controls an Organization at the highest level
Traceability	Ability to trace the history, application or location of an object
U	
V	
Validation	Confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled.
Verification	Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled
Vision	Aspiration of what an Organization would like to become as expressed by top management
W	
Work Environment	Set of conditions under which work is performed

	Department	MANAGEMENT	Page No.	9
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 3	QUALITY SPECIFIC POLICIES & PROCEDURES	Revision	00

X	
Y	
Z	

	Department	MANAGEMENT	Page No.	10
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 3	QUALITY SPECIFIC POLICIES & PROCEDURES	Revision	00

QMS Processes of Mumbai Port Activities



Detailed roles & responsibilities, stakeholders needs & expectations, compliance requirements within the activities of respective department, quality performance w.r.t. QMS objectives of the department and their action plans are outlined by respective departments in their departmental documentation.

	Department	MANAGEMENT	Page No.	11
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 3	QUALITY SPECIFIC POLICIES & PROCEDURES	Revision	00

MbPT Quality Policy

MUMBAI PORT AUTHORITY Policy has been formulated to meet the strategic direction. The policy is used as a means of leading the organization towards improvement of its performance and QMS.

The QMS Policy is developed and implemented based on the service quality requirements, customer focused complaint handling priorities, compliance obligations, risks envisaged in the processes, activities and services related to quality provided by MbPT to its interested parties. The following other inputs are considered in framing the QMS policy is as under:

- Regulatory Focus and Commitments by MbPT under various guidelines, directives & notification by customer
- Requirements of QMS
- Commitment to statutory and regulatory requirements
- Customer focused
- QMS focused
- Operational and organizational requirements

QUALITY POLICY

WE, AT THE MUMBAI PORT AUTHORITY, PROVIDE INTEGRATED SEA-PORT FACILITIES FOR SAFE HANDLING, STORAGE AND DELIVERY OF CARGO / CONTAINER TO THE REQUIREMENTS OF OUR CUSTOMERS.

WITH AN AIM OF IMPROVING STAKEHOLDER SATISFACTION, WE ARE COMMITTED TO:

- STRIVE FOR EXCELLENCE IN PORT OPERATIONS
- CONTINUALLY IMPROVE THE SERVICE PROCESSES AND QUALITY SYSTEMS
- THE COMPLIANCE OBLIGATIONS WHILE DELIVERING ITS SERVICES
- ACHIEVE OBJECTIVES FOR PROVIDING EFFICIENT AND TRANSPARENT SERVICES TO THE PORT USERS;

THIS WILL BE ACHIEVED BY IMPROVING INFRASTRUCTURE FACILITES; INTER-DEPARTMENTAL TEAMWORK, TRAINING AND EFFECTIVE DATA BASED REVIEW SYSTEM.

	Department	MANAGEMENT	Page No.	12
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 3	QUALITY SPECIFIC POLICIES & PROCEDURES	Revision	00

MbPA Quality Objectives

MbPT has established objectives at relevant departments, levels and processes as described in the Departmental Manuals. These objectives are consistent with QMS policy, measurable, monitored, communicated, updated, they are relevant to conformity of products and services, enhance customer satisfaction and take into account the applicable requirements (Ref. Departmental Manuals, Objective action plan).

While building these QMS objectives, MbPA also determined

- a) What will be done
- b) What resources will be required
- c) Who will be responsible
- d) When it will be completed

And the results are evaluated by enumerating the current status w.r.t. target status and are reviewed during management reviews. Following are the strategic QMS objectives decided by the organization showing the responsibility who accountable for achieve it.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	13
	Title	IMS APEX MANUAL	Date	13.02.2023
	Section 3	QUALITY SPECIFIC POLICIES & PROCEDURES	Revision	02

MBPA CORPORATE QUALITY OBJECTIVES

ISO 9001:2015 QMS

MBPT CORPORATE QUALITY OBJECTIVES

1. To Improve Turn Around Time for all cargo vessels by 1% year on year basis.
2. To maintain average Ship Berth day Output for General cargo 2650 tonnes (excluding Automobile and Project cargo).
3. Imparting training and arranging skill development programs for 30% of staff below age of 55 yrs. will be imparted training every year at PMTC.
4. To maintain average ship day throughput for Liquid cargo to 17000 tonnes.
5. To render vessel related bills for midstream discharge within 8 working days of sailing of vessels.
6. To ensure 75% of harbour tugs and 66% of dock tugs are available every month at Indira Dock for operations.
7. To maintain 'Incident Rate' of occupational accidents occurred to Dock workers of operational Departments of MbPA and Port Users, below 0.5 in every month.
8. To attend 100% cargo handling related civil maintenance works (minor nature) within 8 working days after receipt of requisition.
9. Preparation of Tender Scrutiny Report for Technical Cover within 30 calendar days from date of opening of technical bids. - Target is 80%
10. Preparation of Tender Scrutiny Report for Financial Cover within 15 calendar days from date of opening of price bids. - Target is 80%
11. Maintain the minimum required illumination level for safe working condition inside the Residential area and Cargo handling Area/ operational dock area by 25 Lux, in the offices 150 Lux and the outside area 10 Lux.
12. Availability of lights in the streets and MbPA owned places: 90% of the street lights and lighting at MbPA owned places will be maintained.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	13
	Title	IMS APEX MANUAL	Date	13.02.2023
	Section 3	QUALITY SPECIFIC POLICIES & PROCEDURES	Revision	02

13. Audit clearance of 100% of ad-hoc/estimated bills within 5 working days, measured bills within 10 working days and final bills within 20 working days from the date of receipt of bills complete in all respect in finance department.
14. Advice to bank for payment of bills through NEFT/RTGS will be issued within two working days from the date of receipt of voucher complete in all respect in Treasury Branch of Finance Department.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	1
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 4	ENVIRONMENT SPECIFIC POLICIES & PROCEDURES	Revision	00

Section -4

Environment Specific Policies & Procedures

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	2
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 4	ENVIRONMENT SPECIFIC POLICIES & PROCEDURES	Revision	00

Definitions

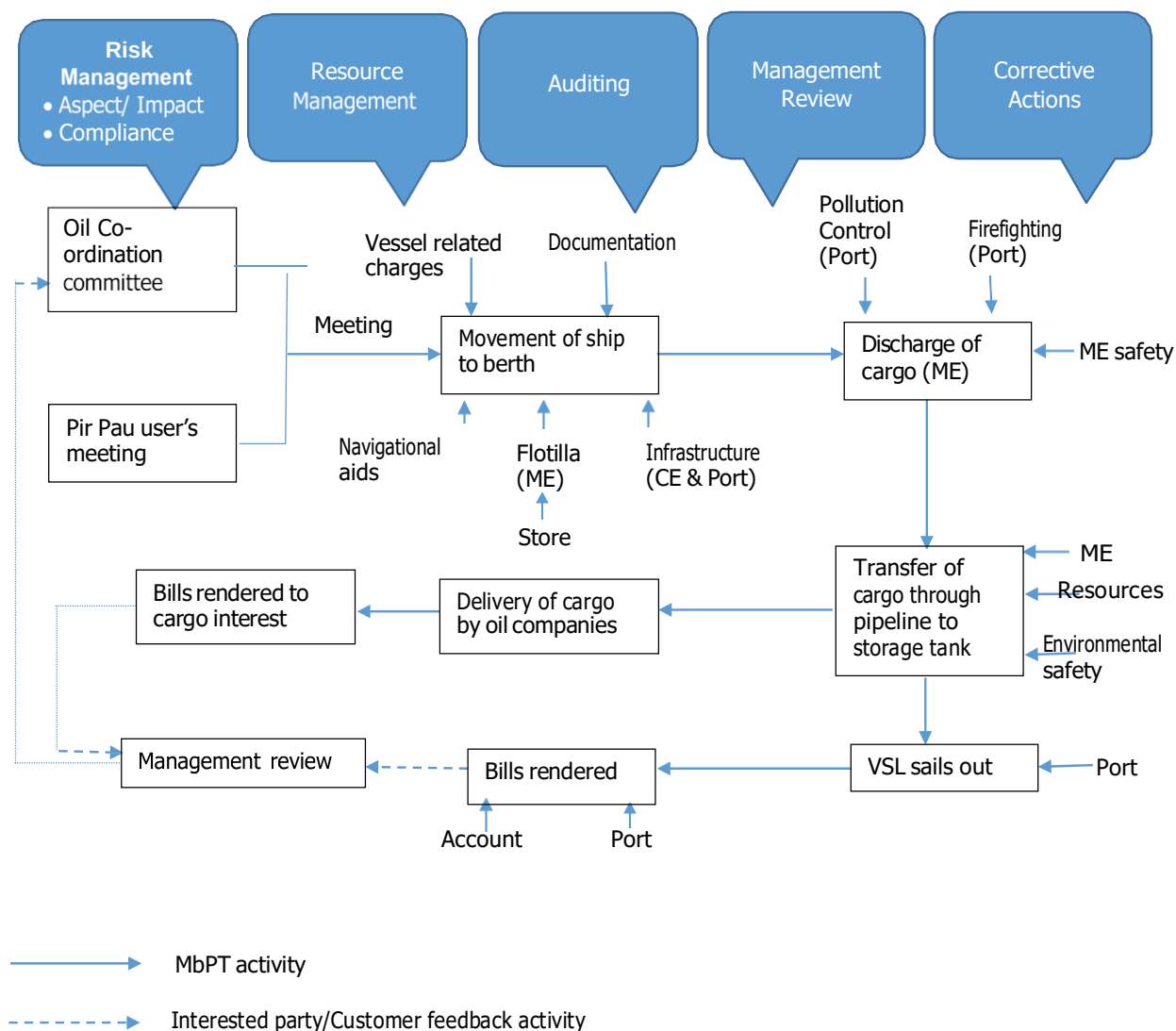
<u>Term</u>	<u>Definition</u>
A	
B	
C	
Compliance obligations	Legal requirements that an organization has to comply with and other requirements that an organization has to or chooses to comply with.
D	
E	
Environmental Management System	Part of the management system used to manage environmental aspects, fulfil compliance obligations, and address risks and opportunities.
Environmental policy	Intentions and direction of an organization related to environmental performance, as formally expressed by its top management.
Environment	Surroundings in which an organization operates, including air, water, land, natural resources, flora, fauna, humans and their interrelationships.
Environmental aspect	Element of an organization's activities or products or services that interacts or can interact with the environment.
Environmental condition	State or characteristic of the environment as determined at a certain point in time.
Environmental impact	Change to the environment, whether adverse or beneficial, wholly or partially resulting from an organization's environmental aspects.
Environmental objective	Objective set by the organization consistent with its environmental policy.
Environmental performance	Performance related to the management of environmental aspects.
F	
G	
H	
I	
Indicator	Measurable representation of the condition or status of operations, management or conditions.
J	
K	
L	

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	3
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 4	ENVIRONMENT SPECIFIC POLICIES & PROCEDURES	Revision	00

Life cycle	Consecutive and interlinked stages of a product (or service) system, from raw material acquisition or generation from natural resources to final disposal.
M	
N	
O	
Outsource	Make an arrangement where an external organization performs part of an organization's function or process.
P	
Prevention of pollution	Use of processes, practices, techniques, materials, products, services or energy to avoid, reduce or control (separately or in combination) the creation, emission or discharge of any type of pollutant or waste, in order to reduce adverse environmental impacts.
Q	
R	
Risks and opportunities	Potential adverse effects (threats) and potential beneficial effects (opportunities).
S	
T	
U	
V	
W	
X	
Y	
Z	

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	4
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 4	ENVIRONMENT SPECIFIC POLICIES & PROCEDURES	Revision	00

EMS Processes of Mumbai Port



Detailed roles & responsibilities, aspects & impacts, controls for significant aspects, compliance requirements within the activities of respective department, environmental performance w.r.t. EMS objectives of the department and their action plans are outlined by respective departments in their departmental documentation.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	5
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 4	ENVIRONMENT SPECIFIC POLICIES & PROCEDURES	Revision	00

MbPT Environmental Policy

MUMBAI PORT AUTHORITY Policy has been formulated to meet the strategic direction. The policy is used as a means of leading the organization towards improvement of its performance.

The EMS Policy is developed and implemented based on the EMS requirements, compliance obligations, environmental risks envisaged in the processes, activities and services provided by MbPT to its interested parties. The following other inputs are considered in framing the IMS Policy is as under:

- Regulatory Focus and Commitments by MbPT under various guidelines, directives & notification by customer
- Requirements of EMS
- Commitment to statutory and regulatory requirements
- EMS focused
- Operational and organizational requirements

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	6
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 4	ENVIRONMENT SPECIFIC POLICIES & PROCEDURES	Revision	00

ENVIRONMENTAL POLICY OF THE MUMBAI PORT

WE, AT THE MUMBAI PORT AUTHORITY, WILL STRIVE TO PROVIDE INTEGRATED SEA-PORT FACILITIES FOR SAFE & ENVIRONMENT FRIENDLY HANDLING, STORAGE AND DELIVERY OF CARGO / CONTAINER TO THE REQUIREMENTS OF OUR CUSTOMERS AND PROMOTE DOMESTIC AND INTERNATIONAL CRUISE SHIPPING.

WITH AN AIM OF IMPROVING ENVIRONMENTAL PERFORMANCE, WE ARE COMMITTED TO:

- STRIVE FOR PROTECTION OF ENVIRONMENT, PREVENTION OF POLLUTION CONSIDERERERING LIFE CYCLE PERSPECTIVE.
- DISPOSE, SOLID WASTE IN AN ENVIRONMENT FRIENDLY MANNER COMPLY WITH ALL STATUTORY AND REGULATORY AND OTHER COMPLIANCE OBLIGATIONS.
- CONTINUALLY IMPROVE THE ENVIRONMENTAL MANAGEMENT SYSTEMS.

THIS SHALL BE ACHIEVED BY CONSIDERING ENVIRONMENTAL OBLIGATIONS AND ENVIRONMENTAL PERFORMANCE IN EVERY PROCESS BY THE WAY OF INVOLVEMENT OF EMPLOYEES AND INTERESTED PARTIES, TRAINING AND DATA BASED REVIEW SYSTEM.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	7
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 4	ENVIRONMENT SPECIFIC POLICIES & PROCEDURES	Revision	00

MbPT Environmental Objectives

MbPT has established objectives at relevant functions, levels and processes as described in the Departmental Manuals. These objectives are consistent with EMS policy, measurable, monitored, communicated, updated, they are relevant to MbPT's significant environmental aspects and associated compliance obligations, and considering its risks and opportunities. (Ref. Respective Departmental Manuals, Objective action plan).

While building these EMS objectives, MbPT also determined

- a) What will be done
- b) What resources will be required
- c) Who will be responsible
- d) When it will be completed

And the results are evaluated by enumerating the current status w.r.t. target status and are reviewed during management reviews. Following are the strategic EMS objectives decided by the organization showing the responsibility who accountable for achieve it.

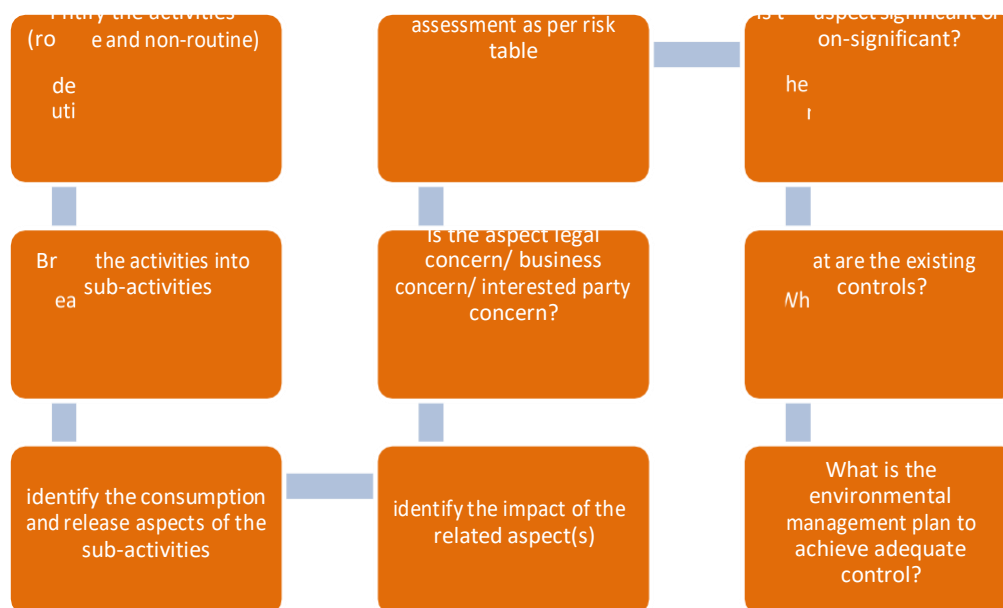
 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	8
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 4	ENVIRONMENT SPECIFIC POLICIES & PROCEDURES	Revision	00

MBPT CORPORATE ENVIRONMENTAL OBJECTIVES
(for the year 2021-2022)

Sr.No.	Objective	Responsibility
1	Optimization in Energy Consumption.	CME
2	Increased Use of renewable energy sources.	CME
3	Provide unhindered Garbage Collection Facility to the ships calling Mumbai Port.	Chief Engineer (As Garbage Collection is under C.E. Dept)
4	Provide Unhindered Reception Facility in accordance with MARPOL Convention.	Deputy Conservator/ Harbour Master/ P.C.C.
5	Maintain Oil Spill Response Facility to Combat Oil Spill at Mumbai Port.	Deputy Conservator/ Harbour Master/ P.C.C.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	9
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 4	ENVIRONMENT SPECIFIC POLICIES & PROCEDURES	Revision	00

Procedure to determine aspects & impacts



Risk Table used for environmental aspect-impact:

1-2 (TRIVIAL)	NO ACTION IS REQUIRED
3-5 (TOLERABLE)	NO ADDITIONAL CONTROLS ARE REQUIRED. MONITORING IS REQUIRED TO ENSURE CONTROL IS MAINTAINED.
6-8 (MODERATE)	EFFORTS ARE REQUIRED TO REDUCE RISK. CONTROLS ARE TO BE IMPLEMENTED WITHIN A SPECIFIED TIME.
9-12(SUBSTANTIAL)	NEW WORK NOT TO START UNTILL RISK REDUCED. IF WORK IS IN PROGRESS, URGENT ACTION TO BE TAKEN. CONSIDERABLE RESOURCES MAY BE REQUIRED.
12-16 (INTOLERABLE)	WORK SHALL NOT BE STARTED OR CONTINUED UNTIL THE RISK HAS BEEN REDUCED. IF REDUCTION IS NOT POSSIBLE,THE ACTIVITY SHALL BE PROHIBITED.

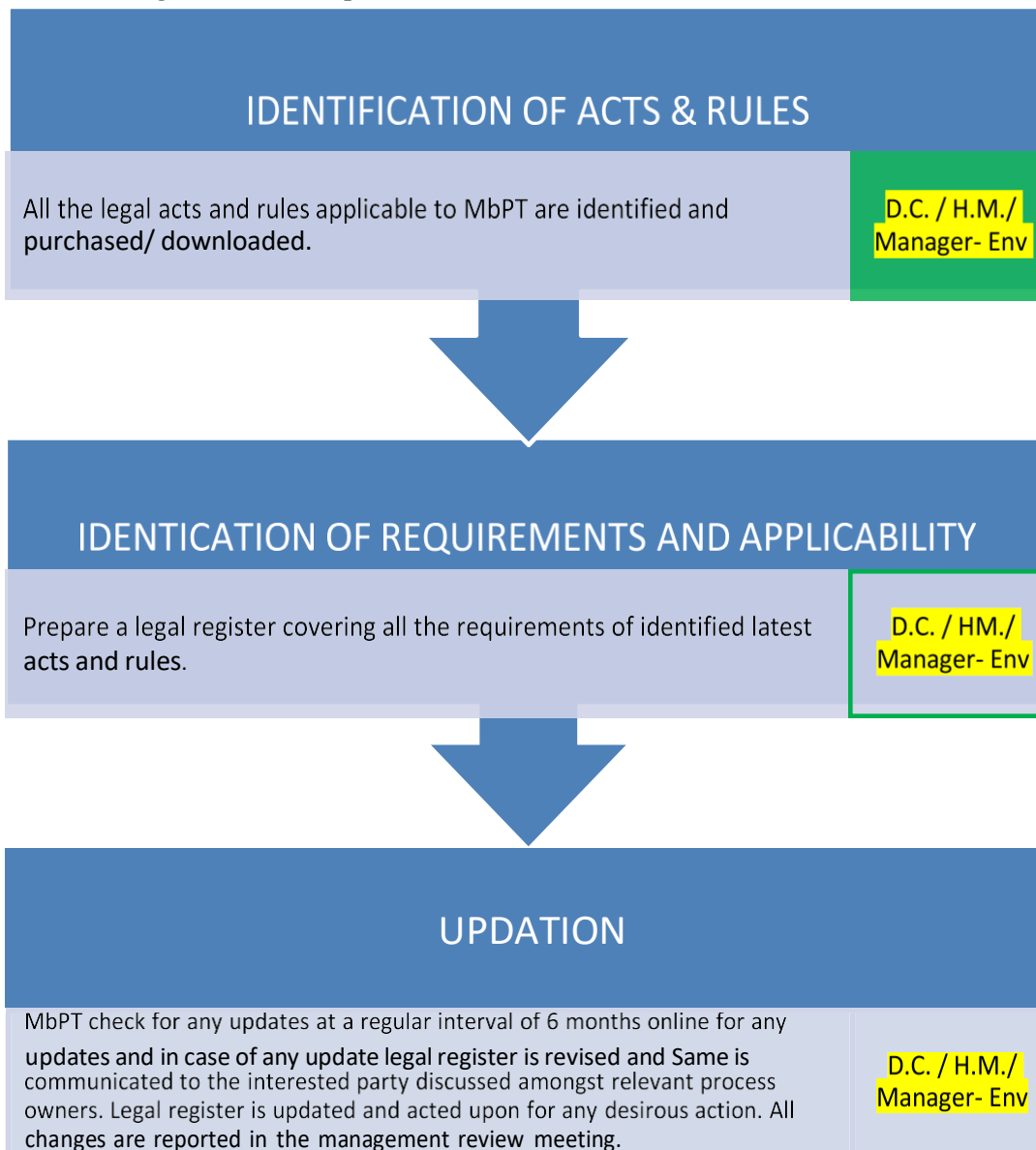
Procedure to determine compliance obligations

MbPT is working with the complete knowledge of all the statutory and regulatory requirements applicable on it. To determine the compliance obligation and continue to work safely Marine Department has maintained a legal register in which all the legal requirements are listed, these requirements are reviewed from time to time. These requirements are taken into consideration while establishing, implementing, maintaining and continually improving the IMS. (Refer Legal Register). Harbour Master ensures that all the environmental compliance requirements are identified in context of its applicability with Mumbai Port activities and respective department is guided to meet the environmental compliance requirements.

 MUMBAI PORT AUTHORITY		Department	MANAGEMENT			Page No.	10
		Title	IMS APEX MANUAL			Date	03-02-2020
		Section 4	ENVIRONMENT SPECIFIC POLICIES & PROCEDURES			Revision	00
LIKELIHOOD OF OCCURANCE	CERTAIN (Constantly in normal conditions)	4	4	8	12	16	
	LIKELY (Intermittent in normal conditions, weekly or monthly)	3	3	6	9	12	
	OCCASIONAL (Possibly may occur, annually, may be due to staff or equipment failure)	2	2	4	6	8	
	UNLIKELY (To occur ,no evidence of occurring, extreme situation only)	1	1	2	3	4	
	SEVERITY OF ONSEQUENCES		1	2	3	4	
		MINIMAL IMPACT (Environmental impact reversible in 1 month)	MINOR IMPACT (short term localized impact reversible in 1 year)	MODERATE IMPACT (Medium term localized impact not reversible in 1 year)	MAJOR IMPACT (Long term impacts irreversible)		
LEGAL/ POLICY/ OTHERS			Effecting policy and procedures	Potential breach of regulations	Actual breach of regulations.		
REPUTATI ON			Potential for internal complaint	Potential for external complaint	Because of breach actual serious complaint/PR issue		
Carbon Emissions		Reduction in carbon emissions	No increase or decrease in carbon emission	Minor increase in carbon emission.	Major increase in carbon emission		

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	11
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 4	ENVIRONMENT SPECIFIC POLICIES & PROCEDURES	Revision	00

Process for legal and other requirement identification is as below:



 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	12
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 4	ENVIRONMENT SPECIFIC POLICIES & PROCEDURES	Revision	00

List of Acts & Rules applicable to MbPT

S.NO.	Title
1	Indian Port Act, 1908
2	Merchant Shipping Act, 1958
3	Customs Act, 1962
4	Major Port Trusts Act, 1963
5	MbPT Harbour Craft Rules, 1999
6	Dock Workers (safety, Health & Welfare) Act, 1986
7	Dock Workers (safety, Health & Welfare) regulations, 1990
8	MbPT (Licensing of Stevedores & Allied Matter Amendment) regulations, 1989
9	General Financial rules
10	Scales of Rates
11	IMO Regulations, 1974
12	Indian railway Act, 1890/Revised-1989
13	Railway Claims Tribunal Act 1989
14	Indian Railways Commercial Manual, 1967
15	Indian Railway Conference Association rules I and regulations, 1967
16	Mumbai (Bombay) Port railway Goods Tariff
17	Indian Vessels Act, 1917
18	Bombay Port trust Employees (Recruitment, Seniority and Promotion) Regulations, 1977.
19	The Port of Bombay (Responsibility For Goods) regulations, 1975
20	Bombay Port Trust (Licensing of Stevedores & Allied Maters) Regulations, 1989
21	Bombay Port Trust (Licensing & Control of Pilots) Regulations, 1975
22	Bombay Port Trust (Handling of Hazardous Cargo) Regulations, 1986
23	Bombay Port Trust (Destraint or Arrest and Sale of Vessels) Regulations, 1988
24	Bombay Port Trust General By-Laws, 1879
25	Bombay Port Trust Docks By-Laws, 1879
26	Bombay Port Trust Dry Docks By-Laws, 1879
27	Bombay Port Trust Warehouse By-Laws, 1947
28	Bombay Port Trust Pilotage By-Laws
29	Port of Bombay (Pilotage, Tug Assistance, Towage, Mooring & other fees) Order, 1988

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	13
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 4	ENVIRONMENT SPECIFIC POLICIES & PROCEDURES	Revision	00

30	Transport, Handling & Storage of Dangerous Goods in the port of Bombay regulations, 1944.
31	MARPOL 73/78
32	International Convention on Oil Pollution Preparedness, Response and Cooperation (OPRC), 1990
33	Coastguard Act, 1978
34	The Water (Prevention & Control of Pollution) Act, 1974, amended in 1988
35	Environment Protection Act, 1986 (amended 1991)
36	Coastal Regulation Zones Notification – 2019
37	The Air (Prevention & Control of Pollution) Act, 1981
38	The Solid Waste Management, Rules 2016
39	The E Waste Management, Rules 2016
40	The Plastic Waste Management, Rules 2016
41	The Hazardous and Other Wastes (Management & Transboundary Movement), Rules 2016
42	Environmental Impact Assessment Notification, 2006
43	The Manufacture Storage & Import of Hazardous Chemicals Rules, 1989

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	14
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 4	ENVIRONMENT SPECIFIC POLICIES & PROCEDURES	Revision	00

Communication Policy regarding environment

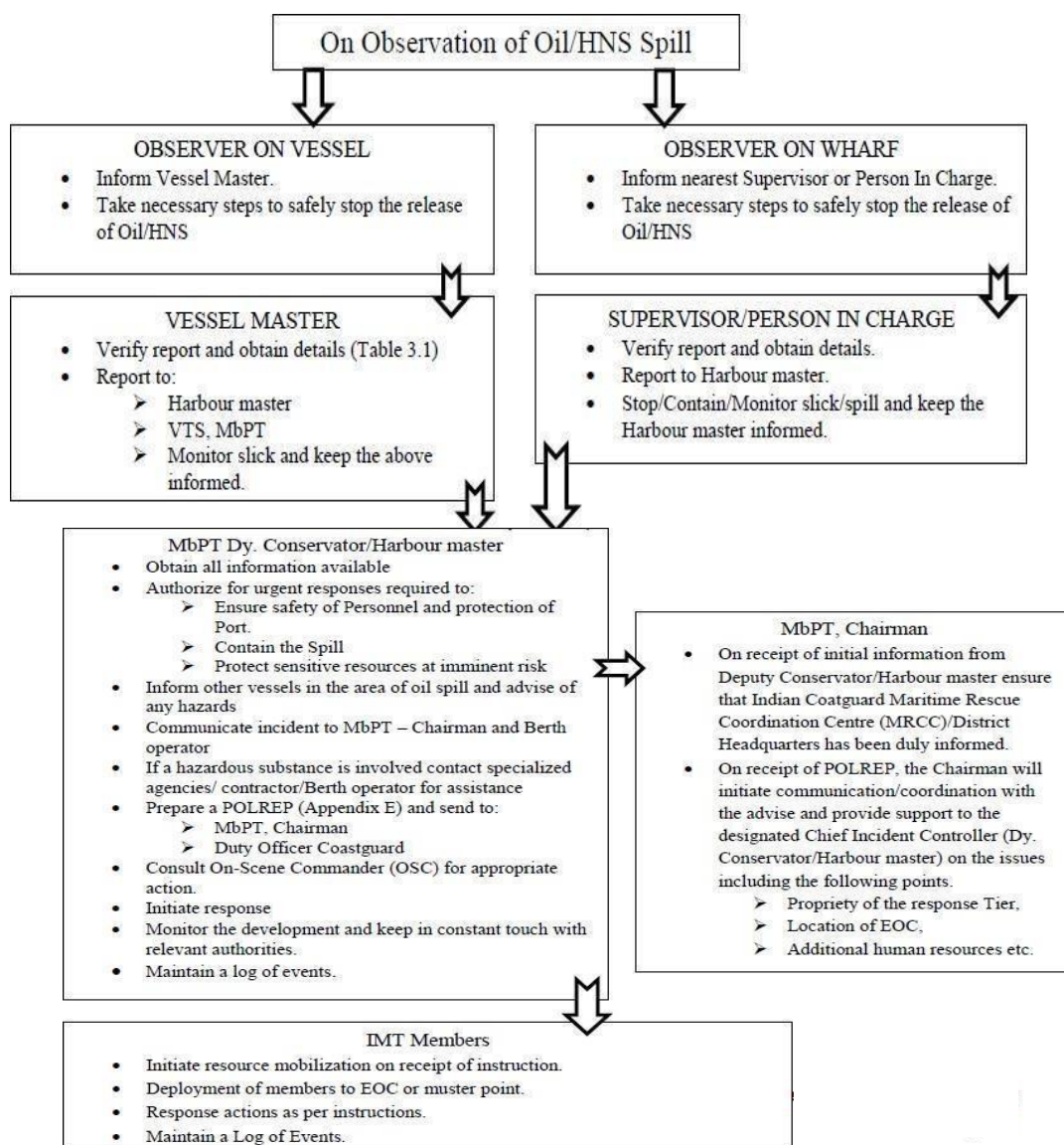
Communication					
S. No.	What To communicate	Who	With Whom	When	How
Internal					
1.	EMS Policy	Marine Department	Employees of MbPT	After every updation in policy	Display means
External					
2.	EMS Policy	MbPT	Stakeholders	After every updation in policy	E-Mail

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	15
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 4	ENVIRONMENT SPECIFIC POLICIES & PROCEDURES	Revision	00

Environmental Emergency preparedness & response

Marine Department has identified the environmental related emergency situations that are being addressed in the Contingency Plan. It presents all the potential emergency situations that can occur possibly in the future. This Oil Spillage Contingency Plan provide the mechanism, how to response in case of any emergency and these responses are checked/ practised in form of regular mock drills and Exercise involving all stake holders at least once in every year. (Refer Oil Spillage Contingency Plan.)

MUMBAI PORT AUTHORITY OSCP ACTION FLOWCHART



 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	1
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Section - 5

Information Security Specific Policies & Procedures

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	2
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Definitions

<u>Term</u>	<u>Definition</u>
A	
Access control	Means to ensure that access to assets is authorized and restricted based on business and security requirements
Attack	Attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset
Authentication	Provision of assurance that a claimed characteristic of an entity is correct
Authenticity	Property that an entity is what it claims to be
Availability	property of being accessible and usable on demand by an authorized entity
Audit Conclusion	Outcome of an audit, after consideration of the audit objectives and all audit findings
B	
Base measure	Measure defined in terms of an attribute and the method for quantifying it
C	
Confidentiality	Property that information is not made available or disclosed to unauthorized individuals, entities, or processes
Consequence	Outcome of an event affecting objectives
Control	Measure that is modifying risk
Control objective	Statement describing what is to be achieved as a result of implementing controls
D	
Derived measure	Measure that is defined as a function of two or more values of base measures
E	
Event	Occurrence or change of a particular set of circumstances
External context	External environment in which the organization seeks to achieve its objectives
F	
G	

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	3
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Governance of information security	System by which an organization's (3.50) information security (3.28) activities are directed and controlled
Governing body	Person or group of people who are accountable for the performance and conformity of the organization
H	
I	
Information need	Insight necessary to manage objectives, goals, risks and problems
Information processing facilities	Any information processing system, service or infrastructure, or the physical location housing it
Information security	Preservation of confidentiality, integrity and availability of information
Information security continuity	Processes and procedures for ensuring continued information security operations
Information security event	Identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that can be security relevant
Information security incident	Single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security
Information security incident management	Set of processes for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents
Information security management system (ISMS) professional	Person who establishes, implements, maintains and continuously improves one or more information security management system processes
Information sharing community	Group of organizations that agree to share information
Information system	Set of applications, services, information technology assets, or other information-handling components
Integrity	Property of accuracy and completeness
Internal context	Internal environment in which the organization (3.50) seeks to achieve its objectives
J	
K	
L	

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	4
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Level of risk	Magnitude of a risk expressed in terms of the combination of consequences and their likelihood
Likelihood	Chance of something happening
M	
Measure	Variable to which a value is assigned as the result of measurement
Management System	Set of interrelated or interacting elements of an Organization to establish policies and objectives, and processes to achieve those objectives
Measurement function	Algorithm or calculation performed to combine two or more base measures
Measurement method	Logical sequence of operations, described generically, used in quantifying an attribute with respect to a specified scale
N	
Non-repudiation	Ability to prove the occurrence of a claimed event or action and its originating entities
O	
Objective	Result to be achieved
Organization	Person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives
Outsource	Make an arrangement where an external Organization performs part of an Organization's function or process
P	
Performance	Measurable result
Policy	Intensions and directions of an Organization as formally expressed by its top management
Preventive Action	Action to eliminate the cause of a potential nonconformity or other potential undesirable situation
Procedure	Specified way to carry out an activity or a process
Process	Set of interrelated or interacting activities that use inputs to deliver an intended result
Q	

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	5
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

R	
Reliability	Property of consistent intended behaviour and results
Residual risk	Risk remaining after risk treatment
Review	Activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives
Review object	Specific item being reviewed
Review objective	Statement describing what is to be achieved as a result of a review
Risk acceptance	Informed decision to take a particular risk
Risk analysis	Process to comprehend the nature of risk (3.61) and to determine the level of risk
Risk assessment	overall process of risk identification, risk analysis and risk evaluation
Risk communication and consultation	Set of continual and iterative processes that an organization conducts to provide, share or obtain information, and to engage in dialogue with stakeholders regarding the management of risk
Risk criteria	Terms of reference against which the significance of risk is evaluated
Risk evaluation	Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable
Risk identification	Process of finding, recognizing and describing risks
Risk management process	Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context and identifying, analysing, evaluating, treating, monitoring and reviewing risk
Risk owner	Person or entity with the accountability and authority to manage a risk
Risk treatment	Process to modify risk
S	
Security implementation standard	Document specifying authorized ways for realizing security
T	
Threat	Potential cause of an unwanted incident, which can result in harm to a system or organization

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	6
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Trusted information communication entity	Autonomous organization supporting information exchange within an information sharing community
U	
V	
Vulnerability	Weakness of an asset or control that can be exploited by one or more threats

Organization of ISMS Processes

Information Security Org structure, Roles and responsibilities

IS Governance Structure is as depicted below:

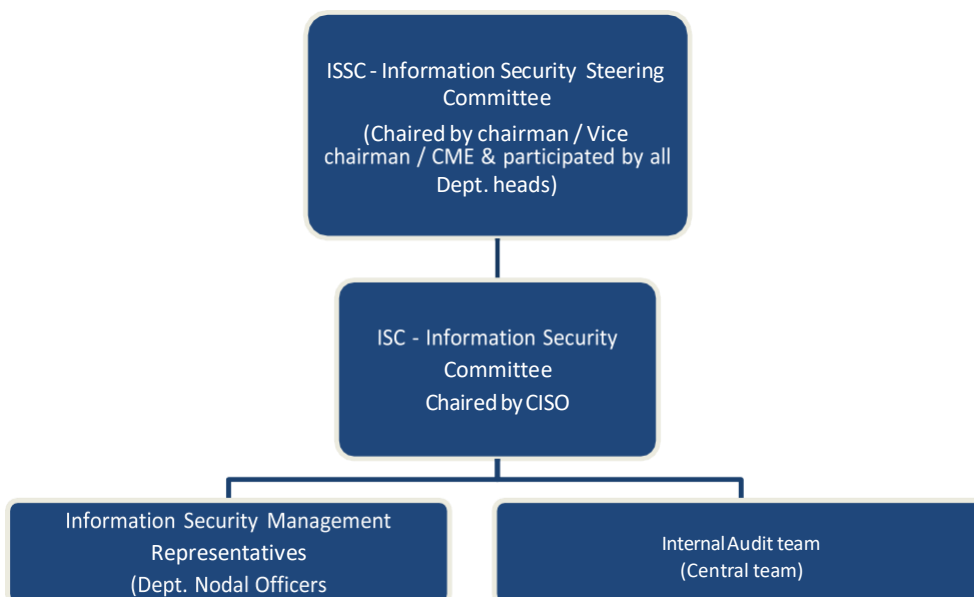


Figure 2: IS Governance Structure

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	7
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Below is the role to organizational representation mapping for Governance of ISMS:

S. No.	Roles	Organizational Representation
1.	Information Security Steering Committee (ISSC)	Chairman / Deputy Chairman/ Chief Mechanical Engineer and other HOD's / Divisional Heads / Commandant CISF / Chief Security Officer
2.	Information Security Committee (ISC)	Information Security Management Representatives from all MbPT locations and under the chairmanship of CISO.
3.	Chief Information Security Officer (CISO)	Joint Director
4.	Information Security Management Representative	Nodal officers of Dept. for all MbPT locations
5.	Enabling Function Heads	Unit/Department Heads / Process owners

Table 2: Mapping of Organizational representation to governing roles of ISMS

Responsibility

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	8
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Information Security Steering Committee (ISSC): The Information Security Committee shall take overall responsibility for information security, including:

- Define and provide guidance for the alignment of Information security goals & objectives to the MbPT's overall business goals and objectives.
- Ensure that information security goals are identified and it meets other legal compliance requirements;
- Approve and provide support to Information Security initiatives to enhance overall information security posture of MbPT;
- Drive and initiate information security awareness programs for all the employees in MbPT;
- Decide on future security solutions to be implemented at MbPT based on recommendations from CISO and Security Committee;
- Identify key roles and assign information security management responsibilities.
- Approve assignment of key members and provide resources to implement information security policies, procedures and controls.

Information Security committee (ISC): The Security Committee shall promote security within the company through appropriate commitment and adequate resources. The SC shall be responsible for:

- Approving the Information security policies and subsequent changes to the same;
- Reviewing major information security incidents with due assistance from the CISO;
- SC shall review the information security status at least once in six months in the Steering Committee meetings (i.e. management review meeting);
- Approving major initiatives to enhance information security; and
- Providing adequate resources (financial, human) to implement and improve the ISMS at MbPT.

In addition to the above responsibilities the other activities that an SC is responsible for has been detailed within the activity to responsibility matrices within the subsequent sections of this document.

Chief Information Security Officer (CISO):

To ensure a structured mechanism, in accordance with best information security system practices, it is necessary to identify a member of senior management as a 'Chief Information Security Officer (CISO)' to establish a cyber-security program, coordinate security policy compliance efforts across the organization and interact regularly with CERT-In 'Point of Contact'. The CISO must be given the mandate and resources to establish an Information Security program, coordinate security policy compliance efforts across the organization and interact regularly with regulatory agencies such as CERT-In.

The roles and responsibilities of the CISO (in addition to the responsibilities mentioned for SC) shall include:

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	9
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

- Coordinating with the teams to ensure that the MbPT ISMS is closely integrated with the information security requirements;
- Providing approvals for Information security policies and subsequent changes to the same; and
- In case of any major IT information security incident that requires communication with the MbPT employees, the CISO is responsible for sending notification to the affected parties.

In addition to the above responsibilities, the other activities that a CISO is responsible for, has been detailed within the activity to responsibility matrices within the subsequent sections of this document and in the document issued by INDIAN-COMPUTER EMERGENCY RESPONSE TEAM, Ministry of Electronics and IT, Government of India vide No. 6(12)/2017-PDP-CERT-In Dated: 14/03/2017.

5.6.4. Information Security Management Representatives: The members of the ISC are the location heads for all the MbPT locations. The responsibilities of the ISC members shall include:

- Approving the department/ location specific documents (for example: Information Asset registers, Risk Registers and likewise);
- Suggest Location/ Function specific initiatives to enhance information security;
- Review high impact information security incidents with due assistance from the Incident Response team;
- Maintain information Security posture within the Location/Function;
- Provide inputs in Non-Conformity and Corrective Action (NCCA) report for their Location/ Function;
- Take appropriate closure actions for the observations and non-conformances within their Location/ Function; and
- Work with Department Champions during the annual Asset register and Risk register updates.

In addition to the above responsibilities, the other activities that ISC members are responsible for have been detailed within the activity to responsibility matrices within the subsequent sections of this document.

Department Champions: The Department Champions report to the respective ISC members and are responsible for preparing and updating all the ISMS procedures as well as the asset and risk registers and the risk treatment plan among other ISMS documents.

In addition to the above responsibilities, the other activities that Depart Champions are responsible for have been detailed within the activity to responsibility matrices within the subsequent sections of this document.

Function Heads: The MbPT enabling Function Heads have the following roles and responsibilities:

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	10
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

- Assisting the ISC in identifying the ISO 27001:2013 controls managed and owned by their respective function;
- Ensuring that all the reports identified to be exchanged in a timely manner for showcasing compliance to ISMS; and
- Reporting any Information security incident, event or weakness to the ISC and working closely with the IRT to perform the required remediation to close them.

Individual responsibilities: Employees play a critical role in information security management at MbPT. Employees should follow and comply with the requirements of ISMS, data security and the applicable legal and contractual obligations. All employees should undertake the necessary preventive precautionary, as well as designated reactive, steps with regard to incidents. Following are the responsibilities of all employees at MbPT:

- Shall be aware of the ISMS Policy and Objectives;
- Ensuring active participation in ISMS initiatives like ISMS training and awareness, ISMS audits, reviews, etc.;
- To report about incidents/ security breaches and suspected incidents to either the nominated ISC member of their Location/ Function;
- To understand the importance of data protection and data security responsibilities as part of their job functions;
- Maintaining the strict confidentiality of personal data and organizational data;
- To dispose confidential and restricted information in their possession in accordance with the organization's disposal policy; and
- Taking all appropriate legal, organizational, and technical measures, in accordance with MbPT's policies, to protect the confidentiality of organizations data, against accidental or unlawful disposal or accidental loss, alteration, unauthorized disclosure and against all other unlawful forms of processing, keeping in mind the nature of such data.

Third-party Employees, Vendors and Consultants: MbPT has critical dependency on third party employees, consultants and vendors for its operations. These external parties often visit or work out of MbPT premises.

All external parties (i.e. third party employees, vendors, consultants and interns) should participate and assist MbPT in undertaking the necessary precautionary/ preventive, as well as reactive, steps towards controlling information security breaches.

Following are the responsibilities of all external/ third parties at MbPT:

- To understand and follow MbPT ISMS Policy (when accessing MbPT's information systems/ assets and while visiting MbPT offices); and
- Ensuring active participation in ISMS initiatives like training and awareness, audits and reviews (where applicable); and
- Ensuring instant communication and reporting of breaches or suspected incidents to ISC/ IT help desk, as applicable.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	11
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

ISMS policies

MbPT Information Security Policy

INFORMATION SECURITY POLICY

‘MUMBAI PORT AUTHORITY’ is committed to maintain robust security practices and controls to preserve Confidentiality, Integrity and availability of information by optimal processes, technology and trained personnel from applicable threats, whether internal or external, deliberate or accidental.

The overall information security framework is established to ensure

- ✓ Information is available and usable when required and the systems that provide it can resist and recover from failures (availability)
- ✓ Information is accessed by or disclosed to only those who have right to know (Confidentiality)
- ✓ Information is protected against un-authorized Access and modifications (Integrity)
- ✓ Business transactions as well as information exchange between organization locations or with partners/users can be trusted (Authenticity and non-repudiation)
- ✓ Continual improvements of ISMS

All employees of MUMBAI PORT AUTHORITY shall be committed in true spirit for compliance of applicable ISMS and Legal / Regulatory requirements in accordance with the set documented procedures as per ISO 27001:2013.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	12
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

MbPT Information Security Objectives

‘MUMBAI PORT AUTHORITY’ has proposed to establish, implement, maintain and continually improve its information Security management system.

In this direction, MbPT has established information security objectives at relevant functions and levels which are consistent with information security policy and has taken into account applicable information security requirements and results from risk assessment and risk treatment.

Information Security Objectives are mentioned in below table.

S.no.	Information Security Objective	Target
1	ISMS awareness to all personnel	100%
2	Number of critical information security incidents reported in a year	Less than 3
3	Compliance to applicable Legal / Regulatory requirements	100%

MbPT shall put into place robust monitoring and measurement process to monitor the performance and report results of these objectives to top management as part of management review process. These Information Security Objectives shall be reviewed and updated at least once in a year and shall be communicated to all employees.

For planning to achieve these information security objectives, MbPT shall determine:

- 1) Action required for achieving these results
- 2) Resources requirement
- 3) Responsibility
- 4) Timelines to achieve
- 5) Evaluation of results

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	13
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

ISMS scope of application

The Information Security Management System of MUMBAI PORT AUTHORITY applies to Port Operations, Financial management, Materials Management, Vessel Traffic System (VTS), CCTV Surveillance and Access Control Systems supported by HR, IT, Administration, Traffic, Marine and Finance at its Mumbai locations of Ambedkar Bhavan, Yantra Bhavan and Sr. Dock Master ID office, as per SOA Version number V1.0 This includes end user equipment's and passive/activenetwork devices as per SOA Version number V1.0 1 March 2021

ISMS activities shall include all the areas mentioned below:

S. No.	Location	Business Functions
1	Ambedkar Bhavan	• Projects Management • Application programming • Software Change Management • IT Security Management • Website Management Content Updation • Vendor Management • Network Administration and Maintenance • Antivirus Updation, Spam Protection and Web /SMS Gateway • IT Procurement • IT Infrastructure Management • IT Resource Management • Governance of outsourced systems / Applications
2	SDM (ID-Office – DOCK Master control station)	• VTMS
3	Yantra Bhavan	• CCTV central servers (DVR)

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	14
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Exclusions:

The Following MbPT applications are excluded from scope:

- 1) Docks Auction Sales
- 2) Employee Information management system
- 3) Payroll
- 4) Pension
- 5) PF System
- 6) Pierce-rate application
- 7) Housing Loan
- 8) Estate billing

Brief description

The IT infrastructure (Servers, desktops/laptops, network switches) is maintained by outsourced agencies HPE, Acer, & Dell.

Details of In-scope Projects and its management is as below.

Sr	Project Name	Project Development (In-house / outside)	Operated by	Maintained by
1	IPOS	Outside (CMC computers)	In-house	In-house
2	FMS	Outside (3i Infotech computers)	In-house	In-house
3	IMMS	In-house	In-house	In-house
4	VTs	Outside (Airbus)	In-house	Outsourced (Marine electrical)
5	CCTV	Outside (Sonal Enterprises)	In-house	Outsourced (Sonal enterprise)
6	Access control	Outside (Wipro)	In-house	Outsourced (Wipro)

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	15
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Information Assets:

The Information Security Management System (ISMS) applies to the information assets (including asset types

-Physical, Software, Paper, People, Information, Service and Site) of MbPT, for the business functions and office locations, mentioned above, including but not limited to the following:

- All proprietary information that belongs to MbPT;
- Personal information relating to employees;
- All client information held by MbPT;
- All suppliers, contractors, partners and other third party information, held by MbPT;
- All software assets, such as application software, system software, development tools and utilities, databases and data files, system documentation, user documentation, training materials, which are owned by MbPT;
- All physical assets, such as servers, switches, firewall, routers, computer equipment, communications equipment, media, hard-copy files and papers, and equipment relating to facilities which are maintained by MbPT (Enabling Functions);
- The technology (including hardware, networking, software and operations systems, where appropriate) employed in the scope offered for certificate;
- All services, such as power, lighting and HVAC.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	16
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Procedure for Information security risk assessment & treatment

Purpose:

The purpose of performing Risk Assessment is to ensure that

- MbPT's Information Security Management System achieve its intended objectives,
- Prevent or reduce undesired effects
- Achieve continual improvement
- Establish risk acceptance criteria
- Criteria for performing information security risk assessment

During this activity, MbPT shall identify the relevant threats and its areas of vulnerabilities and the ways to remediate these threats. Without such an assessment, it would not be able to determine what it should protect, the level of protection it should implement.

Scope:

This applies to the IT infrastructure of all areas managed by the company that contain information and information processing facilities.

Responsibilities:

Process owner: IT Team

Terms / Definitions and abbreviations (in alphabetical order):

Dept.	Department
Doc	Document
HOD	Head of Department
ISMS	Information Security Management System
ISO	International Organisation for Standardization
IT	Information Technology
M.D	Managing Director
NCR	Non Conformance Report
Non-conformity	Non fulfilment of requirement
NR	Nominated Representative
Observation	Opportunity for improvement. Observation could be positive or a gap.
PR	Procedure
QM	Quality Management
Rev	Revision
MGMT	Top Management
Risk	The effect of uncertainty on organization Objectives
Risk Assessment(RA)	Overall process of risk analysis and risk evaluation.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	17
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Risk Analysis	Systematic use of information to identify sources and to estimate the risk level
Risk Evaluation	Process of comparing the estimated risk against given risk criteria to determine the significance of the risk
Risk Management	Coordinated activities to direct and control an organization with regard to risk. Risk management typically includes risk assessment, risk treatment, risk acceptance and risk communication.
Residual Risk	The remaining risk after risk treatment
Asset	Anything that has value to the organization
Business Owner	The business person(s) with the overall responsibility of the asset/process being assessed.
Threat	A potential cause of an unwanted incident, which may result in harm to a system or organization
Vulnerability	A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.
Risk Treatment (RT)	Process of selection and implementation of measures to modify risk.
Control	Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature
Risk Mitigation/Reduction	Actions taken to lessen the probability, negative consequences, or both, associated with a risk.
Risk Acceptance/Retention	Acceptance of the burden of loss, or benefit of gain, from a particular risk.
Risk Transfer	Sharing with another party the burden of loss or benefit of gain, for a risk.
Risk Avoidance	Decision not to become involved in, or action to withdraw from, a risk situation.

Activity/Steps:

1. Risk Assessment periodicity

- a) Risk identification, assessment and review to be conducted periodically once in 6 months and for any new asset that is going to be added/modified in the Asset Inventory

2. Identification and Assessment risks

- a) The identification and assessment of Security Requirements is based on Threats and Vulnerabilities against each of the assets. The threats and vulnerabilities are identified based on the threat-vulnerability database which would be reviewed yearly based on emerging risks and changes in threats as per organizational changes
- b) A threat is the potential for a particular threat-source to successfully exercise a particular vulnerability. Vulnerability is a weakness that can be accidentally triggered or intentionally exploited. A threat-source does not present a risk when there is no vulnerability that can be exercised
- c) Information security risk assessment process shall be applied to identify risk associated with the loss of confidentiality, integrity and availability for information within the scope MbPT's information Security Management System
- d) Risk Impact assessment

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	18
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

The following criteria will be applied when calculating a rating score for the Impact:

- The business impact caused by the threat is estimated on a scale of 1-4 where '1' being 'low' impact and '4' being 'high' impact
- The severity of the impact is estimated using the IMPACT ESTIMATION grid provided below:

Impact	Business / Impact Operational	Reputational	Legal Regulatory
Low (1)	Users Affected – Particular Department, no or low impact to organization, can be resolved quickly, Insignificant financial impact	Limited Media Coverage, large scale user complaints, some customer loss	Potential Consequence / Impact may be seen and includes Executive Management Involvement
Medium (2)	User Affected – One Location Isolation; Stakeholder concerns causing their dissatisfaction and having business impact, customer being the significant stakeholder here.	High negative media coverage, serious user / customer loss,	Inadequate compliance systems / issues, impact on any Licensing Obligation
High (3)	User Affected – Entire Organisation; Has long term business impact (includes all Product Safety incidents).	Very high negative media coverage, large scale user / customer Loss	Serious inadequate compliance systems / issues, serious impact on any Licensing Obligation

a. Calculation of Rating of likelihood / Probability

- The probability is the likelihood of threat agent exploiting the vulnerability resulting in threats to assets.
- As part of the Information Security Risk Analysis process, it is requirement to ascertain a score for the likelihood of the threat exploiting a vulnerability of an information asset. Probability should be based upon the incidents that have occurred in the past and have led to operational failures or delays.
- The following criteria will be applied when calculating a rating score for likelihood of the threat happening

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	19
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Probability	Description
Highly Unlikely (1)	Occurs once in 2-4 years
Unlikely (2)	Occurs once in 1 -2 years
Likely (3)	Occurs more than once in year
Highly Likely (4)	Occurs up to monthly or almost every month

3. Calculation of Risk Score

- The 'Existing Risk' calculation comprises of the following components:
- The risk exposure is calculated as a product of the probability/likelihood and the severity/Impact using the formula:
- $Risk\ Score = Probability \times Severity$
- The preventive controls shall affect the likelihood of the occurrence whereas the corrective controls shall affect the severity of the impact
- To calculate the 'Existing Risk' it is necessary to multiply each of the Existing Risk Components with each other (i.e. Existing Risk = Severity x Probability).
- The higher the resultant score - the higher the Existing Risk. The highest Risk Impact Rating on this basis is therefore, 12, with the lowest possible Risk Impact Rating being 1
- The template captures overall risk levels (rollups) which usually is the highest risk level after considering all the threat-vulnerability scenarios. The RA and RTP sheet also captures the management's decision on the risk treatment plan

Risk Score:

Level	Range
Low	≤ 3
Medium	>3 and < 8
High	≥ 8

4. Risk Acceptance Criteria

- Risk treatment option is selected by the process owner based on the following guide
- To the extent possible, all the risks identified shall be considered for the risk treatment
- In exceptional cases the existing risk of greater than 8 (i.e. >8) may be 'Accepted' with an appropriate Business justification (E.g. the cost of implementing and maintaining the required control is higher than the actual estimated impact on the business) or explicit Management approval as it may be the risk of providing the services and cannot be mitigated or there could be implementation constraints on the mitigation measures
- The overall risk score of less than 8 as the cumulative value will be accepted
- However, the overall risk score of equal to or greater than 8 (i.e. ≥ 8) as the cumulative value will be used for treatment

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	20
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

5. Risk Evaluation

- a. Risk evaluation involves comparing the results of risk analysis with the risk acceptance criteria
- b. Prioritizing the analysed risk for risk treatment.
- a. Risks are prioritized on the basis of risk score.
- b. Risks having higher risk score ratings shall be prioritized over the other risks

6. Risk treatment

- a. To the extent possible, all the identified and evaluated risks shall be taken for risk treatment.
- b. Risk treatment involves selecting the appropriate information security risk treatment options, taking account of the risk assessment results
- c. Since the elimination of all risks is usually impractical, MbPT will use the least-cost approach and implement the most appropriate controls to reduce the risk to an acceptable level
- d. The residual / balance of the risk, which is not covered, is consciously considered as acceptable risk which organization believes is inherent to the MbPT business and organization decides to live with it.
- e. Risk treatment can be achieved through any of the following risk treatment options:
 - i. Risk Avoidance – Deciding by not going ahead with an activity likely to generate risk
 - ii. Risk Mitigation - (a) Reduce the likelihood - By reducing probability of occurrence (b)Reduce the consequences – By reducing severity of vulnerability or by modifying the assets at risk in some way
 - iii. Risk Transference – By arranging another party to compensate for the loss, such as purchasing insurance
 - iv. Risk Acceptance – The organization bears all the risk
- f. Appropriate controls to reduce the assessed risks to an acceptable level will be identified and selected with cost/benefit justification.
- g. The selected controls shall be compared with those described in Annex A of ISO 27001:2013 requirements manual and care shall be taken to ensure that no necessary controls have been omitted
- h. While preparing the RTP, already existing and planned controls will be taken into account in the selection to avoid unnecessary duplication of controls. It is also possible that an existing or planned control may no longer be justified and may need to be removed, replaced by a more suitable control, or remains as it is due to cost reasons.
- i. The vulnerabilities and the associated threat indicate where additional controls may be required and the form it should take. Risk Treatment Plan will include suggested countermeasures
- j. When selecting controls, besides cost considerations and availability; other related factors need to be considered are the ease of implementation, time and cost of maintenance
- k. The Organization needs to manage risks and safeguard operations in order to protect information and information processing facilities effectively. Part of the process of judging whether the security of information is appropriate, is by acknowledging the fact that risks cannot be avoided completely and there will always be some residual risk
- l. The Organization, after internal assessment of exposure for risk impact and related business impact, reviewed that the threshold for Acceptable risk is less than 8. And for all exposures above this, the organization shall implement controls to reduce the risk to an acceptable level.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	21
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

7. Risk Residual

- a. After implementing controls to reduce the risks, a leftover risk or intentionally unaddressed risk is called as residual risk; as they constitute either a low risk area or cost of implementing controls for these domains does not justify the investment.
- b. All Risk owners shall review RTP and residual risks to ensure that risks are adequately addressed. While finalizing RTP, Inputs / suggestions from risk owners shall be sought to fine tune it. Management approval needs to be taken for acceptance of the residual risk.

Process performance indicators

Indicator 1	Identification & timely updation of risk assessment associated with organization.
Indicator 2	Identification & timely updation of risk treatment plan associated with organization.
Indicator 3	Identifying improvements Adherence to timely closure of RTP actions Trends of number of high risks over period of time

Risk and Opportunities

Risks	All interested parties and their related concerns not identified which may lead to negative impact. Inadequate identification of risks facing the organization resulting in financial loss and/or loss of brand image. Non fulfilment of statutory and regulatory requirements may lead to heavy penalties on organization.
Opportunities	Helps in taking proactive action on identified issues/concerns resulting in positive impact for the organization. Helps leveraging the opportunities for business growth/expansion, new product / service development , continual improvements

Relevant documents incl. guidelines, laws, standards and regulations

EC Directives, as applicable	-
Statutory & Regulatory requirements	IT ACT, Cyber security incident reporting to CERT-in, NCIIPC
Standards	ISO 27001:2013
	ISO 27002 (Security techniques, code of practice)

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	22
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

(National & International)	27005 (ISMS Risk Management)
Internal documents (Procedures / work instruction etc.)	Information security risk management policy (ISMS-L1-03) Information Security Management System manual

Documents

Documented information	Information security risk assessment and risk treatment results (ISMS-L1-03)
------------------------	--

Statement of Applicability (SOA)

ISO 27001 : 2013 Control	ISO 27001 : 2013 Control Description	ability (Yes/ No)	on for Applicability/ Non- Applicability	Implementation Status
A.5	Security Policy			
A.5.1	Management direction for information security		To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.	
A.5.1.1	Policies for Information Security –A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties	Yes	Information security policy document provides guidance for successful ISMS implementation. Information security policy is a means to show concern for Information Security and is required to convey management's point of view to the users.	Completed
A.5.1.2	Review of the policies for Information Security – The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness	Yes	Review & evaluation of information security policy addresses changes in the operating environment. Regular review ensures the continuing suitability, adequacy and effectiveness of the security policy.	Completed
A.6	Organization of information Security			
A.6.1	Internal Organization		To establish a management framework to initiate and control the implementation and operation of information security within the organization.	
A.6.1.1	Information Security roles and responsibilities – All information security responsibilities shall be defined and allocated.	Yes	Proper allocation of security responsibility is necessary to efficiently perform multiple tasks required for the implementation of ISMS.	Completed

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	23
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

ISO 27001 : 2013 Control	ISO 27001 : 2013 Control Description	Applicability (Yes/ No)	Justification for Applicability/ Non-Applicability	Implementation Status
A.6.1.2	Segregation of duties- Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.	Yes	Segregation of duties is important to reduce the risk of unauthorized or unintentional misuse or modification of organization's assets	Completed
A.6.1.3	Contact with authorities- Appropriate contacts with relevant authorities shall be maintained.	Yes	To perform its day-to-day operations and manage information security MbPT interacts / works with many organizations.	Completed
A.6.1.4	Contact with special interest groups - Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.	Yes	NIC teams, cyber security team and government bodies like CISF, IB, CERT-In and DeitY.	Completed
A.6.1.5	Information Security in Project Management- Information security shall be addressed in project management, regardless of the type of the project.	Yes	Assessing risks during project management is an important aspect.	Completed
A.6.2	Mobile devices and Teleworking	To ensure the security of teleworking and use of mobile devices.		
A.6.2.1	Mobile Device Policy- A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.	Yes	Mobile devices are allowed within the server farm area.	Completed
A.6.2.2	Teleworking- A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.	No	Teleworking is at present not allowed for MbPT operations.	Completed
A.7	Human Resources security			
A.7.1	Prior to employment	To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered.		

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	24
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

ISO 27001 : 2013 Control	ISO 27001 : 2013 Control Description	Compliance (Yes/ No)	Reason for Applicability/ Non-Applicability	Implementation Status
A.7.1.1	Screening - Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	Yes	MbPT team includes resources certain vendors. Hence, it is important to have screening of all working staff.	Completed
A.7.1.2	Terms and conditions of employment - The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.	Yes	MbPT may host highly critical information (valuable to customers) at its data centre. Terms & Conditions of employment binds the employees to perform only actions approved by the management.	Completed
A.7.2	During employment	To ensure that employees and contractors are aware of and fulfil their information security responsibilities.		
A.7.2.1	Management Responsibilities - Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.	Yes	Employees, Contractors and Third-party users are provided with access to information pertaining to their area of scope.	Completed
A.7.2.2	Information security awareness, education and training - All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular	Yes	Education and training helps the users become aware of information security policy and responsibilities.	Completed

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	25
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

	updates in organizational policies and procedures, as relevant for their job function.			
A.7.2.3	Disciplinary Process - There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.	Yes	Disciplinary process provides fair treatment to employees suspected of breach of security. It also acts as an effective tool to enforce information security policy compliance within the Organization.	Completed

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	26
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

ISO 27001 : 2013 Control	ISO 27001 : 2013 Control Description	Compliance (Yes/No)	Reason for Applicability/ Non-Applicability	Implementation Status
A.7.3	Termination or change of employment	To protect the organization's interests as part of the process of changing or terminating employment.		
A.7.3.1	Termination or change of employment responsibilities -Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.	Yes	Process of employment termination or change of employment needs to be clearly defined and assigned as MbPT employs vendor/outsourced resources who have access to MbPT critical information.	Completed
A.8	Asset management			
A.8.1	Responsibility for assets	To identify organizational assets and define appropriate protection responsibilities.		
A.8.1.1	Inventory of assets – Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.	Yes	MbPT has important assets, which need to be identified and protected.	Completed
A.8.1.2	Ownership of assets - Assets maintained in the inventory shall be owned.	Yes	Each information assets is used for different purposes by a concerned department, so ownership needs to be defined which would bring accountability for each asset.	Completed
A.8.1.3	Acceptable use of assets - Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.	Yes	To ensure that information assets are used only for business and operational purposes, and are protected from damage due to non-official usage.	Completed
A.8.1.4	Return of assets - All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.	Yes	To ensure all the critical MbPT information is protected, return of all MbPT assets needs to be ensured.	Completed

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	27
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

ISO 27001 : 2013 Control	ISO 27001 : 2013 Control Description	Compliance (Yes/No)	Reason for Applicability/ Non-Applicability	Implementation Status
A.8.2	Information Classification	To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.		
A.8.2.1	Classifications of Information - Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.	Yes	MbPT has important assets, which need to be identified and protected. Classifying the assets helps in implementing protection (controls) commensurate with the value of the information asset.	Completed
A.8.2.2	Labelling of information - An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	Yes	Labelling of assets is needed to inform the criticality and sensitivity of the asset in place.	Completed
A.8.2.3	Handling of assets- Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	Yes	MbPT has important assets, which need to be identified and protected from unauthorized access.	Completed
A.8.3	Media Handling	To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.		
A.8.3.1	Management of removable media- Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.	Yes	MbPT uses removable media. USB access is provided to users. The tape drives are also used.	Completed
A.8.3.2	Disposal of media- Media shall be disposed of securely when no longer required, using formal procedures.	Yes	A process that defines disposal requirements is necessary to cover the risks of insecure disposal of media	Completed
A.8.3.3	Physical media transfer- Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.	Yes	Media can be transported containing MbPT critical information between MbPT's locations.	Completed
A.9	Access Control			

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	28
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

ISO 27001 : 2013 Control	ISO 27001 : 2013 Control Description	Compliance (Yes/No)	Reason for Applicability/ Non-Applicability	Implementation Status
A.9.1	Business Requirement for Access Control	To limit access to information and information processing facilities.		
A.9.1.1	Access Control Policy – An access control policy shall be established, documented and reviewed based on business and security requirements for access.	Yes	MbPT has critical information systems to which access has to be given to personnel in a controlled manner.	Completed
A.9.1.2	Access to networks and network services- Users shall only be provided with access to the network and network services that they have been specifically authorized to use.	Yes	Considering the criticality of MbPT network, access needs to be restricted.	Completed
A.9.2	User Access Management	To ensure authorized user access and to prevent unauthorized access to systems and services.		
A.9.2.1	User Registration and deregistration – A formal user registration and de-registration process shall be implemented to enable assignment of access rights.	Yes	MbPT has multi-user information systems.	Completed
A.9.2.2	User access provisioning - A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.	Yes	User access provisioning is required.	Completed
A.9.2.3	Management of privileged access rights- The allocation and use of privileged access rights shall be restricted and controlled.	Yes	MbPT hosts information that needs to be given access on need to know basis.	Completed
A.9.2.4	Management of secret authentication information of users - The allocation of secret authentication information shall be controlled through a formal management process.	Yes	The authentication information management is critical to MbPT applications.	Completed
A.9.2.5	Review of User Access Rights – Management shall review users access rights at regular intervals using a formal process	Yes	MbPT has multiple user access levels and change from one category to another is often required.	Completed

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	29
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

ISO 27001 : 2013 Control	ISO 27001 : 2013 Control Description	Compliance (Yes/No)	Reason for Applicability/Non-Applicability	Implementation Status
A.9.2.6	Removal or adjustment of access rights - The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.	Yes	Removal mechanism needs to be established.	Completed
A.9.3	User Responsibilities	To make users accountable for safeguarding their authentication information.		
A.9.3.1	Use of secret authentication information - Users shall be required to follow the organization's practices in the use of secret authentication information.	Yes	Required for user access and authorization.	Completed
A.9.4	System and application access control	To prevent unauthorized access to systems and applications.		
A.9.4.1	Information access restriction - Access to information and application system functions shall be restricted in accordance with the access control policy.	Yes	As per access control policy.	Completed
A.9.4.2	Secure log-on procedures - Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.	Yes	As per access control policy.	Completed
A.9.4.3	Password management system - Password management systems shall be interactive and shall ensure quality passwords.	Yes	As per access control policy.	Completed
A.9.4.4	Use of privileged utility programs - The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.	Yes	As per access control policy.	Completed
A.9.4.5	Access control to program source code - Access to program source code shall be restricted.	Yes	As per access control policy.	Completed
A.10	Cryptography			
A.10.1	Cryptographic controls	To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.		

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	30
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

ISO 27001 : 2013 Control	ISO 27001 : 2013 Control Description	Compliance (Yes/No)	Reason for Applicability/ Non-Applicability	Implementation Status
A.10.1.1	Policy on the use of cryptographic controls - A policy on the use of cryptographic controls for protection of information shall be developed and implemented.	Yes	Required for eTendering applications and will be required in near future when VPN/ERP would be set up.	Completed
A.10.1.2	Key management - A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.	Yes	Required for eTendering applications and will be required in near future when VPN/ERP would be set up.	Completed
A.11	Physical and environmental security			
A.11.1	Secure areas	To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.		
A.11.1.1	Physical security perimeter – Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.	Yes	MbPT houses important information assets in its premises, which need to be protected.	Completed
A.11.1.2	Physical entry controls – Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	Yes	MbPT houses important information assets in its premise, which need to be protected from unauthorized physical access.	Completed
A.11.1.3	Securing offices, rooms and facilities – Physical security for offices, rooms and facilities shall be designed and applied	Yes	Since MbPT hosts client's critical information and additional physical entry controls are required.	Completed
A.11.1.4	Protecting against external and environmental threats - Physical protection against damage from fire, flood, earthquake, explosion, civil unrest and other forms of natural or man-made disaster shall be designed and applied.	Yes	Assets are important for MbPT and hence it requires protection from external and environmental threats.	Completed
A.11.1.5	Working in secure areas - Physical protection and guidelines for working in secure areas shall be designed and applied.	Yes	Since MbPT hosts client's critical information and additional physical entry controls are required.	Completed

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	31
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

ISO 27001 : 2013 Control	ISO 27001 : 2013 Control Description	Compliance (Yes/No)	Reason for Applicability/ Non-Applicability	Implementation Status
A.11.1.6	Delivery and loading areas - Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises shall be controlled and if possible isolated from information processing facilities to avoid unauthorized access	Yes	Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.	Completed
A.11.2	Equipment	To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.		
A.11.2.1	Equipment siting and protection – Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access	Yes	As Information assets are sensitive to environmental conditions, they need additional protection against known threats.	Completed
A.11.2.2	Supporting utilities - Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities	Yes	Power is required for smooth running of operations at MbPT.	Completed
A.11.2.3	Cabling Security – Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.	Yes	Cables carry data, voice & power within the MbPT premises.	Completed
A.11.2.4	Equipment maintenance – Equipment shall be correctly maintained to ensure its continued availability	Yes	Maintenance of equipment is essential to reduce the chances of unexpected failure.	Completed
A.11.2.5	Removal of assets - Equipment, information or software shall not be taken off-site without prior authorization.	Yes	Equipment, information or software is an important asset for a data centre and should be taken to an off-site location after approval.	Completed
A.11.2.6	Security of equipment and assets off-premises – Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.	Yes	Security should be applied to off-site equipment taking into account the different risks of working outside the organization's premises.	Completed

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	32
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

ISO 27001 : 2013 Control	ISO 27001 : 2013 Control Description	Compliance (Yes/No)	Reason for Applicability/ Non-Applicability	Implementation Status
A.11.2.7	Secure disposal or re-use of equipment – All items of equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.	Yes	A process that defines disposal requirements is necessary to cover the risks of insecure disposal of physical and electronic information assets.	Completed
A.11.2.8	Unattended user equipment - Users shall ensure that unattended equipment has appropriate protection.	Yes	Appropriate User policy required to address this	Completed
A.11.2.9	Clear desk and clear screen policy - A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.	Yes	Lot of paper work is performed and maintained in government entities like MbPT.	Completed
A.12	Operations Security			
A.12.1	Operational procedures and responsibilities	To ensure correct and secure operations of information processing facilities.		
A.12.1.1	Documented operating procedures – Operating procedures shall be documented, maintained and made available to all users who need them.	Yes	MbPT has critical information systems, which need to be handled in a standard way to prevent failures.	Completed
A.12.1.2	Change Management - Changes to information processing facilities and systems shall be controlled.	Yes	MbPT has critical information systems, and an appropriate change management process is required to ensure secure and correct operations	Completed
A.12.1.3	Capacity Management – The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.	Yes	Capacity management is required to maintain effective operations at MbPT.	Completed
A.12.1.4	Separation of development, testing and operational environments – Development and testing facilities shall be separated from operational facilities. Rules for the migration of the software from the development to operational status needs to be defined and documented.	Yes	System engineers & Senior System engineers have privileged access to critical information systems.	Completed
A.12.2	Protection from malware	To ensure that information and information processing facilities are protected against malware.		

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	33
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

ISO 27001 : 2013 Control	ISO 27001 : 2013 Control Description	Compliance (Yes/No)	Reason for Applicability/ Non-Applicability	Implementation Status
A.12.2.1	Controls against malware- Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.	Yes	MbPT being a National Critical Infrastructure, this control is important.	Completed
A.12.3	Back up	To protect against loss of data.		
A.12.3.1	Information back up- Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.	Yes	The critical information on information systems needs to be available even in case of system failure.	Completed
A.12.4	Logging and Monitoring	To record events and generate evidence.		
A.12.4.1	Event Logging - Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.	Yes	Audit trail of system use is required for future investigations.	Completed
A.12.4.2	Protection of log information - Logging facilities and log information shall be protected against tampering and unauthorized access	Yes	Application logs for the operations and information processing need to be preserved for a certain period to review them for any incident.	Completed
A.12.4.3	Administrator and operator logs - System administrator and system operator activities shall be logged.	Yes	System engineers & Senior System engineers have privileged access to critical systems.	Completed
A.12.4.4	Clock synchronization - The clocks of all relevant information processing systems within an organization or security domain shall be synchronized with an agreed accurate time source.	Yes	Clock synchronization is required for accurate interpretation of event logs from multiple systems.	Completed
A.12.5	Control of operational software	To ensure the integrity of operational systems.		
A.12.5.1	Installation of software on operational systems - Procedures shall be implemented to control the installation of software on operational systems.	Yes	MbPT uses proprietary and third party software applications.	Completed
A.12.6	Technical vulnerability management	To prevent exploitation of technical vulnerabilities.		

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	34
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

ISO 27001 : 2013 Control	ISO 27001 : 2013 Control Description	Compliance (Yes/No)	Reason for Applicability/ Non-Applicability	Implementation Status
A.12.6.1	Management of technical vulnerabilities - Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	Yes	MbPT systems could be exposed to vulnerabilities whose details have been published.	Completed
A.12.6.2	Restrictions on software installation - Rules governing the installation of software by users shall be established and implemented.	Yes	MbPT systems hold critical information hence only authorized software needs to be installed and allowed.	Completed
A.12.7	Information systems audit considerations -	To minimise the impact of audit activities on operational systems.		
A.12.7.1	Information systems audit controls - Audit requirements and activities involving verification of operational systems shall be carefully Completed and agreed to minimise disruptions to business processes.	Yes	Auditing is an important aspect to understand loopholes and areas of improvement in the current setup	Completed
A.13	Communications Security			
A.13.1	Network security management	To ensure the protection of information in networks and its supporting information processing facilities.		
A.13.1.1	Network Controls – Networks shall be managed and controlled to protect information in systems and applications.	Yes	Networked environment is the integral architectural component of MbPT operations.	Completed
A.13.1.2	Security of network services - Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.	Yes	Security features, service levels, and management requirements of all network services should adhere to Service Level Agreements	Completed

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	35
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

ISO 27001 : 2013 Control	ISO 27001 : 2013 Control Description	Compliance (Yes/No)	Reason for Applicability/ Non-Applicability	Implementation Status
A.13.1.3	Segregation in Networks – Groups of information services users and information systems shall be segregated on networks	Yes	Different “VLANs” are used for different purposes to segregate the network.	Completed
A.13.2	Information Transfer	To maintain the security of information transferred within an organization and with any external entity.		
A.13.2.1	Information transfer policies and procedures - Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.	Yes	Information is transmitted through internet, physical media and phone lines/ VoIP	Completed
A.13.2.2	Agreements on information transfer- Agreements shall address the secure transfer of business information between the organization and external parties.	Yes	No confidential information owned by MbPT should be shared with external parties unless authorized.	Completed
A.13.2.3	Electronic messaging - Information involved in electronic messaging shall be appropriately protected.	Yes	Email security guidelines are documented and enforced.	Completed
A.13.2.4	Confidentiality or non-disclosure agreements- Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.	Yes	Individual NDAs are required to be prepared and signed by all the vendors, employees, third parties and stakeholders.	Completed
A.14	System acquisition, development and maintenance			
A.14.1	Security requirements of information systems	To ensure that information security is designed and implemented within development lifecycle of information systems.		
A.14.1.1	Information security requirements analysis and specification - The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.	Yes	MbPT uses proprietary and third party software applications for its data centre operations.	Completed

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	36
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

ISO 27001 : 2013 Control	ISO 27001 : 2013 Control Description	Compliance (Yes/No)	Reason for Applicability/ Non-Applicability	Implementation Status
A.14.1.2	Securing application services on public networks - Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.	Yes	The MbPT applications are not live. No public applications hosted at present.	Completed
A.14.1.3	Protecting application services transactions - Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.	Yes	The MbPT applications are not live. No public applications hosted at present.	Completed
A.14.2	Security in development and support processes	To ensure that information security is designed and implemented within the development lifecycle of information systems.		
A.14.2.1	Secure development policy - Rules for the development of software and systems shall be established and applied to developments within the organization.	Yes	The SDLC needs to be secured.	Completed
A.14.2.2	System change control procedures - Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.	Yes	Change management is an important aspect for MbPT applications which are being developed.	Completed
A.14.2.3	Technical review of applications after operating platform changes - When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.	Yes	Applicable as assistance in application development to certain user department i is an integral part of MbPT services.	Completed
A.14.2.4	Restrictions on changes to software packages - Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.	Yes	Applicable as assistance in application development to certain user department i is an integral part of MbPT services.	Completed
A.14.2.5	Secure system engineering principles - Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.	Yes	Applicable as assistance in application development to certain user department i is an integral part of MbPT services.	Completed

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	37
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

ISO 27001 : 2013 Control	ISO 27001 : 2013 Control Description	Compliance (Yes/No)	Reason for Applicability/Non-Applicability	Implementation Status
A.14.2.6	Secure development environment - Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.	Yes	Applicable as assistance in application development to certain user department i is an integral part of MbPT services.	Completed
A.14.2.7	Outsourced development - The organization shall supervise and monitor the activity of outsourced system development.	Yes	Applicable as assistance in application development to certain user department i is an integral part of MbPT services.	Completed
A.14.2.8	System security testing - Testing of security functionality shall be carried out during development.	Yes	Applicable as assistance in application development to certain user department i is an integral part of MbPT services.	Completed
A.14.2.9	System acceptance testing - Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.	Yes	Applicable as assistance in application development to certain user department i is an integral part of MbPT services..	Completed
A.14.3	Test Data	To ensure the protection of data used for testing.		
A.14.3.1	Protection of test data - Test data shall be selected carefully, protected and controlled.	Yes	Applicable as assistance in application development to certain user department i is an integral part of MbPT services.	Completed
A.15	Supplier relationships			
A.15.1	Information security in supplier relationships	To ensure protection of the organization's assets that is accessible by suppliers.		
A.15.1.1	Information security policy for supplier relationships - Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.	Yes	MbPT deals with a number of suppliers.	Completed
A.15.1.2	Addressing security within supplier agreements - All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.	Yes	MbPT deals with a number of suppliers.	Completed

ISO 27001 : 2013	ISO 27001 : 2013 Control Description	Compliance (Yes/No)	Reason for Applicability/Non-Applicability	Implementation Status
------------------	--------------------------------------	---------------------	--	-----------------------

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	38
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Control				
A.15.1.3	Information and communication technology supply chain - Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.	Yes	MbPT deals with a number of suppliers.	Completed
A.15.2	Supplier service delivery management	To maintain an agreed level of information security and service delivery in line with supplier agreements.		
A.15.2.1	Monitoring and review of supplier services - Organizations shall regularly monitor, review and audit supplier service delivery.	Yes	MbPT deals with a number of suppliers.	Completed
A.15.2.2	Managing changes to supplier services - Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.	Yes	MbPT deals with a number of suppliers.	Completed
A.16	Information Security Incident Management			
A.16.1	Management of information security incidents and improvements	To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.		
A.16.1.1	Responsibilities and procedures - Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.	Yes	Incident Management is an integral part of MbPT operations.	Completed
A.16.1.2	Reporting information security events - Information security events shall be reported through appropriate management channels as quickly as possible.	Yes	Incident Management is an integral part of MbPT operations.	Completed

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	39
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

ISO 27001 : 2013 Control	ISO 27001 : 2013 Control Description	Compliance (Yes/No)	Reason for Applicability/Non-Applicability	Implementation Status
A.16.1.3	Reporting security weaknesses - All employees, contractors and third party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services.	Yes	Incident Management is an integral part of MbPT operations.	Completed
A.16.1.4	Assessment of and decisions on information security events - Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.	Yes	Incident Management is an integral part of MbPT operations.	Completed
A.16.1.5	Response to information security incidents - Information security incidents shall be responded to in accordance with the documented procedures.	Yes	Incident Management is an integral part of MbPT operations.	Completed
A.16.1.6	Learning from information security incidents - Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.	Yes	Incident Management is an integral part of MbPT operations.	Completed
A.16.1.7	Collection of evidence - The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.	Yes	Incident Management is an integral part of MbPT operations.	Completed
A.17	Information security aspects of business continuity management			
A.17.1	Information security continuity	Information security continuity shall be embedded in the organization's business continuity management systems.		
A.17.1.1	Planning information security continuity - The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.	Yes	Applicable as Information Security is an important enabler for MbPT services.	Completed

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	40
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

ISO 27001 : 2013 Control	ISO 27001 : 2013 Control Description	Compliance (Yes/No)	Reason for Applicability/Non-Applicability	Implementation Status
A.17.1.2	Implementing information security continuity - The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.	Yes	Applicable as Information Security is an important enabler for MbPT services.	Completed
A.17.1.3	Verify, review and evaluate information security continuity - The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.	Yes	Applicable as Information Security is an important enabler for MbPT services.	Completed
A.17.2	Redundancies	To ensure availability of information processing facilities.		
A.17.2.1	Availability of information processing facilities - Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	Yes	Applicable as MbPT services are very critical.	Completed
A.18	Compliance			
A.18.1	Compliance with legal and contractual requirements	To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.		
A.18.1.1	Identification of applicable legislation and contractual requirements - All relevant legislative, statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.	Yes	Applicable as being a Government entity, MbPT is governed by IB and answerable to IB to all the applicable laws and regulations.	Completed
A.18.1.2	Intellectual Property Rights (IPR) - Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.	Yes	Applicable as being a Government entity, MbPT is governed by IB and answerable to IB to all the applicable laws and regulations.	Completed

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	41
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

ISO 27001 : 2013 Control	ISO 27001 : 2013 Control Description	Compliance (Yes/No)	Reason for Applicability/Non-Applicability	Implementation Status
A.18.1.3	Protection of records - Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislator, regulatory, contractual and business requirements.	Yes	Applicable as being a Government entity, MbPT is governed by IB and answerable IB to all the applicable laws and regulations.	Completed
A.18.1.4	Privacy and protection of personally identifiable information - Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.	Yes	Applicable as being a Government entity, MbPT is governed by IB and answerable IB to all the applicable laws and regulations.	Completed
A.18.1.5	Regulation of cryptographic controls - Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.	Yes	Applicable as being a Government entity, MbPT is governed by IB and answerable IB to all the applicable laws and regulations.	Completed
A.18.2	Information security reviews	To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.		
A.18.2.1	Independent review of information security - The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at Completed intervals or when significant changes occur.	Yes	Applicable as to understand the information security posture of MbPT.	Completed
A.18.2.2	Compliance with security policies and standards - Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.	Yes	Applicable as to understand the information security posture of MbPT.	Completed
A.18.2.3	Technical compliance review - Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.	Yes	Applicable as to understand the information security posture of MbPT.	Completed

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	42
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

ISMS control procedures

Information Security polices

Information is an asset which, like other important business assets, has a value to the organization and consequently needs to be protected. Therefore, MbPT recognizes its information assets as a significant and valuable resource. The MbPT, information security policy provides management direction and support to ensure protection of MbPT's information assets, and to allow access, use and disclosure of such information in accordance with appropriate standards and laws. The information security objectives for MbPT and its enabling functions are:

- To develop and maintain an effective ISMS consisting of an information security policy, supporting procedures and a risk assessment framework;
- To identify all assets that directly or indirectly impact the client operations, and understand their vulnerabilities and the threats through appropriate riskassessment;
- To comply with applicable laws and contractual obligations pertaining to information security and data privacy, for its clientdata and internal data; and
- To raise awareness of information security risks within MbPT and create & maintain a security-conscious culture ensuring that all breaches of information security and suspected weakness are reported, investigated and adequate actions are taken.

(Refer information Security Objectives documents for Specific Objectives)

Policy Framework

MbPT Information Security Policy is supported by ISMS Manual, detailed information security policies and procedures, implementation guidelines and templates. The information security procedures are derived from the policy statements and provide the details of necessary actions to achieve the objectives of the policy statement. The templates are derived from the detailed procedures and aim at facilitating the implementation of the Information Security Management System.

Policy Owner

The ownership and responsibility for the maintenance of this information security policy lies with the CISO. He must be contacted in the event of any questions on the contents of this policy, suggestions for improvements, specific security recommendations and any other areas relating to the security of systems, data or information of MbPT and all the enabling functions.

Policy Review and Approval

This policy document shall be reviewed at least annually by the Leadership and CISO or in events of any significant changes (i.e. change in operations, change in technology, regulatory changes, major security incidents) in the existing information security environment affecting policies and procedures. The policy owner will be responsible to make the changes to the policy document. The ISC will be responsible to approve the changes to the policy.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	43
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

All changes to the policy shall be communicated by the CISO to all employees and third party personnel through appropriate forums and channels.

Compliance

- All employees, stakeholders and third party vendors, contractors and consultants having access to MbPT information and all the supporting processes of information processing facilities shall comply with the information security policy. All violation or any attempted violation of the information security policies shall result in disciplinary action to be taken by the ISC in consultation with human resources. Disciplinary action shall be consistent with the severity of the incident, as determined by an investigation department (in accordance with MbPT Code of Conduct); and
- All violations of the information security policy must be reported to the respective Location/ Department Head (for all the supporting processes) and the CISO.

Exceptions

- Approval for exceptions or deviations from the policies, wherever warranted, will be provided only after an appropriate assessment of the risks arising out of providing the exception. This assessment will be conducted by the CISO. Exceptions will not be universal but will be agreed on a case-by-case basis, upon official request made by the asset owner. These may arise, for example, because of local circumstances, conditions or legal reason existing at any point of time. Exceptions to the Information Security Policy may have to be allowed at the time of implementation of these policies and guidelines or at the time of making any updates to this document or after implementation (ad-hoc);
- All exceptions during implementation must be submitted by CISO to the ISC; and
- For any ad-hoc exception required by a user, a request for exception must be submitted by the user through formal channels to the CISO. This request must be approved by the User Department Head / asset owner.

Inquiries

Any inquiries relating to policy or the application of this policy shall be referred to the CISO.

Management direction for information security

The management constituting of CISO, SC and ISC, shall be accountable for enforcing the implementation of MbPT information security policy. The location/ function heads along with the Information Security Management Representatives shall be responsible for managing the overall information security for MbPT. All employees shall read, understand and adhere to MbPT Information security policy. The information security policy for MbPT shall be reviewed at least once in a year and at a time of any major change(s) in the existing environment affecting the policies and procedures. The review shall be carried out for assessing the following:

- Impact on the risk profile due to, but not limited to, the changes in information assets, deployed technology/ architecture and/ or legal requirements, emerging threat landscape; and
- Effectiveness in policies

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	44
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Organization of information security

Internal Organization

The information security roles and responsibilities shall be defined and assigned at all levels ensuring that the individuals understand them. The duties and areas of responsibilities of employees shall be segregated and records of the same shall be maintained to reduce the opportunities for unauthorized or unintentional modification or misuse of the information assets. In cases segregation of duties is not possible; approval of the Functional Head shall be obtained prior to allocating responsibilities to the employee. Also, appropriate compensatory controls such as monitoring of activities, audit trails, management supervision and independent reviews shall be implemented. All processes must adopt the principle of segregation of duties to the maximum extent possible. The initiation of an event must be separated from its authorization. The following principles must be followed:

- Persons involved in operational functions must not be given additional responsibilities in system administration processes and vice versa;
- Persons involved in testing processes must not be given additional responsibilities in system administration processes and vice versa;
- The responsibility for performing a security review of the system or process shall be completely independent from the roles and responsibilities for developing, maintaining, and using the system or process; and
- Where segregation of duties is not possible or practical, the process must include compensating controls – such as monitoring of activities, maintenance and review of audit trails and management supervision.

Contacts with law enforcement authorities, fire department, emergency services and service providers shall be maintained by the facility and security department. The contact details of these agencies should be maintained and displayed at appropriate places that are accessible to users.

The CISO shall maintain appropriate contact with special interest groups and authorized information security and data privacy forums for receiving and distributing updates on new vulnerabilities, security and continuity threats, regulations and/ or risks.

Contacts with special interest groups (such as CERT-In, NIC, CISE, etc.) shall be maintained.

Project management shall be aligned to the information security requirements of MbPT. Development and testing teams shall inform ISC/ CISO about the nature and requirements of the new projects.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	45
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Mobile Device and Work from Home

A formal process shall be developed and established to safeguard and prevent leakage of information through mobile devices such as laptops, smartphones etc. It shall include, but not limited to the following:

- Latest virus definitions shall be regularly updated on the mobile devices and laptops to prevent the corruption of information stored on these devices;
- If the user of the mobile device has access to confidential information, access shall be protected via the user authentication (e.g., user ID and password) and inactive session timeout controls, if applicable;
- Mobile devices are easy to spot and are prime targets for theft. It shall be the employee's responsibility to ensure every effort at their disposal is taken to protect MbPT's mobile devices; and
- Training sessions shall be conducted for the employees, using mobile computing, to increase their awareness on the additional risks resulting from this way of working and precaution that needs to be taken while using the device.

Work from Home requests shall be handled in accordance with the approved procedures. Adequate Work from Home security measures shall be established and implemented.

Segregation of duties

- Duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets;
- Care should be taken that no single person can access, modify or use assets without authorization or detection;
- The following principles will be followed:
 - Persons involved in operational functions should not be given additional responsibilities in system administration processes and vice versa;
 - Persons involved in testing processes should not be given additional responsibilities in system administration processes and vice versa; and
 - The responsibility for performing a security review of the system or process should be completely independent from the roles and responsibilities for developing, maintaining, and using the system or process.
- Whenever it is difficult to segregate duties, additional controls such as monitoring of activities, audit trails and management supervision should be considered

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	46
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Role	Responsibilities
Information Security Steering Committee	Approve the information security policy during its initial documentation and when it is amended; and Establish ISMS objectives and plans. Ensure implementation of information security on an on-going basis; and Coordinate review and approval of ISMS deliverables as per the defined frequency.
CISO	Monitoring security of MbPT's network and ensuring the smooth functioning. Other responsibilities include:
Network Administrators	Installing network Components; and Maintaining network during normal operations and during breakdown.
Server Admin	Monitoring the security and availability of the servers and storage infrastructure and maintaining server infrastructure during normal operations and during breakdown.
Information Security Management Representatives	Ensuring the compliance of Security procedures by their department employees and violation control.

Contact with authorities

The objective of this guideline is to ensure that MbPT maintains appropriate contact with special interest groups and authorized information security forums for receiving and distributing the updates on new vulnerabilities, security threats, regulations and/ or risks pertaining to its business. CISO at MbPT will be responsible for ensuring contacts with Special Interest Groups are maintained in the interest of MbPT's security posture.

The ISC is responsible to maintain the contact with authorities like police department, ambulance service, fire-fighting stations, hospitals etc.

The CISO shall maintain contacts with the following special interest groups, but not limited to:

- **Special Security Forums:** These forums enhance security of Communications and Information Infrastructure through proactive action and effective collaboration with other security bodies. These forum issue security guidelines, advisories, share information relating to latest changes in information security. These forums help in reporting local problems.e.g.cert-in.org;
- **Security Advisories:** Security advisories provide objective, timely and comprehensive information about security threats and vulnerabilities. An example could be certain security advisory websites like securityfocus.com, secunia.com;
- **Network System Updates:** Vendor/ suppliers for information/ technical assets should be contacted for hardware and software updates, patch updating, latest vulnerabilities;

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	47
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

- Application Vendor/ suppliers: Contacts with vendor/ suppliers for application used within MbPT environment should be maintained to ensure latest threats and vulnerabilities applicable to these applications are addressed; and
- Other institutions which can help in solving security issues (CERT-IN, Cyber security Cells of Maharashtra Police)

Contact with special interest groups

CISO shall be associated with the above companies/ institutions with an objective to:

- get updates on new vulnerabilities, security threats, regulations pertaining to telecom industry;
- improve knowledge and keep up-to-date with relevant security information;
- ensure the understanding of the information security environment is current and complete;
- receive early warnings of alerts, advisories, and patches pertaining to attacks and vulnerabilities;
- gain access to specialist information security advice; and
- Share and exchange information about new technologies, products, threats, or vulnerabilities.

Information security in project management

- Information security objectives will be included in project objectives;
- Information security risk assessment will be conducted at an early stage of the project to identify the required controls; and
- Information security controls will be applied in all phases of the project.

Mobile and teleworking

Mobile device policy

- When traveling (in cars, hotels, conference and meeting rooms, public places) an employee shall take reasonable precautions to protect his laptop as much as possible from damage, theft, and eavesdropping. If left unguarded, the laptop should be concealed as far as possible (e.g. locked in the boot of the car). Normally an unattended laptop should be in shutdown mode; an unattended laptop should never be accessible without password protection.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	48
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

- The loss of a laptop/mobile device should be reported to Location Head immediately.
- All MbPT employees must connect their laptops to the MbPT internal network at least once a week so that the specified security patches and Antivirus definitions can be updated. If this is not feasible in a particular case, the employee should at any rate ensure that the virus definition files are updated at least once a week.
- An employee may not make any alterations which circumvent the MbPT security mechanisms for his/her laptop. Apart from disciplinary measures, the employee may also be charged with the costs incurred by MbPT if the laptop is damaged through unacceptable manipulation. Unacceptable manipulation includes, for example,
 - Autonomous set-up of unauthorized Internet connections
 - Switching off virus scanner, particularly with an open connection to the Internet
 - Misuse of privileges granted to enable certain business functions
 - Retrieval of E-Mails from employee's public mailboxes.
- User should be responsible for maintaining the confidentiality, integrity and availability of the information on their mobile computing device.
- IT team will ensure that Users don't have rights to install any software in the laptops given to them. In case of a business requirement, users shall take approvals from the department head and get in touch with the location IT representative.
- IT team shall ensure all Laptops/handheld devices have Antivirus installed on them.

Teleworking

- A secure communication channel is established between the teleworkers and the networks of MbPT;
- Use of appropriate authentication mechanism for authenticating those using the teleworking solutions; and
- Revocation of authority, access rights and return of equipment when the Teleworking activity ceases or when the employee exits from MbPT.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	49
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Human resources security

Including Information Security in job responsibilities

- Prepare a document identifying the various roles in the organization; these roles should include contractors and third party users.
- Chart out the responsibilities associated with each role including Information Security responsibilities of the employees. The information security responsibilities should include but not limit to:
 - Implementing and maintaining the Human Resources Security Policy and Procedure document.
 - Protecting identified assets.
 - Logging activities for certain critical procedures,
 - Adhering to MbPT Information Security Policies and Procedures.
 - Report security events or potential events or other security risks to MbPT.
- Share this with all the employees
- Provide a mechanism to address employees concerns and issues related to his/ her job responsibilities.
- Ensure that all employees, contractors and third party vendor/ suppliers have access to the Information Security Policies and Procedures. Also, an undertaking should be taken to ensure that they have read the Information Security Policies and Procedures and agree to abide by them.

Personnel screening

- For MbPT Employees:
 - The screening and verification process is carried out as per the Government of India guidelines.
- For Third Party/ vendor/ suppliers/ outsourced personnel:
 - The tender document/ master service agreement as drafted by MbPT should contain the clauses for background verification including the following –
 - Educational background checks
 - Police verification / Criminal checks
 - Work experience and skill-set checks

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	50
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Confidentiality agreements

- Confidentiality agreements should be signed with employees along with the appointment letter.
- Prepare standard confidentiality agreements for the employees.
- Confidentiality agreements are to be given to the employee at the time of joining; the Confidentiality agreement to be signed by the employee and returned to the HR at the time of joining.
- All users are required to affirm their obligations by signing non-disclosure agreement. Confidentiality agreements should be reviewed when there are changes to the roles and responsibilities of employees that may occur due to promotion, transfer to another department, etc. **(Refer: L3 – Human Resource Security - MbPT Non-Disclosure Undertaking)**

Terms and Conditions of employment

- For MbPT employees:
 - The terms and conditions of employment as laid by the Government of India is applicable.
- For Third Party/ vendor/ suppliers/ outsourced personnel:
 - The employee's legal and information security related responsibilities like copyright laws or data protection legislations.
 - Responsibilities for the classification of information and management of organizational assets associated with information systems and services.
 - Responsibilities for handling of the information received from other companies or external parties.
 - The extent and duration of the responsibilities.
 - An indication of management action in case the terms of employment is violated.
 - The employees, contractors and third party users agree to terms and conditions concerning information security appropriate to the nature and extent of access they will have to the organization's assets associated with information systems and services.

Training and Awareness procedures

- The methods of training covered in this procedural document include classroom training, training manuals, web-based training, certification exams, on-the-job training, and in-house training.

Training Requirement Review

- Human Resources and the Department Heads need to identify all the requirements of Information Security training for the employees within each of the departments.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	51
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

- The review would involve inputs from the Department Heads including:
 - The training curriculum and plans
 - Approvals / rejections of training plans
 - Prioritization of trainings, allocation of resources, preparation/updating of training calendar
- The training needs are to be identified on the basis of the following:
 - Strategic Information Security trainings based on organizations business objectives.
 - Internal Audits/ Inspection.
 - External Audits/ Inspection
 - Information Security process improvements initiatives etc.
- All the identified trainings should be reviewed by HR on the basis of cost, time, availability of resources, priority of training etc. All the selected trainings should be used as input for preparation of a training calendar.
- Training records should be maintained for the audit trails.

Training calendar for the year

- The Annual training calendar should be discussed and finalized by the HR/ Training team / CISO and the Department Heads at the start of the year. Whenever required, the HR/Department Heads can further review and enhance the calendar. Annual training calendar should be individually conveyed to the employees.
- The training calendar can be prepared as per the following guidelines:
 - Training calendar for operations personnel
 - Identify the key Information Security areas.
 - Based on the identified key Information Security area, identify the skills required for achieving the security initiatives.
 - Identify the personnel required to carry out the Information Security operations.
 - Identify the skills available with these personnel.
 - Perform a gap analysis between the existing skills and required skills and arrive at the training requirements.
 - Identify the personnel available within the organization with the required skills for executing the training.
 - Identify personnel / organizations that will provide training for skills that are not available within the organization (including external training programs)
 - Draft the training calendar based on the training requirements and the trainers availabilities.
 - Roll-out the training calendar during April every year.
 - Training calendar for top/senior/middle management personnel

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	52
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

- Identify the key Information Security initiatives for the next year
- Identify the personnel in top, senior and middle management functions
- Design the training programs based on the initiatives set out for each management function
- Identify external consultants that can provide the adequate training to the personnel
- Chart out a calendar based on the availability of training personnel.

Non-planned training requirements

- For any non-planned training requirements, specific approvals should be obtained from the Department Heads.
- Training records should be maintained for an audit trail.

Operational continuity

- For each key/vital Information Security function, an additional staff member needs to be trained to ensure continuity of operations of the organization. Also consider providing cross training to different personnel

within the operations team in order to continue operations due to shortage of staff. These need to be identified and factored into the training requirements of the staff.

On-the-job training (OJT) program

- Apart from classroom training sessions, MbPT should institutionalize an OJT program. The objective of this program should be to impart critical skills to its staff, enabled by planned deployment on specific areas of operation or specific projects for a specific duration. Time spent on this program should not be treated as a part of the minimum training requirements of the employee.

Knowledge Management (KM)

- MbPT should ensure that the Information Security knowledge gained by the employees is converted into Knowledge Objects that can be shared effectively among employees.
- Care should be taken that the Knowledge Objects are sanitized prior to being shared, to ensure that confidential and proprietary information is masked to prevent disclosure.
- MbPT should consider implementing a simple but effective KM solution to take care of such requirements. This could be implemented through the intranet site of the organization.

Awareness programs

- MbPT should hold awareness programs for its employees on a periodic basis. These programs should be designed to spread awareness among its employees regarding a particular subject.
- Training and awareness sessions should be conducted for the employees to make them aware of the security related incidents, their reporting, their initial resolutions and escalations.
- Awareness programs should be conducted by an internal faculty or in exceptional cases by an external party. All awareness programs and its associated costs should be approved in advance by the CISO.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	53
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Disciplinary process

Refer: L2 - User Policies and Procedures

Termination/ Transfer

- Employee is responsible for getting his clearance before termination or transfer.
- The clearance procedure, for an employee leaving MbPT or getting transferred to some other location within MbPT, will include clearance from the Department Heads. (**Refer:** L3 – Access Control - Revocation of Access rights)
- The Department Head of the employee is responsible to assign a team member for taking a backup of the employee's machine.
- The ISC should ensure that the following activities are performed:
 - Revoking employee's authorization without undue delay (within 48 hrs.) after his last working day.
 - Receiving laptops, access cards, hard disks, badges etc.
 - Revoking all access permissions to critical/ sensitive areas, network switch room, and classified areas.
 - Collecting all hardware, software and information.
- All employees of the organization and, where relevant, third party users, should receive appropriate training and regular updates in organizational policies and procedures. This includes security requirements, legal responsibilities and business controls, as well as training in the correct use of information processing facilities
e.g. log-on procedure, use of software packages, before access to information or services is granted. ISC is encouraged to provide additional security awareness measures, for example the provision of specific Intranet pages on security, or security awareness training (with preference done as part of the standard induction program that might be provided to users).
- There should be a formal disciplinary process for employees who have violated organizational security policies and procedures. Such a process can act as a deterrent to employees who might otherwise be inclined to disregard security procedures. Additionally, it should ensure correct, fair treatment for employees who are suspected of committing serious or persistent breaches of security.
- Usually, the Department Heads are responsible for handling the disciplinary process.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	54
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Asset management

Responsibility for assets

Inventory of assets

Asset: Asset is defined as “anything of value to MbPT”. In the realm of information, asset can range from data files to physical assets like removable media, servers, and desktops, software, hardware, services, people, vendor/ supplier, etc.

- **Physical Assets (IT/ NON IT Assets):** these includes Application Servers, DB Servers, Gateway Servers, Switches, and Routers, infra / Facility equipment's like UPS, Battery banks, Chillers, AC's, Fire alarm systems, CCTV, VESDA, AHU, HT Panel, Transformers and Site, Passive and Active network devices etc.
- **Software Assets:** This would include Application software, System software, Development tools & Utilities etc.
- **Information Assets:** these include data, SOP, SLA, reports, system requirement specifications, DB design documents, daily checklists, critical logs, dialog diagrams etc.
- **Services:** This would include general utility services such as Power, Lighting, Air Conditioning and in- house or external services etc.
- **Paper Assets:** Information in physical hard copy form, which is used / required / generated during the course of operations, and is used to manage business processes. E.g. Bill of material, Contracts, Agreements, Invoices, Manuals.
- **People Assets:** This would include personnel required to support and run other assets
- **Site:** This would include the building of operation for the organization.

All functions shall identify and document all the information assets related to their processes and function in the Information Asset Register. The information asset register shall contain, at a minimum, the following information about each of the assets:

- The type and location of asset;
- Name of the function that uses this asset;
- The Asset Owner, Custodian and User;
- The classification of the asset;
- The Confidentiality, Integrity and Availability (CIA) ratings of the information asset; and
- The overall criticality rating for each of the identified information asset.

Ownership of assets

- Information Security Management Representatives in conjunction with the department head is responsible to identify all the assets in their respective departments.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	55
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

- The department head will identify and allocate the responsibility of ownership and custodianship of the asset
- The asset owner is defined a person or group of people who have been identified by management as having responsibility for the determining and maintenance of the Confidentiality, Integrity and Availability of that asset. The asset owner may change during the lifecycle of the asset.
 - Asset owner is responsible for determining the Asset's classification and how / by whom the asset can be used/ accessed and what security controls shall be applied on the asset
 - Asset owner shall ensure that appropriate controls are implemented by Asset Custodian
 - Asset custodians are people, teams, or departments responsible for implementing the authorized controls for information assets based on the classification level. Based on the Asset owner's requirements and MbPT's ISMS policies the custodian will take the necessary actions to secure the information, applying safeguards appropriate to the information's classification level.
 - Asset Custodian is responsible for day-to-day operations and maintenance of assets. Asset Custodian shall:
 - Ensure that appropriate level of physical security is provided to the assets
 - Ensure that assets are labelled as per Information Labelling and Handling Guidelines
- The Department head in consultation with the asset owner shall classify all the departmental assets in- terms of the asset classification levels (i.e. restricted, confidential, internal only, public) and confidentiality, availability and integrity requirements of the asset.
- The respective department information Security Management Representatives will verify and approve the information asset register once it is created.

The Asset registers will be reviewed on a yearly basis or when there is a significant change.

Acceptable use of assets

Refer : ISMS L2 user policy/procedures

Assets handling as per Asset classification

Hard Copy Assets

Asset / handling	Restrictive	Confidential	Internal only
Creation	-Copies to be named (recipients marked)	Copies to be controlled	As exists
Transmission	-Till extended possible should be personally carried.	Should go through internal or specified courier only	As exists

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	56
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

	-If not possible, then Sealed envelope (Tamper proof envelope or signature across the openings)		
	-Ensure the confirmation from the recipient		
Storage	-Lockable Fireproof cabinets	Lockable Cabinets	As exists
Duplication	-To be personally monitored	Done by authorized personnel	As exists
Destruction	-To be shredded personally	Can be put in lockable bins	As exists

Soft Copy Assets

Asset / Stage of Asset	Restricted	Confidential	Internal only
Creation	- No extra copies to be made	- Copies to be controlled	As exists
Transmission	- Encryption to be used.	- Encryption to be used	As exists
	- No pen Drives / External Removable Hard disk to be used / Encrypted pen drives	Password protection - No pen Drives to be used / Encrypted pen drives to be used	
Storage	- Within encrypted drive / Password Protection/ access restrictions - No pen Drives to be used / Encrypted pen drives	- Within access control folder / Password Protection	As exists
Availability	- Till extent possible store on server	- Till extent possible store on server or the allocated space	As exists
Destruction	- Shift+Delete, Spring cleaning to be carried out once in six months	- Shift+Delete, Spring cleaning to be carried out once in six months	As exists

Return of assets

- The IT and HR function ensured that at the time of termination/ change of employment or change in the responsibilities or transfer of employee, all the assets belonging to MbPT are returned by the employee

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	57
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

- All employees shall return information assets that were issued to them during their tenure in MbPT; and
- Relevant Functional Heads dealing with the third party employees shall ensure that at the completion of the assignment in MbPT or change in the responsibilities, third party employees return assets allocated to them such as corporate documents, equipment, mobile devices, software, access cards and/ or any other asset that is the property of MbPT.

Information Classification

Classification of Information

- Every asset has different degrees of sensitivity and criticality to the business. The following asset classification categories shall be used to define an appropriate level of protection or special handling. The classification of the information will be consistent with the business requirement of the Organization.
- Employees, third party staff, vendor/ suppliers, consultants etc. are required to classify the information that they create for MbPT as per the following classifications:-
 - **Restricted:** Restricted information is characterized as sensitive information that is intended for a very limited group of individuals who should be specified by name. This level contains information, which if disclosed to unintended audience (including internal or public disclosure) would provide access to business secrets and could jeopardize important interests or actions of MbPT or its

clients and would be to the serious personal or financial detriment if revealed to unauthorized persons.

For Example: Unaudited financial data, Business plans etc.

- **Confidential:** Information whose unauthorized disclosure, compromise or destruction would directly or indirectly have an adverse impact on MbPT, its customers or employees. Confidential information may be shared with parties who have a relationship with MbPT, if they have signed a non-disclosure agreement, and have a need to know. Sharing with internal MbPT employee should be done based on business need and approvals from asset owner
Example: Organization Risk Register, VA/PT Reports etc.
- **Internal Only:** This classification applies to information that is specifically meant for employees of MbPT. While its unauthorized disclosure is against policy, it is not expected to seriously or adversely impact the business, employees, and customer, stockholders and / or business partners. Example: ISMS policy documents, HR policies etc. All un-labelled assets shall be treated as Internal only.
 - **Public:** Information that can be disclosed to anyone is termed as public. It would not violate an individual's rights to privacy. This classification applies to information, which has been explicitly approved by MbPT management for release to the public. Example: Annual Financial Reports, Press release

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	58
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Labeling of information

Handling of assets

Usage	Confidential/ Restricted	Internal	Public
Labeling	Marked as "Confidential/ Restricted" on cover page; Labeling Position: At the top/ bottom of each page; All pages shall be numbered (e.g., 1, 2, 3) to ensure that no page is missing; Document shall carry name of owner; and Date of creation	Marked as "Internal" on cover page; Labeling Position: At the top/ bottom of at least the cover page; All pages shall be numbered to ensure that no page is missing; and Date of creation	Marked as "General Business" on at least the Cover page; Labeling Position: At the top/ bottom of at least the cover page; All pages shall be numbered to ensure that no page is missing; Document shall carry name of MbPT on cover page; and Date of creation
Duplication	Mandatory to have a distribution list for sharing in softcopy/ hardcopy	Duplication for business purposes only	No special requirements
Mailing of Information	Mailing allowed with permission of owner using secure email channel; Restricted/ Confidential marking on cover sheet; and Confirmation of receipt at discretion of information owner	Mailing requirements determined by information owner	No special requirements

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	59
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Usage	Confidential/ Restricted	Internal	Public
Disposal	Owner shall observe physical destruction beyond ability to recover	Controlled physical destruction	No special requirements
Storage	Locked up when not in use; and Master copy secured against destruction	Master copy secured against destruction	No special requirements
Distribution/ Read Access	Owner establishes user access rules, generally highly restricted	Owner establishes user access rules	No special requirements, generally available within and outside company
Reclassification Review	Information owner to establish specific review date	Information owner to review at least annually	No special requirements

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	60
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Media Handling

Management of removable media

- MbPT does not make use of any removable media;
- There is a restricted item list pasted at all entry points;
- Security team will allow carry out media once they receive the approval email;
- Any user having access to customer information is not allowed to Printing rights;
- All media should be stored in a safe, secure environment to ensure the Confidentiality, integrity and availability of the media and the information, and to maintain it in accordance with the manufacturers' specifications;
- All media should be handled with care and it will be ensured that it is not kept near strong magnetic material and not exposed to extreme heat or pollution;
- Documents will be labeled appropriately. This is for the user to ensure that
 - Storage of the document is commensurate with the labelling;
 - Associates handling the document will ensure that no authorized user gains access to the document at any time;
 - Any unlabeled document is considered Internal only; and
 - If no longer required, the previous content of any re-usable media will be deleted in

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	61
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Accordance with the information classification.

Disposal of media

Media shall be disposed of securely when no longer required, using Organizations formal procedures.

Physical media transfer

- In case of media in transit, following procedures should be followed:
- Reliable transport or couriers should be used.
- Packaging should be adequate to protect the contents from any physical damage likely to arise during transit and in accordance with manufacturers' specifications; and should be clearly marked and labelled before transporting.
- Special controls should be adopted, where necessary, to protect sensitive information from unauthorized disclosure or modification e.g. use of locked containers, tamper-evident packaging (which reveals any attempt to gain access) and confidentiality encryption.
- It's the responsibility of all employees at MbPT to protect the Information (ensure its C, I, A) as per the classification.
- All media will be handled and labelled as per their classification. Any unlabelled media or information shall be treated as "internal only".

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	62
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Access control

Business Requirement of Access Control

Access Control Policy

An access control matrix has been documented, implemented and reviewed to protect information assets against unauthorized access. It takes into account the security requirements of business applications and segregation of access control roles.

Access to Networks and Network Services

- Appropriate interfaces will be created to segregate MbPT networks from the networks owned by other organizations and public networks, wherever applicable;
- Appropriate authentication mechanisms is applied for users and information systems;
- Control of the user access to information services is enforced;
- Users are provided access only to the services that they are specifically authorized to use;
- Matrix for providing access based on role of an individual user is in place and is being implemented; and
- Approval matrix for approving the access and Access Repository Matrix are in place and are being implemented.

User Access Management

User registration and de-registration

- Once the employee resigns, supervisor sends an intimation email to MbPT HR, Security, and MbPT MbPT;
- MbPT HR will initiate the process for all login id deletion with effect from last working day;
- Security team will deactivate the access card effective given date;
- In case of JA (Job Abandonment). Uninformed absence for two working days, supervisor will send an intimation email to MbPT HR;
- MbPT HR initiates JA process. At the end of the process termination letter is sent to the employee. ID deactivation process is initiated in PeopleSoft, similar to resignation;
- MbPT HR will also intimate security and MbPT. Security team will further deactivate his access control;
- ID administration team will deactivate all ids granted, post end of last working day.
- Once a member of MbPT, MbPT team process resigns all his special privileges are revoked, and record maintained; and

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	63
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

- MbPT Operations manager maintains list of associates (both insource and outsource) with special access privileges. This list is updated once:
 - any user resigns;
 - new user joins in;
 - Role change;
 - Respective leads (Server, network, Voice) are responsible for the updating of this list;
 - Special access privilege includes;
 - Rights on network equipment;
 - Voice infrastructure;
 - Local server admin;
 - Desktop admin;
 - Printer access; and
 - Read/write access on share drive.

User access provisioning

- Every user requiring logical access to MbPT information systems should complete requisition form for Creation of New User Account (Refer: L3 – Access Control - New Account Request Form) and forward it to system administrator for operating system and email access/internet or network administrator for access to network devices and services or application administration for application and database access after approval and authorization.
- Respective Department Heads should approve new user accounts in Operating systems, applications, and database.
- For third party users (consultants, auditors, vendor/ suppliers, etc.) concerned department head should approve and ISC should authorize.
- The approval and authorization should be given after analyzing whether the access rights requested by the user are the minimum required to perform his/ her duties. Respective Job-Function matrices should be referred for this purpose.
- Administrators should verify the completeness of the form, approval and authorization before creating the user accounts.
- System Administrators and Application Administrators should maintain list of user credentials (Operating Systems, Applications, Databases, etc.) along with full name, designation and contact information of the user. Network administrators should maintain user credentials for network equipment and other network services. They should update the list when a user account is created, modified and deleted.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	64
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

- Common user IDs should not be issued to multiple users when it is technically feasible to provide individual IDs. In situations where a common ID is required, specific permission and authorization should be taken from the CISO and ISC, detailing the reason and users who have been granted the right to use this ID and password. ISC should review the usage based on register for the individual businesses and audit logs at least on a monthly basis, if not more frequently in case of shared/ common privileged accounts.
- For contract employees and consultants, a user account having expiration date, which coincides with the conclusion of the contracted project, should be created; else care should be taken by the system administrator to disable the account on the expiry date. In case the ID is still required, the account should be kept active after seeking an approval from Department Head.

Management of privileged access rights

Privilege – Job function Matrix

- System administrators, Network Administrators, Application administrators along with the Department Heads should identify all the privileges associated with all Operating System, Business applications, Databases and Network elements used within individual businesses.
- These privileges should then be mapped with the job functions of the personnel involved in MbPT's operations to develop and document Privilege – Job Function Matrix. In most applications, operating systems and databases privileges required for performing a job function are put together to create an application role for effective and secure management of access privileges. Wherever applicable, application roles should be created for each of the corresponding job function in the business.
- The respective Team Lead should review the Privilege – Job Function Matrix annually.
- This exercise should be carried out whenever an Application or Operating System or a Database or network equipment is to be used for the firsttime.
- Privilege – Job function Matrix should be modified by the Department Head in the following scenarios:
 - When an Application, Operating System, Database or network equipment undergoes a major change or new module or functionality is added.
 - A new job function or role is created
 - Job Function or Role is changed.
- Privilege – Job Function Matrix should be approved by CISO before implementation.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	65
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Granting Privileges

- Privileges are granted to users on two occasions. One is during the creation of user account and when a user requests for additional privileges due to changes in job function or changes in responsibilities. Users assigned high privileges for special purposes should be required to use a different user identity for normal business use (e.g. “System Administrator” login is not to be used for running the application).
- When a new user is created, the privileges should be granted as per the request after verifying the approval and authorization
- If a user requires additional access rights, then he should fill the Additional Access Request Form (**Refer: L3** – Access Control - Additional Access Request Form) and forward to Department Head for approval.
- Department Heads should review the business need and then approve and forward to ISC/ CISO for authorization before the access right is given to the users. Department Heads should ensure that the additional access rights are absolutely required for performing his job functions.
- Any access that is not explicitly authorized is forbidden.

Review of Privileges

- While the Department Heads should review the access granted to his/her department personnel on a half yearly basis, the ISC should review the List of Users in various information systems along with their access privileges on an annual basis. She/he should verify in the information systems whether the privileges granted to the user is as per what is approved and documented.
- The Department Head who approved the additional access/privilege should ensure that the same is revoked when the business purpose of the access ceases to exist.
- Department Head should verify whether the privileges are granted removed when the expiry date of them is over.
- Department Head should also check whether any additional privileges are obtained in an unauthorized manner and report any deviations to the ISC.
- Privilege allocations are to be checked by Department Head at regular intervals to ensure that unauthorized privileges have not been accidentally granted to anyone.
- Review of Access Control List of the network shares for servers should be done by Department Head on half yearly basis and exceptions shared with the ISC.
- System Administrator should set appropriate access controls on all necessary file shares.
- All users of the information systems will be responsible for taking due care in the use and operation of the information systems through their user ID. Users will be held responsible for any activity carried out through their User IDs.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	66
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Management of secret authentication information of users

Allocation of secret authentication information shall be controlled through the following:

- Users shall be forced to change their own secret authentication information on first use;
- Identity of the user shall be verified prior to providing replacement or temporary secret authentication information and an acknowledgement shall be obtained from the user via separate mode of communication;
- Temporary secret authentication information shall be given to the users in a secure manner avoiding the use of external parties or unprotected (clear text) email messages;
- Secret authentication information shall be unique for an individual;
- Default vendor/ supplier secret authentication information shall be altered following installation of systems or software.

Review of user access rights

The MbPT has multiple user access levels and change from one category to another is often required. The same is regularly reviewed to ensure the user has only the required rights.

Removal or adjustment of access rights

- The Department Head of the resigned or terminated employee should immediately notify CISO and the HR Function. Admins should revoke the access of terminated/ resigned employee based on the HR Clearance Form.
- In case of transferred employee or employee who would be changing roles, the Department Head should immediately notify the CISO and HR Function (Refer: L3 – Access Control - Revocation of Access Rights Form) Department Head should approve the removal of accounts or revocation of access rights of the concerned employee.
- Administrators should ensure that the user-Id is revoked upon termination or resignation of employees and revoked or access modified upon change of responsibilities. Department Head should review to ensure that the user credentials are removed or access rights are revoked on the last working day of the terminated employee.
- In case where a common user account is used or the resigned employee's user account needs to be maintained for auditing purposes or if the application does not permit to remove the user account, then passwords of these accounts should be changed on the last working day of the employee.
- The Department Head should ensure that all the responsibilities are transferred to another individual.
- The Department Head should also monitor the activities of the resigned/ terminated employee from the moment he resigns.
- The HR function should ensure that all company assets with the employee such as PCs, keys, ID cards, proximity cards, software, data, documentation, manuals etc. of terminated employees should be returned to the employee's Department Head or the Human Resource Department.
- Above procedures should be followed for involuntary termination of the employees.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	67
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

User Responsibilities

- Users are responsible for following the organizations password policy and procedure;
- Users are responsible to keep their password confidential and avoid writing of passwords on paper unless there is a business need for the same and in such a case controls must be implemented to ensure that the passwords are stored securely;
- Users are responsible for changing the passwords whenever there is any indication of possible system or password compromise or the password is nearing expiration;
- Users will not leave their system unattended while logged on. They shall lock the system
- Users will keep their work area clean and ensure that there are no confidential or restricted information attended on their desk or printers or fax machines or photocopiers. All confidential or restricted information shall be locked in secure cabinets at all times.

Use of Secret Authentication Information

- User identification and authentication shall be performed using the active directory. Authentication controls shall be built into all information systems; and

System and Application Access Control

Information Access Restriction

- Access to information and application systems shall be on “need-to-know” basis and in accordance with this policy;
- System administrator or the person performing the equivalent role shall be required to maintain the updated access control matrix with privileges assigned to the users; and
- Function/ Location Head shall review the access rights at regular intervals.

Secure Log-on Procedures

The operating systems of servers, workstations and/ or network devices shall be controlled through a secure log-on like:

- Not display system or application identifiers until the log-on process has been successfully completed;
- Display a general notice warning that the computer should only be accessed by authorized users;
- Not provide help messages during the log-on procedure that would aid an unauthorized user;
- Raise a security event if a potential attempted or successful breach of log-on controls is detected;
- Not display a password being entered;
- Not transmit passwords in clear text over a network;

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	68
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

- Display date and time of the previous successful log-on and details of any unsuccessful log-on attempts since the last successful log-on on completion of a successful log-on; and
- Restrict connection times to provide additional security for high-risk applications and reduce the window of opportunity for unauthorized access.

The log-on procedure shall not disclose any information of the system. The remote log-on shall be designed with consideration of encryption of information during its transmission. A secure network channel shall be established for the remote access.

Password Management System

- Password Parameters in Operating System, Applications, Databases and network equipment should be configured as per password management policies detailed in Information Security Policy – Access Control Policies. Wherever password policies cannot be configured due to certain limitations, the same should be documented and authorized by the Security Management Representatives.

Use of Privileged Utility Programs

- Any use of utility programs that could override the system and application controls shall be restricted and strongly controlled. Only utilities authorized for the remote management of the servers, workstations and network devices shall be used;
- It shall be ensured that vendor/ supplier default utilities are disabled during new server or network device commissioning; and
- If for troubleshooting purpose there is a need to use these utilities, administrators of the servers and network devices shall ensure that such utilities are enabled for an authorized activity after approval from IT Head and are disabled immediately after the use. They shall ensure that activities carried out by using such utilities are logged and are approved prior to the use.

Access Control to Program Source Code

- Access to the program source code of operational systems are strictly controlled to prevent any corruption of the application programs;
- Support personnel from MbPT don not have access to program source code; and
- All updates or issue of the program sources to developers is carried out through an authorized request.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	69
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Cryptographic controls

Policy on the use of cryptographic controls and Key Management

Determination of Encryption Requirements

- a. The ISC should develop MbPT's Encryption Strategy defining:
 - ▶ The classes of sensitive data/ information (e.g. Confidential and Internal) that require encryption (Refer: Information Classification Guideline).
 - ▶ The conditions under which encryption is required, i.e. the 'Confidentiality' and/or 'Integrity' ratings for data in transit or storage (e.g. for data stored within MbPT, for data shared within MbPT, for data shared with external parties, for data residing on storage media accessed by third parties, for data flowing over third party networks, etc.)
 - ▶ Requirements for ensuring authenticity and message integrity in applications.
 - ▶ The level of protection required for different types of information, based upon inputs from Risk Assessment (Refer: MbPT ISMS – L1– Risk Management Policy and Procedure).
- b. Based upon the Encryption Strategy, ISC should determine:
 - ▶ Strength of encryption algorithm(s) required
 - ▶ Intended users of encryption algorithm(s)
 - ▶ The required period of encryption, i.e. duration for which the data needs to be encrypted
 - ▶ Potential system overhead/ performance issues.
- c. ISC should also identify the encryption requirements related to:
 - ▶ Amount of data to be encrypted, i.e. the volume of information
 - ▶ Areas of existence of sensitive information (during storage/ transmission)
 - ▶ The number and/or type of transactions requiring encryption
 - ▶ Ease of usage considerations.
- d. Information Security Management Representatives should determine applicable laws, regulations and contractual requirements, if any, for data encryption. The laws to be considered should include the following, if applicable:
 - ▶ Restrictions on import and/or export of computer hardware and software for performing cryptographic functions
 - ▶ Restrictions on import and/or export of computer hardware and software which is designed

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	70
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

to have cryptographic functions added to it

- Restrictions on the usage of encryption
- Mandatory or discretionary methods of access by the government authorities to information encrypted by hardware or software to provide confidentiality of content.

Product Selection

- a. Based upon MbPT's identified encryption requirements, the Information Security Management Representative should determine the type of encryption algorithm(s)/ mechanism(s) to be used. The types of encryption algorithm(s) that may be considered include:
 - Public Key Algorithms
 - Symmetric Key Algorithms
 - Message Authentication Codes
 - Hash Functions
 - Digital Signatures
- b. Information Security Management Representatives should then review encryption solution(s) for protection of sensitive information contained in e-mails. Available solutions may include:
 - Digital signatures for ensuring message integrity, authentication and non-repudiation
 - Encryption algorithms for ensuring message confidentiality
 - Review and evaluate the products/ solutions available for the selected encryption algorithm(s).
- c. CISO should approve encryption solution(s) for use by MbPT.
- d. ISC should then prepare an Approved Encryption Software List recording all approved encryption algorithms, along with the acceptable key length for each.

Roles and responsibilities for encryption

- a. Information Security Management Representatives should ensure that only authorized personnel shall be allowed to use encryption software.
- b. Information Security Management Representatives should identify Owners and Custodians of encryption keys. Ensure that no single individual has sole custody of critical keys such as master keys used to derive encryption keys (i.e. 'split knowledge' for critical keys).
- c. CISO should define and implement procedures to establish accountability by:
 - Uniquely identifying keys

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	71
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

- Identifying users of encryption keys
 - Identifying dates and times of key use along with the data that is protected
 - Identifying other keys that are protected by a secret or private key
 - Limiting the amount of time a secret or private key is in plaintext form
 - Preventing users from viewing plaintext secret or private key.
- d. Information Security Management Representatives should ensure users, key owners and custodians are provided appropriate training, regarding usage of encryption software.
- e. Information Security Management Representatives should:
- Conduct review of adherence to the Key Management Policy and Procedures for usage of encryption software on a Quarterly basis.
 - Verify that implemented procedures continue to support the Key Management Policy.
 - Verify that the protective mechanisms employed offer the desired level of security for encryption keys.
- f. Information Security Management Representatives should maintain contact with vendor/ suppliers of encryption solution(s) for receiving updates on new developments, threats and for obtaining assistance in case of incidents related to encryption solution(s).

Encryption key management

- a. Information Security Management Representatives should define procedure for authentication and secure registration of users, systems or applications in the encryption solution.
- b. Information Security Management Representatives should initialize the encryption solution:
- Define encryption algorithm preferences
 - Identify trusted parties
 - Identify recognized certificate policies.
- c. Key administrators should initialize the registered users, systems or applications by installation of initial keying material.
- d. Information Security Management Representatives should review installation process and ensure physical security of keying material during entry into software/ hardware/ system/ application/ or encryption device for initial installation.
- e. Information Security Management Representatives should establish encryption keys for secure communication between registered entities.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	72
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

- f. Information Security Management Representatives should distribute the established encryption keys as per the deployed symmetric/ asymmetric encryption algorithm's defined procedure for secure distribution. Further, they should ensure that:
 - Identity of the receiving party is established based on the authentication information provided during registration.
 - Secure distribution channel is used for keydistribution.
 - Keys are distributed in an encrypted form.
- g. Information Security Management Representatives should ensure that other encryption material, if any, required for usage of encryption keys is also distributed securely. Other encryption material mayinclude:
 - Domain parameters required by some Public key algorithms
 - Initialization Vectors used by symmetric encryption algorithms
 - Random Number Generator (RNG) seeds.
- h. Information Security Management Representatives should perform Key Registration for binding the key information with various users of encryption keys.

Encryption key storage and change

- a. Information Security Management Representatives should identify all devices (such as storage media, device or module performing encryption, backup tapes, etc.) where encryption keys are stored.
- b. Information Security Management Representatives should develop procedure for secure storage of encryption keys and define:
 - Devices where storage of encryption keys is permissible
 - Conditions under which storage is permissible.
 - Personnel authorized to access encryption key storage areas
 - Access criteria for encryption key storage
- c. Information Security Management Representatives should define procedures for securely changing the encryption keys. The keys shall be changed:
 - On expiry of key validity, or
 - When the encryption keys have been compromised/ suspected to be compromised.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	73
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Encryption key archival and recovery

- a. Information Security Management Representatives Should Develop guidelines for archival of encryption keys, based upon recommended practice for the selected encryption solution:
 - Identify encryption keys requiring archival
 - Determine archival period
 - Identify physically separate locations for storing archives
 - Define access control measures for restricting unauthorized access to encryption key archives
- b. Information Security Management Representatives should define Key Recovery guidelines for retrieving the desired keying material from archive storage in order to perform the required cryptographic operation. They should ensure that the guidelines specify:
 - The conditions under which the key recovery process may be initiated
 - Notification procedure to key owners when key recovery has been performed
 - The provision for removal of encryption keys from the system and secure return to the archive.

Key revocation and destruction

- a. CISO should authorize entity de-registration, once the entity is no longer a part of the security domain of encryption system.
- b. The Information Security Management Representatives should de-register entity from encryption system.
- c. The CISO should authorize key de-registration if:
 - Keying material is no longer required
 - Associated information has become invalid
 - Keys have been compromised (Refer: MbPT – ISMS – L2 – Information Security Incident Management Procedure).
- d. The Information Security Management Representatives should then destroy all copies of encryption keys.

The Information Security Management Representatives should identify key attributes to be retained (such as type or Key identifier), post-destruction, for audit purpose. They should also ensure security of this information and restrict access to authorized individuals.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	74
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Physical and environment controls

Physical Security Perimeter

- A Physical security perimeter should exist around secure areas, should be clearly defined and should be appropriately labelled.
- The perimeter surrounding a secure area should be physically sound to prevent break-ins. In case the barrier contains any other outlets including fire doors, apart from the one used normally for access, deployment of suitable intruder detection system(s) like door alarms should be considered for such outlets.
- Doors and windows should be locked when unattended and external protection should be considered for windows, which are at ground level.
- The selection and design of a secure area should take into account the possibility of physical and environmental threats from neighbouring premises.
- Combustible materials should be stored securely at a safe distance from secure areas
- Fallback equipment and Backed up media of high risk IT resources in any secure area should preferably not be kept in the same secure area. If they are kept in the same secure area they should be at a sufficiently safe proximity from operational resources
- MbPT will be logically divided into three different physical zones. Each zone will have an appropriate level of access restrictions and access authorization requirements.
- Areas containing critical IT equipment will be designated as High Security Zones.
 - Zone 1: The Reception area and entrance lobby.
 - Zone 2: Operations and Support (including UPS room, security room and monitoring room)
 - Zone 3: IT Network Room (NOC) and Data Center

Physical Entry restrictions

Physical entry restrictions for premises

- Access to the premises should be restricted to employees and authorized personnel only
- All employees should be allowed in Zone 1. Audit trails for all accesses shall be maintained for accesses in the physical register or card access control.
- Access to some areas in Zone 2 including UPS room, CCTV room, Store room, Compactor room, Conference room and Zone 3 should be restricted to authorized people only. The restriction should be enforced through the use of access cards or Biometric access.

Physical entry restrictions for employees

- The employees should have the ID or access card in person while visiting premises. It would

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	75
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

be a violation of the MbPT Security Policy on the part of any employee using any such cards he or she is not authorized to. All authorized holders of such cards should keep these cards in a secure manner such that they should not be used by anybody else.

- The entrance should be manned by security guards on a 24-hour basis. The guards should challenge all the visitors and direct them to respective employees located inside premises.
- Access to Zone 2 and Zone 3 should be restricted through the use of access cards or through the use of any other suitable access controls like permanent passes authorized by the MbPT Administration. Wherever access cards with automatic logging system are not used, it should be mandatory that every entry and departure should be recorded in a manually maintained log register.
- Issue of these access cards should be strictly controlled and given only to such employees who should require access to secure areas as a part of their regular official duty.
- The proximity card system should log the employee ID/name and time of entry.
- The Administration Head should conduct a review of the log of proximity card records on a fortnightly basis for errors or rejections.

Physical entry restrictions for visitors

- MbPT management should identify areas where outsiders should not be permitted to enter unless the following are done:
 - Visitors should be classified into vendor/ suppliers, service-providers, customers, contractors, consultants, auditors and interview candidates.
 - The uninformed visitors (personal matters, site-visit etc.) should obtain written permission from respective head of department before entering into Zone 2.
 - Visitor should be accompanied by the authorized employee of the concerned Department, who has routine access rights to such areas as a part of his or her normal official duty.
 - Visitors should obtain permission from the Information Security Management Representatives or In-charge Authorized designee before gaining access to Zone 3. The visitors should always be escorted during their visit to the physical areas that store sensitive information or data.
 - The security personnel should randomly frisk all visitors manually and their bags should be checked to record the material carried by them into the visitor's logbook. At the time of their departure, they should be checked again to ensure that nothing (other than what had been logged) is being carried out.
 - Visitors should sign-in, in the visitors' logbook, which should be with the security guard. This should be retained for a minimum of 6 months and reviewed every month.
 - Visitors carrying laptops, tablets USB drives, CDs, floppies etc. need to enter the details of the same in the Visitor register.
 - Employees should intimate the Administration department of expected visitors well in advance. The Administration department should, in turn, inform the concerned employee about the arrival of the visitor in the office.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	76
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

- Visitors should wear a visitor badge to inform personnel that a non-employee is in the premises.
- All visitors should be instructed to return the badge before leaving the premises.
- Visitors should obtain prior permission from the respective department to work on weekends and holidays.

Access to Network room and Data Centers

- Access to Data Center in Zone 3 should be restricted by an access card reader system. The access should be granted only to the authorized team with due authorization. The CISO or Authorized Designee should authorize the access. The Department head and Information Security Management Representatives should review the accesses granted to the various personnel on a quarterly basis.
- Vendor/ suppliers need to access the Zone 3 for maintenance work for the IT equipment, infrastructure equipment and cleaning. The Supervisors or the Administration department team member should accompany such third parties and all the work should be done under their supervision. No third party should be allowed inside Zone 3 unless supervised by MbPT personnel.
- Security cameras should be installed in the Data Center and Network room and should be monitored by dedicated Security personnel. This data should be audited and correlated with other entries. Recorded tapes should be stored for at least 30 days of which 15 days should be running log and previous 15 days as archive. The ISC and the Administrative department should have access to view the recorded tapes in case they feel the need to do so.
- The NOC access details shall be noted for the visitors/Third Party Contractors. In addition, the logbook should contain the details of the activity performed by visitors and should also be countersigned by the accompanying MbPT IT personnel. All the Data Center /NOC entry logs should be retained for a minimum of six months.

Protecting against External and Environmental Threats Refer: 11.17 Environmental Security Standards

Working in Secure Areas

- MbPT personnel should be aware of the existence of and activities taking place within, a secure area on a need to know basis.
- Working Areas should be secured with emergency exits, uncluttered passages to main gate / emergency area, Fire exit signs. Working areas should have comfortable temp, Sufficient Lights and environment condition for safe working.
- Adequate care and precautions should be taken for working in area having flammable material.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	77
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Public access, delivery and loading areas

- Access to a delivery and loading area from outside of the building should be restricted to only identified and authorized personnel.
- The delivery area should be designed so that supplies can be unloaded without delivery personnel gaining access to other parts of the building.
The external doors of a delivery and loading area should be secured when the internal doors are opened.
- Incoming material should be inspected for potential threats before this material is moved from the delivery and loading area to the point of use.
- Incoming material should be registered in accordance with asset management procedures on entry to the site.
- Incoming and outgoing shipments should be physically segregated, where possible.

Equipment siting and protection

- Information processing facilities handling sensitive data should be positioned and the viewing angle restricted to reduce the risk of information being viewed by unauthorized persons during their use, and storage facilities secured to avoid unauthorized access.
- All Control Rooms should be housed in a separate isolated area, with access granted only to specific, named individuals on a need basis by the concerned Department Authority/MbPT Administration Department. However where physical isolation is not possible, appropriate measures shall be taken to restrict unauthorized access.
- Suitable floor structuring, lighting and power requirements should be considered given the nature of the operations.
- Infra / Supporting utilities of these equipments should be supervised regularly for their health checks , preventive maintenance and their emergency preparedness.
- Guidelines for eating, drinking, and smoking in proximity to information processing facilities should be established. (**Refer:** 11.17 Environmental Security Standards)

Security of electronic office equipment

- Electronic office equipment includes faxes, printer, scanner and projector. These should be physically secured, as they are sources of receipt or processing of data in a physical format. The security considerations are as follows:
 - The faxes and printers should be placed in Zone 1/ Zone 2. Access to both should be restricted to ensure that no visitor can gain easy access without notice of the staff. Supervisors responsible for the fax/ printer should ensure the physical access security and take necessary precautions. These equipment should be protected from heat, pollution and other environmental hazards.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	78
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

- Regardless of ownership, the use of any information processing equipment outside the organization's premises should be authorized by management.
- Equipment and media taken off the premises should not be left unattended in public places; portable computers should be carried as hand luggage and disguised where possible when travelling.
- Adequate insurance cover should be in place to protect equipment off-site.

Physical security of desktops and laptops

- IT users assigned to every desktop and laptop should take appropriate measures for ensuring the physical security of their desktops and laptops.
- All desktops should be provided with UPS for protection against loss or fluctuation of power.
- The respective users should ensure desktop security against fire, water and pollution damage.
- Their responsibilities include taking all possible steps to ensure safety and inform the Administration team in case any event is noted.

Physical security of Network Switches

- Network Switches located throughout the premises should be placed in locked cabinets and should be protected from fire, heat, dust, water and unauthorized access.
- All network jacks and access points should be enabled as and when needed by authorized employees only.

Supporting Utilities

Refer: 11.17 Environmental Security Standards

Cabling Security

- Power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage.
- The following controls should be implemented:
 - Power and telecommunications lines into information processing facilities should be underground, where possible, or subject to adequate alternative protection.
 - Network cabling should be protected from unauthorized interception or damage, for example by using conduit or by avoiding routes through public areas.
 - Power cables should be segregated from communications cables to prevent interference.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	79
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

- For sensitive or critical systems further controls to consider include:
- Cable and equipment markings should be clearly identifiable and used to minimize handling errors, such as accidental patching of wrong network cables;
- Installation of armored conduit and locked rooms or boxes at inspection and termination points.
- Use of alternative routings or transmission media.
- Initiation of technical sweeps for unauthorized devices being attached
- Use of fiber optic cabling.
- Structured cabling with marked labeling to identify it without any ambiguity.
- Site maps / equipment rooms should be displayed with equipment diagram at site along with cabling routes.

Maintenance of Electronic office equipment

- All equipment should be maintained in accordance with the supplier's recommended service intervals and specifications.
- Only authorized maintenance personnel should carry out repairs and service equipment.
- Records of all suspected or actual faults, preventive and corrective maintenance should be kept.

Appropriate controls should be implemented when equipment is scheduled for maintenance, taking into account whether this maintenance is performed by personnel on site or external to the organization; where necessary, confidential and highly sensitive information should be cleared from the equipment, or the maintenance personnel should be sufficiently cleared with respect to security controls such as access control procedures.

Office equipment management

- Photocopiers, Printers, etc. are important equipment for managing day to day operations in MbPT. The following procedures should be followed to ensure that these equipment are working properly continuously:
 - All users of the office equipment should be adequately trained to ensure that they use them appropriately. They should operate the equipment as per the guidelines provided by the vendor/ supplier of the specific equipment.
 - Administrators at the start of each shift should check the Fax machines, Photocopiers and key printers to ensure that they are working in good condition. If the cartridges are about to empty, ensure that spare cartridge is in place so that they can be replaced at any point of time that day.
 - As part of the maintenance schedule, every fax machine, projector, scanner, photocopier, printer, air conditioning system and Uninterrupted Power Supply (UPS) should be checked to ensure that they are working in good condition.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	80
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

IT Hardware management

- NOC team is responsible for Managing Servers, SECURITY team is responsible for managing workstations and Network team is responsible for managing network equipment.

Preventive maintenance

- Preventive maintenance is an important activity that needs to be carried out on IT hardware to ensure continuous availability of all the servers and network equipment.
- Typical maintenance activities may consist of the following:
 - Check hard drive capacity, optimize any local hard drives to defragment files and scan the surface for bad sectors.
 - Cleaning up of temp files and backed up log files
 - Regular housekeeping, including but not limited to maintaining a dust-free environment, removal of debris from immediate area etc. and the regular checks for integrity of cable installations, including attachment of cable ends, coiling of excess cable lengths, orderly cable runs, and cleanliness of connections.
 - Assurance of Uninterruptible Power Supply (UPS), including maintenance of battery installations, cleanliness of power cord junctions and contacts, cleanliness and integrity of grounding straps and conduits, checks of case ground integrity, earthing checks, Battery charge –discharge tests etc.
 - Monitoring physical installation integrity, including but not limited to tightness of rack mounting bolts and screws, slide hardware, and ancillary connections.
 - The preventive maintenance checks should be carried out where ever applicable, by the NOC team/service provider as recommended by manufacturer.
- NOC Administrators and Network Administrators should carry out maintenance activity based on the Preventive Maintenance Schedule.
- Information Security Management Representative or CISO Authorized Designee should review the maintenance activities carried out by the Administrators on a quarterly basis.
- Respective department head should ensure that the vendor/ suppliers and administrators regularly conduct the preventive maintenance as per the schedule.
- For all maintenance activities the Administrators should ensure that:
 - Preventative maintenance schedule and maintenance activities do not disrupt or impact in anyway critical or sensitive applications.
 - Maintenance activities are not scheduled during critical periods of data processing or other IT activities such as back up or restoration.
 - All parties are notified before any maintenance activity should be carried out.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	81
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Security of Equipment off-premises

- Regardless of ownership, the use of any information processing equipment outside the organization's premises should be authorized by the department head. A log should be maintained for the equipment moved off-site. (**Refer:** L3 – Off-site Movement Log.xls) The same should be reviewed periodically.
- Equipment and media taken off the premises should not be left unattended in public places.
- Manufacturers' instructions for protecting equipment should be observed at all times.

Disposal of Media

- Media should be disposed off securely and safely when no longer required. Sensitive information may be leaked to outside persons through careless disposal of media. Formal procedures for the secure disposal of media should be established to minimize this risk. The following procedures should be followed:
 - Media containing sensitive information and licensed software should be stored and disposed off securely and safely, e.g. By incineration or shredding, degaussing or formatted before use by another application within the organization.
 - The following list identifies items that require secure disposal:
 - Paper documents
 - Output reports
 - Magnetic tapes
 - Removable disks or tapes
 - Optical storage media (all forms and including all manufacturer software distribution media)
 - Test data
 - System documentation
 - Disposal of sensitive items should be logged in order to maintain an audit trail

Removal of assets in and out premises

- Any removal of sensitive information from the premises (temporarily or permanently) either physically or electronically should undergo the prior approval process of the Departmental Head.
- Information transfer using emails, faxes, hardcopies and verbal communication of confidential and sensitive information should be approved by the Department Head concerned.
- Information entry/removal using any other storage media like CDs, Hard disks, magnetic

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	82
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

tapes, emails containing sensitive information should have the prior approval of the Department Head concerned

- There should be frisking of bags of contractors by the security personnel, when they are leaving the office premises to avoid the theft of assets.
- Time limits for equipment removal should be set and returns checked for compliance.
- Where necessary and appropriate, equipment should be recorded as being removed off-site and recorded when returned.

Material going out

- All movement of material in and out of the premises should be controlled by security. All outgoing material needs to be accompanied by a gate-pass, which should be authorized by the Administration department and asset owner.
- Security personnel should check the material including IT assets against the gate-pass and enter the details in a register.
- In case an IT asset is sent out for repairs, probable date of return should be noted.
- The MbPT Administration team should review the register on a weekly basis. In case return of asset is delayed by a week, the delay should be pointed out to the Administration team and explanations should be obtained from the vendor/ supplier.

Material coming in

- Security personnel should enquire about the nature of material, which is being brought in, and record the details in a register maintained to record the receipts.
- The concerned employee should be informed of the receipt of the material.
- The concerned employee should conduct an initial inspection and acknowledge the receipt of the material.
- The concerned employee should also sign in the register to acknowledge receipt of material.
- The Administration team should review the register on a weekly basis.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	83
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Environmental security controls

Power supply

- Power supply is critical for uninterrupted functioning of the company. The power supply arrangements are as follows:
 - **Local Power Supply**

Electricity supply from the local power providers is regular. This should terminate at a local transformer to regulate the power that is available to the Operations area, which should not exceed permissible threshold (220-250 v). Further, within the Network room the voltages maintained should all be regulated to suit the servers as per the vendor/ supplier recommendations. Circuit breakers of appropriate capacity should be installed to protect the hardware against increase in power voltage.
 - **Uninterruptible Power Supply (UPS)**
 - A dedicated UPS (Uninterruptible Power System) with maintenance-free batteries (which should be replaced regularly depending on vendor/ supplier specifications) should be maintained for Network room and servers. The UPS should ideally reside in a similar dust free environment. There should be adequate space around the UPS for maintenance purposes. The UPS should be adequate to provide for voltages at the same level as the regular supply and there should be no glitches in the process of the UPS taking over the electricity supply as these glitches can severely harm the machines.
 - A single line diagram showing electrical connections and emergency contacts for the UPS should be prominently displayed in the room where the UPS is housed. UPS facility should be under lock and key and supported by Engineers 24x7.
 - The UPS and the generator should be tested regularly to ensure the smooth functioning of the power supply to the server room.
 - **Generator**
 - Generator should be automated to start up as soon as the electricity supply from the local power supplier gets cut off.
 - **Testing**
 - The UPS and the generator should be tested regularly to ensure the smooth functioning of the power supply to the Network room.
 -
 - **Heat and air pollution**
 -
 - The whole premises should have air-conditioning facilities to prevent dust, heat and air pollution affecting IT equipment.
 - **Temperature**
 - The Data Center should have dedicated air-conditioning equipment with the temperature

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	84
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

maintained at 20

- +/- 2 degrees Centigrade.
- **Humidity**
- The humidity level in the server room should not cross 55%. A humidity monitoring system or a humidifier should be placed in the Network room.
- **Dust**
- A dust free environment should be maintained by ensuring a high level of maintenance in the Network room.
- **Fire safety**
-
- **Network Room:** The Network room should ideally be fitted with a fire extinguisher.
- **Fire Alarms:** The whole premises should be fitted with automatic fire alarms. There should be manual
 - alarms located at strategic places in the building, which can be started, by any employee who notices fire, which the fire detectors have failed to detect.
 - For protection from fire following measures should be taken:
 - The combustible material should not be stored in the vicinity of the information assets.
 - There should be no eating, drinking or smoking in the operational site. The work areas should be kept clean at all times.
 - Fire extinguishers should be installed throughout the premises and their locations clearly marked with appropriate signs.
 - Periodic testing, inspection, refueling/ Recharging and maintenance of the fire equipment and systems should be conducted.
 - Procedures for the safe evacuation of personnel in an emergency along with the escape directions should be visibly posted throughout the premises. Periodic training and fire drills should be conducted.
- **Firefighting methods:**
 - When the heat of a fire is brought down, the minimum heat required to burn a fire is no more and the fire is arrested (caused by the absence of one contributory factor). Water is used to put out a fire in this manner. This method can be adopted in the case of burning wood, paper, etc.
 - A fire should continue only if inflammable articles are around. Therefore a fire can be brought under control, when such items are removed from the premises. If the burning item is physically shifted (such as a gas cylinder), the fire can be controlled. If it cannot be shifted, other inflammable items around should be removed from the affected area.
 - Firefighting equipment should be located throughout the premises and employees should be trained in its usage on a periodic basis.
- Emergency exits: Emergency exits (where present) or Evacuation Routes should be clearly

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	85
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

marked throughout the premises. They should always be kept obstacle free. Fire drills should be practiced on semi- annual basis.

- Reacting to fire contingencies:
 - As soon as a fire breaks out, fire alarm should be activated promptly.
 - Inform the fire wardens and the Administration Division immediately.
 - Consult the Administration Head or ISC and act according to instructions issued by the fire wardens.
- When the fire alarm is activated
 - An emergency squad should be readily available to respond for any contingencies such as fire, robbery and bomb threats. They should promptly respond to the fire alarm.
 - First of all the Administration team should check on the activation of the fire alarm.
 - Fire wardens should be responsible for informing employees of the fire and guiding them to safety during the fire.
 - These instructions should vary according to the type of fire and the area where it had occurred.
 - Fullest co-operation of employees is required. Employees and Customers within MbPT premises should remain calm and act according to instructions issued by the fire wardens.
- Instructions to fire wardens:
 - Select employees should be designated as fire wardens and provided training in firefighting techniques.
 - Fire wardens are required to use the knowledge acquired in firefighting procedures in the event of a sudden break out of fire.
 - If the situation is beyond the capacity to control, the fire alarm should be activated. Maintain calmness around and make arrangements to evacuate everyone from the floor. Sick people and those who are unable to move due to various reasons should have to be removed to the safe areas by the Administration team.
 - Admin should have list and location of sitting for Physically disabled person and their evacuation should be ensured in the event of fire.
 - Fire wardens should check whether everyone has left before leaving the premises themselves.
 - Any missing persons should be notified to the Security personnel.
- Responsibility of the occupants of the premises:
 - Find out ways and means of saving lives.
 - Learn to activate the fire alarm.
 - Learn to operate the firefighting equipment.
- The following should be avoided:
 - Shouting and creating a commotion. People become more and more restless thisway.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	86
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

- Pausing to collect personal belongings.
- Use of lifts during incident
- Fire alarms operating on a break glass system, and pillar hydrants, should be installed in the lobby area of every floor. In addition, the following firefighting equipment should be available on every floor:
 - Hydro fire equipment
 - Carbon dioxide fire equipment
- Smoke detectors should be located on each floor and should automatically get triggered off the smoke alarm in the event that smoke is detected.
- In addition to smoke detectors, water sprinklers may be installed. The water sprinklers should be automatically activated when heat in the vicinity causes the acid tube embedded within to burst
- Each floor should be divided into sections, and the fire alarm system should detect and highlight the floor and section that triggered off the fire alarm. This information should be used by security to quickly proceed to the exact location that triggered off the alarm.
- After investigating the cause of the alarm, fire wardens should inform the occupants of the building as to the cause of the alarm and what further action is required to be taken. These instructions should be noted carefully and followed.

Earthquake safety

- It is recommended to conduct earthquake evacuation drills on an annual basis. However, in case of rented premises, adequate training on evacuation should be provided.

Lighting safety

- It is recommended to install lightning arrest conductors on the top of the building for MbPT owned premises.

Theft safety

- The serial numbers of the laptops should be recorded during entry and exit of non-employees from the premises.
- Assets should be tagged and the material coming in and out should be tracked.
- All unused access cards should be kept un-configured and under lock and key.
- All information and data may be adequately labelled and based on the sensitivity, stored in separate safes or locations.

Water damage safety

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	87
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

- **Protection from Floods:** The premises should have adequate flood and rainwater drains. The premises should be continuously maintained to ensure that water seepage, if any, is detected and corrective action is initiated.
- **Location of Data Center:** All the walls of the Network room should be such a way that they should be isolated from any external atmospheric influence. The IT equipment in the Network room should be kept in waterproof shelves.
- **Drainage System:** The drainage system should be such that water and drainpipes are located away from the Network room.

Miscellaneous

- **Flooring:** The flooring should be at an ideal height of one foot from the ground and should be tiled with anti- static material.
- **Switches:** Switches and sockets should all be grounded (provided with earthling) and provided with circuit- breakers to avoid any untoward occurrences due to faulty wiring or short circuits.
- **Restriction to Ports in Visitor Rooms:** All network ports in the visitors' rooms should be disabled. They should be provided access only if there is a requirement of such an access.
- **Cleanliness:** To avoid dust from entering the Network room from the entrances, there should be a strict instruction on leaving the shoes outside the Network room with special rubber slippers provided for the server room. Also no food or eatables should be allowed in the Network room. Further, the surroundings of the Server should be kept clean and no trash or dustbins should be placed next to the Server.
- **Emergency Lamps:** Self-activating emergency lamps should be placed within the premises, as they may be required to handle abrupt power failures. Also alternate arrangements such as emergency lights, torches and ventilators should be present.
- **Hazardous or combustible materials:** Hazardous or combustible materials should be stored at a safe distance from a Zone 3.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	88
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Ops security

Operational Procedures and Responsibilities

Documented operating procedures

- Respective team representatives/ SMEs are responsible to document standard operating procedures for their domains. These procedures will be document controlled as per the Control of documents records procedure;
- While documenting and approving operating procedures, segregation of duties are to be considered;
- Operating Procedures within each department are made available through Share folder. Overall network usage guidelines, including desktops, internet, E-mail are as per IS guidelines applicable for all users;
- Operating procedures, and the documented procedures for system activities, will be treated as formal documents and changes to the same will be authorized by the respective department heads;
- For MbPT all business related documents, SOP's, process documents should be available to all associates and team members as and when required as per the document access control; and
- The Operations Manager (for MbPT) should be responsible to ensure that the operating procedures are maintained and up-to-date.

Change

management User request and approval

- ☐ Information resource changes (like system engineering changes, hardware, networking, communications, infrastructure facilities, information processing facilities, system configurations, changes associated with system development cycle, major database changes, high impact modification or relocation of desktops, any unscheduled high impact changes required to complete tasks associated with normal job requirement such as cabling systems etc.) are required in the IT infrastructure due to the need for additional capacity, application up gradation, implementation of new applications, etc.
- ☐ **Request for Change:** RFCH's are initiated through the Department Head. A request for change can be initiated from a Service Call, Request for Service, or Incident. The change may be initiated by a customer or technology user. The Change Request Form (**Refer:** L3 – Communications and Operations Management - Change Request Form) is created by the Departmental Head for the change.
- ☐ **Preliminary Planning and Requirements Analysis:** Preliminary information regarding the change is gathered. This includes describing the change and its objectives, identifying the benefits to the customer, and identifying the systems and the type of change.
- ☐ **Impact Analysis and Risk Assessment:** An initial impact and risk analysis is conducted to

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	89
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

determine who and what may be affected and the degree of impact. An assessment of impact for not doing the change is also included. Alternatives to doing this change are also identified as part of the initial assessment.

- **Review and Approve:** The change request is reviewed by the respective team, and/or Department Heads, depending upon the impact classification and scope of the change. Approval is granted/denied by the Department Head.

Testing and Implementation

- **Design and Implementation requirements:** The Change is classified as High, Medium, or Low impact. To arrive at this assessment you identify who and what will be potentially affected by the change including Department(s), systems, configuration items, procedures, costs, schedules, and resources. The implementation procedure and schedule requirements are also documented at this stage.
- **Test Development Plan**
 - o The Testing team, and system and network administrators should do the setup and testing of technology assets. System Administrators should prepare a test plan for testing the changes. Testing for information resource changes should be done in a test environment independent of MbPT operations. Once the test is conducted satisfactorily, the changes should be implemented in the production environment.
 - o During this phase, ISC should ensure that the user operating manual, system documentation and Minimum baseline security standards are updated before migrating to the production environment.
- **Fall back plan**
 - o Prior to implementation of the changed programs on the production systems, there should be a very clear Rollback Plan created by System Administrators and Impact Analysis document prepared to counter any problems that may occur during the implementation of the changed programs on the production systems.
 - o Backup of the live servers should be taken before carrying out any major changes on the servers.
 - o Sign-off from CISO and the Head of Departments (if affected by the technology asset change) should be obtained for successful completion of change control procedures and accuracy as well as integrity of data. System Administrators or Network Administrators should do the rollout of the technology asset after getting the sign-off.
- **Test Results**
 - o Test Results are documented to ensure that the results of the testing have provided input to the Design and implementation Requirements as needed to facilitate a successful implementation.
 - o The Change Administration Board makes a decision on whether the change should be implemented based on the information supplied in the RFCH.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	90
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

The above processes are intended to provide enough information to evaluate and validate the technical feasibility, risk and effect a change will have on the production environment

Change closure

- A post-implementation review is conducted to determine whether the change has achieved the desired goals. Post-implementation actions include assessing the implementation process, validating success, identifying lessons learned, and finalizing the change documentation.

Complete Documentation: Post implementation documentation consists of providing sufficient information to determine the effectiveness of the change. This should consist of testing and monitoring results, whether the goals of the change were met, the identification of any lessons learned, whether the change stayed within schedule and budget, and documentation of fall back execution.

- **Post Implementation Review:** The Post implementation review is held at the next Change Management meeting after implementation. In addition to making a success or failure decision on the change implementation, the review will also consider how the change was deployed, and whether it was implemented on time and within budget. This exercise may result in additional documentation of lessons learned from the change.
- **Finalize All Documentation:** Once the change has undergone final review all associated documentation should be filed with the appropriate ticket and the ticket closed.

Emergency Change

- Depending upon the criticality of requirement, ISC will decide for changes, in consultation with Department Head, and implement the same with proper justification. Subsequently the ratification will be done with proper sequence of approval.

Capacity management

- **Monitoring System performance**
 - o Important aspects such as disk usage, memory, and CPU utilization of critical application systems should be monitored by Administrators on a weekly basis to ensure that any anomaly or potential disruptions are detected early and corrective action can be taken. Network equipment should be monitored by Network Administrators at multiple points of time every day for memory and CPU utilization.
 - o If the disk space is over utilized by system or application data, Administrators should request CISO for increasing the storage space or alternatively, reduce the data managed by deleting some of the historical data after approvals from CISO and ISC.
 - o Further Administrators should continuously monitor systems for any error messages that alert about imminent problems and such errors should be appropriately escalated and addressed.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	91
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

☐ **Monitoring Bandwidth utilization**

- o The Network Administrator should regularly supervise the bandwidth utilization using tools or custom scripts and peak levels should be defined in the bandwidth-monitoring tools/scripts such that alerts are generated and automatically communicated to the Network team so that the team is made aware of the choking or disruption of any particular link.

☐ **Monitoring Parameter Thresholds**

Component	Parameter	Point-in-time Threshold Levels	Period of time Threshold Levels
Servers	RAM	70%	65%
Servers	Hard disk	75%	60%
Servers	CPU	85%	70%
Network devices	RAM	75%	60%
Network devices	CPU	85%	75%
Links	Link utilization	75%	70%
Links	Verification of Service Levels against SLA	80%	80%

☐ **Reporting**

- o Administrators monitoring various information systems should update capacity monitoring form. This should be reviewed by supervisors of Administrators and ISC.
- ☐ Quarterly reports based on the above forms should be generated to clearly depict patterns of utilization of System performance and Bandwidth over a period of time. These should be submitted to the Department Head and ISC.

Separation of development, test and operational environments

- MbPT does not develop applications in house. Hence there are no separate development facilities;
- For Desktops, Servers, Image and IOS Patch upgrade, currently there is no separate Test environment. It is anticipated to be provisioned in the future.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	92
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Protection from Malware

Installation of virus and malicious software protection software

- System Administrator should ensure that Anti-Virus software is installed in all possible entry points (Servers, Desktops, etc.) of viruses and Malicious Software. He should also ensure that they are installed with the latest version of the Anti – Virus Software.

Update of virus ‘signature files’

- These are the files, which contain the data on virus signatures. The update of anti-virus can be automated using software or can be done manually.
- **Automatic Update**
 - A system connected to the Internet checks the vendor/ supplier site at a scheduled time for any new virus updates.
 - If there is any update it should download and it should push the update to a server.
 - From the server, an operating system job should be scheduled in the network server for pushing these signature file updates onto servers/client computers/laptop computers/network nodes connected.
 - This job should be scheduled to run immediately after copying the signature files on the central host computers.
 - Specific vendor/ supplier software can also be used to push signature files on the clients / servers.
- **Manual update**
 - A system connected to the Internet checks the vendor/ supplier site at a scheduled time for any new virus updates.
 - If there is any update it should download and it should notify the System Administrator about the new update.
 - The System Administrator should then update the servers / desktops / laptop computers with the latest virus signature files.

Anti-virus software upgrades

- The upgrades are the newer versions of the anti-virus software. It is the responsibility of the ISC to procure and provide newer versions/engines of Anti-virus programs in regular and timely manner and ensure a quick rollout.

Review of logs

- Server Administrators should check the logs to review whether the desktops / laptop computers / servers were infected with viruses. He should report to the ISC every month

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	93
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

about virus incidents detected and removed during that month.

- System Administrator should review the anti-virus software activity/logs, especially to check whether the users are running the AV system regularly on their desktop computers (in case the user has the option to stop the scan).
- System Administrator should also check all the servers / desktops to ensure that they are updated with latest version.

Backup

Identification of data to be backed up

- The information to be backed up should be decided based on the legal, regulatory and contractual requirements.
- Also, the frequency of data to be backed up, medium of backup, location of storage of the backup media, retention period for the backup and overall backup plan for that data should be defined and documented based on legal, regulatory and contractual requirements (**Refer:** L3 – Communications and Operations Management - Backup Instruction Form).
- The users are responsible for taking and maintaining the backup of all critical data residing on their individual workstations.
- Based on the data identified for the backup a daily, weekly, monthly backup schedules should be prepared by the Department Heads. (**Refer:** L3 – Communications and Operations Management - Backup Schedule).
- In situations where confidentiality is of importance, back-ups should be protected by means of encryption.
- Two copies of the backup should be made to reduce the risk of failure in restoration. This control however should apply to only servers identified at high risk.

Backup Procedure

- Administrators should monitor the backup software logs. They should also store them securely for possible future reference.

Backup monitoring

- In addition to the scheduled backups, backups should also be taken and stored at a centrally located space in case any of the following events occurs:
 - Configuration change in an information asset.
 - Upgrade of any OS/Firmware/Application system etc.
- The Administrator should maintain the Backup Register and the reports generated by the system on the data which has been backed up.
- In case of any error messages during the system backup the Administrator should maintain

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	94
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

such report with response to errors.

- The Department Head should review the log on a monthly basis.

Backup media

- Choice of backup media should be guided by considerations like:
 - Criticality of data
 - Size of data to be backed up
 - Requirements of backup application
 - Speed of backup and restoration process
 - Data retention requirement
 - The expected life of storage media itself
 - Reliability requirements
 - Available technology
- Backup media should be rotated for backups based on the Backup Plans and Backup schedule.
- For Database Backup, server is being used in all the cases.
- It should be ensured that the media is regularly examined for readability of the data. The backup media should be replaced immediately after encountering the error or at predefined time intervals whichever is earlier.

Storage of backup data

On-site

- If on-site data backup is taken on tapes then it should be maintained in safe custody in a fireproof cabinet. Controls should be in place near the cabinet for protecting the cabinet from fire disaster.
- The key to the cabinet should be available only with the Administrator in charge of the backup and with the Operations head for emergency.
- A register should be maintained to record the names of personnel accessing the fire proof cabinet and the reason for the same.

Off-Site

- As per the backup schedule, identified back up media should be stored at an off-site location, in a fireproof cabinet. If the fireproof cabinet is not used, they should be stored in normal lockers.
- Whenever, the backup media is moved to and from off-site location, it should be carried in sealed and tamper-proof envelope or pouch. The backup media should be stored in

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	95
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

‘Fireproof Cabinet/Safe’. The key to the cabinet/safe should be only with the Security Personnel and should be provided only to the designated Administrator. The Security personnel should maintain the backup movement logs for the backups at off-site location. (Refer: L3 – Communications and Operations Management - Off-site Backup Movement Log)

Data Retention

- The data retention period is determined based on need and requirement basis of MbPT.

Backup Restoration

- If a backup restoration is required due to data loss or for testing purposes, the user should make a request for restoration and get the approval from the Department Head for the request. The Department Head should ensure that the user has the right to access the data required for restoration prior to forwarding the request to ISC for authorization.
- Once the approval and authorization is obtained, the data should be restored by the Administrators.
- A log should be maintained by the Administrator, containing the date and time along with the name and signature of the person who requested for the restoration of the data. The log also includes number of backup media used for restoration.
- All the backup media, which were used for restoration, should be returned to the off-site location after the restoration is complete in a sealed and tamper proof envelope (in case off-site backup media was employed).
- After successful restoration it should be ensured that the data restoration has not cause inadvertent alterations that might affect application performance.
- In case of emergency restorations, a telephonic approval from Department Head is sufficient but all necessary procedures and documentation should be completed after the restoration has been successfully carried out.

Restoration Testing

- The backup media kept as ‘Off-site backup’ should be used for such restoration. The ‘offsite’ location should have the same physical security controls as implemented for the normal operations environment.
- After successful restoration, the backup media should be marked as in ‘Proper Condition’ with the date of testing.
- All the backup media, which were used for restoration, should be returned to the off-site location after the restoration is complete, in a sealed and tamper proof envelope (in case off-site backup media was employed).

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	96
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

It should be ensured that the restored data is deleted from the test servers after successful completion of testing.

Logging and Monitoring

Event logging

- IT function shall ensure that the event logs recording the critical user-activities, exceptions and security events shall be enabled and stored to assist in future investigations and access control monitoring; and
- Logs shall be monitored and analyzed for any possible unauthorized use of information systems;

Protection of log information

- Security controls shall be built to ensure the integrity of logs;
- It shall be ensured that the system administrators do not have permissions to erase or deactivate logs of their own activities; and
- Access to audit trails and event logs shall be provided to authorize personnel only.

Administrator and operator logs

- All admin activities shall be logged in log files. Controls shall be in place to ensure that the device admin cannot tamper with the logs.
- These users shall not have access rights to access administrator and operator logs; and
- Administrator and operator logs shall be reviewed at specified intervals.

Clock synchronization

- The correct setting of system clocks is important to ensure the accuracy of audit logs, which is required for investigations or as evidence in legal or disciplinary cases. Inaccurate audit logs hinder such investigations and damage the credibility of such evidence. A system shall be put in place to ensure that all the servers, network equipment and desktops are synchronized to have same time;
- The network administrators must ensure that users cannot change this setting;
- Desktops – Are synchronized with the domain controller at US;
- Network Devices – All network devices synchronize with internal core; and
- Clock synchronization is enabled on the Voice devices.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	97
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Control of Operational Software

Installation of software on operational systems

- Windows patches are pushed by way of Marimba server;
- MbPT uses **Nessus/NMAP tool** for vulnerability management. Reports are extracted on a periodic basis by the external authorized agency or Stateside IT team in order to ensure that no device is vulnerable. This report is sent across to the MbPT team for action; and
- MbPT will ensure closure of the vulnerabilities and reportback.

Technical Vulnerability Management

Management of technical vulnerabilities

- A list of assets detailing the critical assets of MbPT is maintained;
- Internal technical vulnerability assessment of all the critical assets related to Servers, Network equipment's, desktops and laptops of MbPT are carried out on a yearly basis;
- On identification of vulnerabilities they are addressed on the basis of its criticality and reported to Admins;
- Timeline is defined for closure of each of the vulnerabilities identified depending on its criticality level; and
- In case of the remediation being infeasible, the risks are documented and reported to the Information security committee group for their actions. State Side Security engineering team provides the timeline to mitigate the respective vulnerabilities.

Restrictions on software installations

- Installations of software is strictly prohibited in the organization; and
- In case of business requirements, a formal approval is required from the concerned SME.

Information Systems Audit Considerations

Information systems audit controls: Refer Internal Audit procedure

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	98
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Communications Security

Network Security Management

Network controls

- Access to MbPT's network and network resources must be on need to know basis and will be controlled by user access privileges;
- Networks shall be logically or physically divided based on the criticality of the information stored in the networks;
- To maintain the privacy of the company information, and to protect the network equipment's from viruses, DoS attacks company networks must not be used for personal and/or private information, downloading unauthorized software's/ freeware unrelated to business activities; and
- IT team shall implement a firewall to restrict and scan all incoming and outgoing network traffic. The firewalls rules shall be updated regularly to cover all know vulnerabilities.

Security of network services

Information security clause is defined in the contract with all the vendor/ suppliers providing information systems to the organization.

Segregation in Networks

Segregation of network will be done on the basis of rules defined in firewall.

Information Transfer

Information transfer policies and procedures

- Retention and disposal guidelines for all business correspondence, including messages, will be in accordance with relevant national and local legislation and regulations; (Refer: Compliance Policy and Procedures);
- Sensitive or critical information must not be left on copiers, printers and facsimile machines as they may be accessed by unauthorized personnel;
- Automatic forwarding of communication facilities e.g. Automatic forwarding of electronic mail to external addresses will be restricted; and
- MbPT personnel, process will take appropriate precautions, not to reveal sensitive information to avoid being overheard or intercepted when making a phone call by people in their immediate vicinity, wiretapping or people at the recipient end.

Agreements on information transfer

- MbPT prior to beginning of any work with vendor/ supplier teams will take sign off from the MbPT

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	99
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Legal team. MbPT Legal ensures that a valid contract is established with the vendor/ supplier prior to begin of work as per MbPT guidelines.

- Exchange agreements shall consider the following security conditions:
- Management responsibilities for controlling and notifying transmission, dispatch, and receipt of information; and
- Agreements for non-disclosure, unauthorized use and Escrow agreements, if needed
- Responsibilities and liabilities in the event of information security incidents, such as loss of data;
- Ownership and responsibilities for data protection, copyright, software license compliance and similar considerations; and
- Any special controls that may be required to protect sensitive items such as cryptographic keys (if any).

Electronic Messaging

- Electronic messaging is a facility extended by the parent organization to MbPT. All MbPT employees are entitled to email services extended by the Parent organization to MbPT;
- MbPT follows secure usage guidelines, which are communicated to the users from time to time;
- Information involved in electronic messaging such as e-mail and instant messaging will be appropriately protected in lines with sensitivity of the information that is being sent via the email. Security controls for electronic messaging should include the following;
- Protecting messages from unauthorized access, modification or denial of service;
- Ensuring correct addressing and transportation of the message;
- General reliability and availability of the service;
- Legal considerations, for example requirements for electronic signatures as appropriate;
- Stronger levels of authentication controlling access from publicly accessible networks such as two factor authentication;
- Incoming and outgoing e-mail should be scanned for virus infiltration; and
- Use of encryption should be considered for emails containing confidential and highly sensitive information.
- Only the e-mail services provided by MbPT or provided by NIC shall be used for official communications by all organizations except those exempted under clause no 14 of this policy. The e-mail services provided by other service providers shall not be used for any official communication.
- This policy is applicable to all employees of MbPT that use the e-mail services of MbPT/ GoI. The directives contained in this policy must be followed by all of them with no exceptions. All users of e-mail services can find further information in the supporting policies available on

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	100
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

<http://www.meity.gov.in/content/email-policy> under the caption “E-mail Policy”

- Relevant Policies framed by Ministry of Home Affairs, relating to classification, handling and security of information shall be followed.
- Use of Digital Signature Certificate (DSC) [6] and encryption shall , be mandatory for sending e-mails deemed as classified and sensitive, in accordance with the relevant policies of Ministry of Home Affairs. Updation of current mobile numbers under the personal profile of users is mandatory for security reasons. The number would be used only for alerts and information regarding security sent. Updation of personal e-mail id, in addition to the mobile number, shall also be mandatory in order to reach the user through an alternate means for sending alerts
- Users shall not download e-mails from their official e-mail account, configured on the GoI mail server, by configuring POP [9] or IMAP [10] on any other e-mail service provider. This implies that users should not provide their e-mail account details (id and password) to their accounts on private e-mail service providers.
- Any e-mail addressed to a user, whose account has been deactivated /deleted, shall not be redirected to another email address. Such e-mails may contain contents that belong to the MbPT/GOI and hence no e-mails shall be redirected
- The concerned nodal officer (EDP) of the organization shall ensure that the latest operating system, anti-virus and application patches are available on all the devices, in coordination with the User
- In case a compromise of an e-mail id is detected by the IA, an SMS alert shall be sent to the user on the registered mobile number. In case an “attempt” to compromise the password of an account is detected, an e-mail alert shall be sent. Both the e-mail and the SMS shall contain details of the action to be taken by the user. In case a user does not take the required action even after five such alerts (indicating a compromise), the IA reserves the right to reset the password of that particular e-mail id under intimation to the nodal officer of that respective organization.
- In case of a situation when a compromise of a user id impacts a large user base or the data security of the deployment, the NIC shall reset the password of that user id. This action shall be taken on an immediate basis, and the information shall be provided to the user and the nodal officer subsequently. SMS shall be one of the prime channels to contact a user; hence all users should ensure that their mobile numbers are updated.
- Forwarding of e-mail from the e-mail id provided by GoI to the Government official’s personal id outside the GoI email service is not allowed due to security reasons. Official e-mail id provided by theMbPT/NIC can be used to communicate with any other user, whether private or public. However, the user must exercise due discretion on the contents that are being sent as part of the e-mail.
- Auto-save of password in the Government e-mail service shall not be permitted due to security reasons

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	101
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

- More details regarding security measures and Responsibilities of Users are available in “NIC Security Policy” at <http://www.meity.gov.in/content/email-policy> under the caption “E-mail Policy”

Confidentiality or non-disclosure agreements

Confidentiality or non-disclosure agreements reflecting MbPT needs for the protection of information will be identified and maintained with all the third parties and this will be based on the criticality of the information to be protected. These requirements will be reviewed at least once in a year, and at the time of any change of the business environment, legal requirements and contractual obligations. Confidentiality and non-disclosure agreements will comply with all applicable laws and regulations for the jurisdiction to which they apply.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	102
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

System acquisitions development and maintenance

Security Requirements of Information Systems

Information security requirements analysis and specification

- All new information systems and services that are acquired, developed or enhanced will undergo security assessment using a formalized process, to ensure that appropriate security controls are identified and incorporated in them;
- All new information systems and services, whether developed within MbPT, and/ or a commercial product, shall be assessed from all the following perspectives:
 - Business Process Controls;
 - Access Controls;
 - Authorization Controls;
 - Authentication Controls;
 - Application Controls;
 - Database Controls;
 - System Controls; and
 - Network Controls.
- A formal sign off shall be obtained from the IT, Business Function and Quality Analysis team before deploying the information systems in operational environment.

Securing application services on public networks

- Prior to deployment, all publicly available systems for e.g website is tested for threats such as denial of service, etc. and it shall be ensured that the identified vulnerabilities are fixed prior to publishing any information in such systems;
- Review of all public interfaces shall be carried out periodically;
- Firewall configurations for these applications will be reviewed and suitably updated from security perspective.
- Information contained on the publicly available systems like website, is accurate, authentic and posted only after the required approval is obtained; and
- Processed information shall be obtained in compliance with the required data protection legislation.

Protecting application services transactions

- IPSec is configured to ensure confidentiality of the MbPT's WAN traffic.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	103
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Security in Development and Support Processes

Secure development policy

- MbPT engages in software development activities however currently does not support separate testing facilities.
- Rules/Guidelines for secure software development shall be established .
- Test environment where ever required **will be** setup and maintained by the Development and Testing teams; and
- Software is selected by the user and procured with the help of MbPT. MbPT does assist the user to perform evaluation for the software.

System change control procedures

- MbPT will follow the change control procedure as listed in MbPT Change Management
- All local IT Operational changes (e.g., LAN, WAN, infrastructure/ operations) which would have any impact on business/production at MbPT shall also go through the change management process; and
- There are freeze periods implemented across MbPT in order to ensure smooth functioning of systems during critical periods.

Technical review of applications after operating platform changes

- New releases/ Patches pertaining to the operating system shall be tested before being implemented in the operational environment to ensure that there is no adverse impact on operation, application controls or security. In case of any exceptions due to technical limitations, approval shall be taken from the IT Head for acceptance of tests conducted by the vendor/ supplier, which shall be subjected to audit;
- The application controls shall be reviewed to ensure that they have not been compromised by the operating system changes; and
- It shall be ensured that notification of operating system changes is provided in time so that appropriate tests and reviews are done before implementation.

Restrictions on changes to software packages

- A detailed Business Request Document is shared with the vendor/ supplier mentioning the changes required as per the requirements of the function;
- Functional Specification Document (FSD) is further shared by the vendor/ supplier. The document clearly defines the requirement from the function;
- A final sign off is taken on the FSD by the Business Owner, IT Head and then Quality Analysis team before any customization is done; and
- Modifications to software packages are restricted, limited to necessary changes and all changes are strictly monitored.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	104
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Secure system engineering principles

Principles for engineering secure systems need to be established, documented, maintained and applied to any information system implementation efforts

Outsourced development

- For the customized (not off-the-shelf/ standard offerings) software developed by third parties, arrangements pertaining to licensing, code ownership and intellectual property rights are documented in the contract between MbPT and the Third Parties;
- The contract shall include that MbPT reserves the right to audit quality and accuracy of software development and testing; and
- VA test reports shall be sought from 3rd party vendors and vulnerabilities shall be addressed to acceptable level before implementation of any software.
- Testing of the software is done before its installation.

System security testing

Testing shall be conducted from security perspective during the development phase. These tests shall be conducted against the security requirements identified in the planning phase and the vulnerabilities, which can be exploited by internal/ external threat source, in the modules being developed.

system acceptance testing

- Acceptance criteria for new information systems and information processing facilities, upgrades and new versions is defined in the Functional Specification Document and Business Request Document;
- Security clearance is obtained from the IT Head/ Business Owner/ Quality Analysis team before any new information systems, upgrades and/ or new versions are accepted; and
- User Acceptance Testing (UAT) is conducted prior to the deployment of the systems in the production environment.

Test Data

Protection of test data

- Acceptance tests shall be carried out using the test data, which shall be similar to the operational data which will not include any Personally Identifiable Information (PII);
- The software development team shall ensure that test data is secured and sanitized during testing;
- Test data is backed up at different stages of testing;
Operational information is erased from test application system immediately after the testing is complete;

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	105
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Supplier relationship

Information Security in Supplier Relationships

MbPT's Location Heads should decide upon the goals and objectives of the outsourcing initiative and communicate how the process will benefit the organization. The outsourcing initiative should serve the objective of MbPT to concentrate on core competencies, obtain financial benefits and gain competitive advantage.

- **Team Constitution**

The coordination for constituting the team and evaluation of the outsourcing should be performed by the Department Head initiating the outsourcing requirement. The team should include the CISO.

- **Business rationale and Risk Assessment**

The Department Heads should identify and document the rationale behind outsourcing an activity and perform a cost – benefit analysis of outsourcing the activity. The team should conduct a Risk Assessment to identify potential risks to MbPT's information security as a result of outsourcing information or data processing functions or services to third party organizations. The team should prepare a document on the business rationale, risk assessment and present it to the Location Heads for analysis and discussion. After the detailed analysis of the document, the Department Heads should approve the same..

- **Communication to Staff**

- There should be a formal communication with staff members explaining the rationale behind outsourcing and the operational modalities.
- Management should communicate effectively to staff members about dealing with third party staff in

daily operations. This is crucial in bridging the gap between personnel of MbPT and third party, enabling them to appreciate their complementary roles.

- **Contracts, Service Level Agreement and Non-Disclosure Agreement Procedures**

- MBPT carries out the vendor/ supplier/ supplier identification and selection process for any requirement raised by MbPT. Once the Vendor/ supplier is selected, a formal contract signed between MBPT and the service provider shall be referred. Vendor/ supplier/ supplier Management Standards are determined by MBPT for various aspects that are included in the contract and SLA.
- MbPT should ensure the following:
 - Usage of SLAs laid down in the contract between the third party vendor/ supplier and MBPT with measurable parameters as the prime reference against which to manage and measure the Vendor/ supplier/ supplier's performance.
 - Adequate time scales before renewing the contract to allow time for review of past performance.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	106
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

- System Availability: It is applicable as per the Master Service Agreement signed between the vendor/ supplier and MBPT.
- MbPT will subject outsourced parties/third parties such as Vendor/ supplier/ suppliers, Auditors, Consultants, etc., to the same access restrictions to which an internal user would be subject. Since confidential/internal information cannot be controlled once it is distributed outside MbPT; third-party access to the same should be restricted to the information they require in completing the contracted work. Non-Disclosure Agreement (NDA) / Confidentiality agreement should be signed by Vendor/ supplier/ suppliers, third parties, contractors and also by sub-contractors of the Vendor/ supplier/ suppliers in order to protect MbPT's information assets.
- Reference to the background checks should be available in the tender document signed between MBPT and the vendor/ supplier/ supplier.
- **Risk assessment and Security Measures**
The Risk assessment and Security Measures will be a part of evaluation and selection process carried out by MBPT for the relevant vendor/ supplier/ supplier.
- **Service Level Agreements with other Departments**
- In addition to SLAs with external parties, MbPT should also establish SLAs with the Internal Departments. This SLA should clearly define the responsibilities of Internal Departments within MbPT and expected service levels from either of them.
- Other considerations such as principal Management Representatives and escalation procedures also need to be defined and formalized in the form of a SLA.
- **Vendor/ supplier/ supplier Management Standard**
- **Considerations for Contract**
- The contract shall be prepared by MBPT for the relevant vendor/ supplier/ supplier as per the terms and conditions laid down by the Government of India.
- **Considerations for Service Level Agreements**
- The tender document shall be prepared by MBPT for the relevant vendor/ supplier/ supplier as per the terms and conditions laid down by the Government of India.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	107
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Information Security Incident management

The purpose of this incident-handling procedure is to provide guidance to restore normal operations quickly and efficiently following an incident at MbPT.

Definitions

Security/Operational incident

A “Security/Operational incident” is an adverse event where:

The IT resource is attacked or threatened with an attack.

- The IT resource is accessed/ monitored/ modified without authorisation.
- The IT resource is used in a manner inconsistent with the established organization/regulatory policy resulting in a real or possible loss of confidentiality, integrity or availability of the IT resource or information.
- Examples of Security incidents are:
 - Internal or external attempts (either failed or successful) to gain unauthorised access to the IT system or its data.
 - Denial of service (DoS) or unauthorized disruption to IT system and infrastructure.
 - Actual or suspected loss of proprietary, confidential or entrusted information of the organization
 - Changes to system hardware, firmware or software characteristics without the Department Head’s knowledge, instruction or consent.
 - Malicious code (virus, Trojan horse) attacks.
 - Social engineering (tricking someone to disclose confidential/proprietary information like passwords that could compromise system security).
 - Hoaxes (deliberate trickery intended to gain an advantage e.g. false virus warnings may lead some user to ignore all virus warning messages, leaving them vulnerable to a genuine, destructive virus).
 - Physical (e.g. break-ins, thefts, vandalism) or logical (e.g. breaching usage policies for Email, Internet, Applications and Desktops or unauthorized computer access) unauthorized entry leading to loss of data or any other significant violation of the MbPT Security Policy Procedures.
 - Loss of confidentiality, integrity or availability of information by internal Employees including outsourced manpower working under control of MbPT
- Examples of Operational incidents are:
 - Firewall Application/hardware failure.
 - Anti-virus Application/hardware failure.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	108
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

- IDS application/hardware failure.
- Downloading unauthorized software/applications

Problem/ Event

- An event is an observed or observable occurrence in a system, a network or daily operations. The event will be reported to designated e-mail id **isms-incident@mumbaiport.gov.in**
An event will be termed as an incident if it is considered to have “adverse” impact on the IT system/infrastructure or through pre-positioned criteria that describes the circumstances under which events will automatically be deemed adverse.
- An event will be an incident when it is analyzed and classified to be adverse by the incident response team.
- Until events are classified not adverse, they are considered as “suspected incidents”.

Incident Response Team (IRT) and Process

- The Incident Response Team (IRT) is formed to address any incidents and initiate immediate action to resolve the same. The Incident Response Team defines procedures to proactively address potential threats/ risks arising out of incidents. Such teams are formed ad hoc; and are based on the severity and impact of the incidents. But most incidents are to be handled at the Incident Team leader level.
- The IRT Help Desk Team and IRT team composition is as follows:

IRT Help Desk Team

Sr.No.	Name and Designation	Section/Department	Contact
1	Ms. Maya Alwa, Programmer	EDP (MEED)	6656-5781
2	Ms. Anita Tijore, Jr. Engineer, Grade-I	ENT (MEED)	6656-5769
3	Mr. Rajesh S. Chandragade, Jr. Programmer	EDP (MEED)	6656-5777

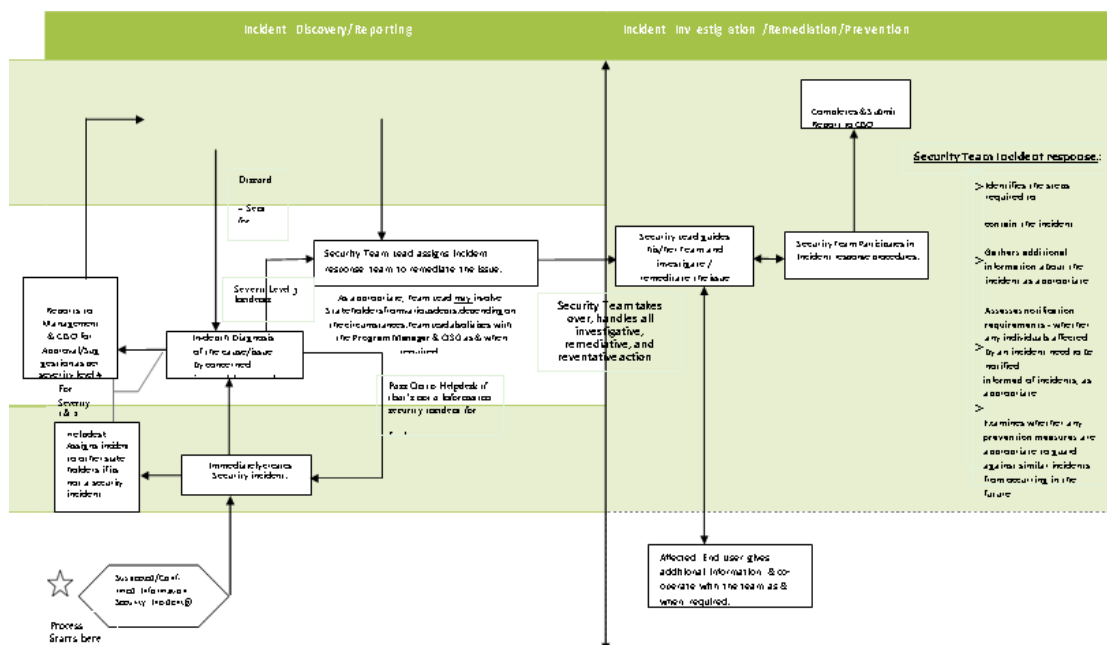
IRT Team

Sr.No.	Name and Designation	Section/Department	Contact
1	Mr. Ramesh Potdar, Dy. Manager	EDP (MEED)	6656-5107
2	Mr. Pradip Meher, Asstt. Director	EDP (MEED)	6656-4116
3	Mr. Vinod R. Bhoj, Asstt. Director	EDP (MEED)	6656-5771
4	Mr. Chandrashekhar Uparkar,		6656-5114

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	109
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

	Asstt. Director.		
5	Mr. Nitin Bane, Programmer	EDP (MEED)	6656-5106
6	Mr. Jagdish Sawant, Programmer	EDP (MEED)	6656-5789

- The IRT process is as follows:



- Expected Reporting Time**

Escalation: The escalation hierarchy is as follows:

- Level 0 – ISC
- Level 1 – ISC/ CISO
- Level 2 – ISC/ CISO
- Level 3 – CISO

Members at appropriate levels should escalate incidents.

Incident Investigation

- The security event should be reviewed by ISC in order to ensure that it is an incident or event.
- The incident should be analysed and impact over the business should be identified, if possible.
- The cause of the incident should be identified to further distinguish as security incident or

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	110
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

operational incident, if possible.

- The incident should be escalated to the CISO.
- The CISO and ISC should classify the incident type as “Operational” or “Security” and incident severity as “HIGH”, “MEDIUM” or “LOW”. The incident can be classified to its severity based on its business impact to the organization’s services.
- At a minimum, following criteria’s should be used to identify the incident as an operational incident:
 - Hardware problem over security and network devices.
 - Inappropriate configuration by the SECURITY TEAM, Networks or DC (Data Center) team.
 - The operational incident should be prioritized as high/medium/low. The following are the examples of operational incidents:
 - **Operational incident – High**
 - Firewall failure due to hardware/software problem
 - Server hardware/software failure
 - Production database failure
 - **Operational incident – Medium**
 - IDS/IPS/ Content filtering appliance hardware failure
 - E-mail relay agent hardware failure
 - Internet link failure / Leased line failure
 - Production application server failure
 - Production application database failure
 - Internal e-mail server hardware failure
 - **Operational incident – Low**
 - One clustered server failure
 - Application zone switch/router hardware failure
 - The security incident should be prioritized as high/medium/low. The following are the examples of security incidents:
 - **Security incident – High**
 - External internet router failure due to successful hacking attempt from the internet
 - Both external and internal firewall failure due to successful hacking attempt from the internet
 - Web server deface
 - Application server compromise due to successful hacking attempt

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	111
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

- E-mail relay agent failure due to successful hacking attempt
 - Virus or worm detection (unconfined)
 - Unauthorized changes to the configuration of network and security devices
 - Unauthorized account in the security and network devices
 - Confirmed security violations of user or external contractor
 - Missing anti-virus software
- **Security incident – Medium**
- Repeated active probes or port mapping from internet
 - Attempted web page attacks or defacements launched from internet
 - Unauthorized modification of the webpages on the webserver
 - Application server hacking attempt
 - Virus or e-mail spam issues with multiple users
 - Unauthorized installation of instant messengers for chatting over the internet;
 - Attempt to gain unauthorized access to the resources / bio-metric devices, either from within or outside the organization's network;
 - Unauthorized modification of production application system without prior approval; and
 - Unauthorized installation of software.
- **Security incident – Low**
- Non-repeated scans or pings from internet over web server and e-mail relay agent
 - Virus or e-mail spam issues for less than 10 users
 - Account lockout due to incorrect password trials
 - Unprotected system console
 - lack of upgrade/update of anti-virus or OS patches

Collection of Evidence

- The collection of evidence for information security incidents should take into consideration the following:
 - Admissibility of evidence: Whether or not the evidence can be used in court.
 - Weight of evidence: The quality and completeness of the evidence.
- To achieve admissibility of the evidence, care should be taken to ensure that MbPT's

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	112
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

information systems comply with any published standard or code of practice for the production of admissible evidence.

- The weight of evidence provided should comply with any applicable requirements. To achieve weight of evidence, the quality and completeness of the controls used to correctly and consistently protect the evidence (i.e. process control evidence) throughout the period that the evidence to be recovered was stored and processed should be demonstrated by a strong evidence trail.
- The following should be considered:
- For paper documents: The original is kept securely with a record of the individual who found the document, where the document was found, when the document was found and who witnessed the discovery; any investigation should ensure that originals are not tampered with.
- For information on computer media: Mirror images or copies (depending on applicable requirements) of any removable media, information on hard disks or in memory should be taken to ensure availability; the log of all actions during the copying process should be kept and the process should be witnessed; the original media and the log (if this is not possible, at least one mirror image or copy) should be kept securely and untouched.
- Any forensics work should only be performed on copies of the evidential material.
- The integrity of all evidential material should be protected. Copying of evidential material should be supervised by ISC and information on when and where the copying process was executed, who performed the copying activities and which tools and programs have been utilized should be logged.

Incident Response and Resolution

- The appropriate solution should be implemented based on the type and impact of the security incidents.
- The cost of information security incidents should be quantified and monitored before implementation.
- Denial of service attacks:
 - Identify the source IP address of the attack on the external firewall and implement the access control rule to block that source IP address at external firewall, external perimeter router.
 - Escalate the incident to the ISP to block the source IP address.
 - Configure the external IDS to perform “TCP reset” and “firewall reconfiguration” over the source IP address of the attack.
- Viruses and Worms:
 - Disconnect the system from the network which is infected with the virus.
 - Update the anti-virus signature on the system and scan the machine at both operating system level and boot level (if possible).
 - Verify the vendor site for any tool which will scan the system for the presence of viruses or

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	113
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

worms on the system.

- In the event of “worm” which may spread through specific “port”, identify the port from the vendor site and block it at all the firewalls.
- Ensure the anti-virus gateway appliance has up-to-date anti-virus signature file.
- Alert all the users in the organization by sending an e-mail stating not to open any e-mails from unknown sources or particular type of e-mail with specific “subject”, “attachment” or “content”.
- Server/System Deface
 - Disconnect system from the network.
 - Collect log files on the web server to trace the source of this attempt.
 - Verify log file on the external IDS/IPS and external firewall.
 - Perform host based vulnerability assessment over the web server to identify any latest vulnerabilities on the system.
 - Verify the file permissions on the production application server and perform host based vulnerability assessment over the system.
 - Verify all the file permission and user permission on the system.
 - Perform penetration testing over the system by restricting it to specific source on the internet.
 - Reconnect the system back to the production network for internet users.
- Additional Resolution Measures
 - In the event of an incident that cannot be resolved an appropriate alternative solution should be implemented where possible and following a review process to obtain approval from Information Security Management Representatives.
 - Should incident response requires changes to security and network devices configurations, changes should be made in accordance with the change management and configuration management process recommended separately.
 - The vendors should be called for any support over the incidents, which cannot be resolved by the MbPT’s team.
 - The incident should be resolved and the IT infrastructure should be brought to the normal working operations.
 - Incident documentation
 - The incident should be documented to clearly identify whether it is a security incident or operational incident. The incident handling form provided in the appendix should be used for the documentation.
 - For operational incidents, the incident handling form will be maintained by the IT team.
 - For security incidents, the incident handling form will be maintained by the ISC
 - The incident severity should be documented.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	114
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

- The person who reported the incident and the personnel involved in resolving the incident should be documented.
- The incident description and the solution implemented should be clearly documented. This will facilitate the IRT team in applying the same solution if the incident occurs again in the future. (**Refer** L3 – Incident Record.doc)
- The time required to identify and to resolve an incident should be documented.
- The incidents as per the incident management policy should be reported to the senior management through Information Security Management Representatives meetings.
- The incident database can be used as a guide to resolve the similar and specific incident occurrence.
- The incident documentation should be supported with evidences in a method, which can be presented to conform to the rules for evidence laid down in the relevant jurisdictions.
- Some of evidence can be:
 - Event Log files
 - Firewall Logs
 - Change of ACL for privileged programs.
 - Presence of common backdoors and Sniffer programs
 - Unauthorized services enabled/files installed.
 - Changes to password files and user accountsfile.

Contact with authorities and special interest groups

- The ISC should maintain contact with external authorities, special interest groups and forums (e.g. law enforcement, Port Security Advisors, CISF team, Cyber security team, CERT-In, NCIIPC, NIC team, utilities and emergency services, telecommunication providers) for information security incidents. Head admin/Admin security SPOC should maintain contact with fire department water suppliers, health and safety, supervisory authorities.
- Membership in special interest groups or forums should be considered as a means to:
 - Improve knowledge about best practices and staying up to date with relevant security information.
 - Ensure the understanding of the information security environment is current and complete.
 - Receive early warnings of alerts, advisories, and patches pertaining to attacks and vulnerabilities.
 - Gain access to specialist information security advice.
 - Share and exchange information about new technologies, products, threats, or vulnerabilities.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	115
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Information security Aspects of business continuity management

Information Security Continuity

- All the information security functions from the MbPT locations under scope have their backup in terms of business continuity and information security continuity.
- In case the helpdesk tool is down, all the security incidents/ events can be reported on the email id

<<isms-incident@mumbaiport.gov.in>>>

- The internal audit team ensures that if one person is unavailable then the other person from the same location takes up the security responsibilities.
- For <<<Backup/BCP Location>>>, the security Management Representatives and their backup information shall be maintained as per below :

Name of Security Person	Backup Person
Shri V.B.S.V. Rao, Jt. Director & CISO	Shri Ramesh Potdar, Dy. Director

- Information security requirements shall be integrated in the Business Continuity Plan;
- The Business Continuity Plan shall include prioritization and treatment for the critical processes, systems and applications and the supporting infrastructure;
- A thorough risk assessment shall be planned for all assets required for business continuity, considering all the events that can cause disruption to the business processes. The considered events shall include, but are not limited to, man-made error/ disaster, natural disaster and technical failure;
- The department head shall ensure that Business Impact Analysis (BIA) reviews and updates are planned and carried out at least annually to identify and prioritize the critical business processes, systems and applications and costs of downtime. The BIA shall cover the major business processes that cut across multiple departments/ functions
- The security continuity plan shall be tested on an annual basis and shall be updated annually to incorporate the changes in business environment and technology infrastructure;

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	116
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

- Exercising methodologies shall be clearly defined, where such exercises should be scoped, signed off by respective functional heads, monitored for adherence to plan and reporting of results of the exercises; and The methodology for business continuity exercise and testing shall be detailed out for easy understanding of the implementation personnel.

Redundancies

Availability of information processing facilities

- MbPT has identified business requirements for the availability of information systems;
- Redundant information systems is tested to ensure the failover from one component to another component works as intended, where ever applicable.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	117
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Compliance

Compliance with Legal and Contractual Requirements

Identification of applicable legislation and contractual requirements

- Advice and approval on the statutory, regulatory and contractual requirements of MbPT Office should be sought from the legal department. The CISO will delegate the responsibility to document the requirements in a register with the corresponding controls associated with each regulatory and legal requirement ; and
- The legal department will instruct the employees on the legal requirements and the compliance to such legal requirements.

Intellectual property rights

- IT team shall identify and maintain records of all third party software's and their licenses
- IT team shall identify and maintain records of all hardware usage licenses;
- IT team shall maintain proof and evidence of ownership of licenses, master disks, manuals etc. and compliance with the licensing policy; and
- IT team will carry out regular checks on user machines, servers and network devices that only authorized software and licensed products are installed.

Protection of records

- All organizations records will be safeguarded and protected from unauthorized access, damages, and natural and environmental risks; and
- Respective department heads are responsible for safeguarding the records of their respective departments.

Privacy and protection of personally identifiable information

- Data protection and privacy will be ensured as required in the identified relevant legislation, regulations, and applicable contractual clauses;
- Based on the Information Classification Policy, all information will be classified as 'Confidential' or 'restricted'; and
- Access to personal information should be on 'need to know' basis and access control should follow the requirements specified for all information classified as 'Confidential' or 'restricted'.

Regulation of cryptographic controls

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	118
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

- Cryptographic controls shall be used in compliance with all relevant agreements, laws and regulations;
- Suitable procedure for compliance assurance shall be documented and maintained by IT with support from Finance/ Legal functions;
PII shall be secured and encrypted (wherever applicable) at all the locations of its storage. These locations include, but are not restricted to, databases, portable digital media, backup logs, audit logs, transportation vehicles; and
- Legal advice shall be sought to ensure compliance with national laws before encrypted information or cryptographic controls are moved to another country.

Information Security Reviews

Independent review of information security

Compliance to the following policies and procedures will be regularly checked for compliance through independent authorities such as internal auditors, external certification auditors, and external consultants.

Compliance with security policies and standards

It's the responsibility of all employees to comply with the organizations information security policy and procedures. All non-compliances shall be treated as security incidents and basis the incident analysis, an appropriate action shall be initiated.

Technical compliance review

- The information systems used shall be regularly monitored by the operations personnel in order to check compliance with the defined standards. A check should be performed every bi- annually to ensure that users are only performing processes that have been explicitly authorized;
- Areas that should be checked for compliance are:
 - Access restrictions;
 - Review of logon patterns for indications of abnormal use or revived user Ids;
 - Allocation and use of accounts with a privileged access capability;
 - Desktop audits, printer access revalidation; and
 - The use of sensitive resources.
 - Compliance to all issues reported in VA and status of closure actions.
- The findings of the compliance check should then be reported to the DEPARTMENT HEAD / CISO

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	119
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

User Policies and procedures

a. Acceptable usage policy

Acceptable Use Policy

- Usage of MbPT information systems
 - Users are only authorized to utilize MbPT information resources for business purposes for which they have been authorized. Usage of MbPT information systems and resources for personal usage or on behalf of a third party (i.e., personal client, family member, political or religious or charitable or school organization, etc.) is strictly prohibited.
 - Users shall avoid accessing areas on the company networks for which they do not have a valid business need. While networks are intended to share information, it is each user's responsibility to exercise judgment over the information they access.
 - Use of MbPT information systems to store, process, download, or transmit data that can be construed as biased (politically, religiously, racially, ethnically, etc.) or supportive of harassment is strictly prohibited.
 - Downloading, redistribution and printing of copyrighted articles, documents, or other copyrighted materials to MbPT information systems are strictly prohibited.
 - Receiving, printing, transmitting, or otherwise disseminating proprietary data, company secrets, or other confidential information in violation of company policy or proprietary agreements is strictly prohibited.
 - Downloading inappropriate material such as picture files, music files, or video files for personal use is strictly prohibited.
 - Users should terminate active sessions when finished, unless they can be secured by an appropriate locking mechanism, e.g. a password protected screen saver.
 - Users are prohibited from changing the configuration, removing, de-activation or otherwise tampering with any Virus and Malicious Software prevention / detection and software that has been installed on systems used by them.
 - Users shall follow a clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities in order to reduce the risks of unauthorized access, loss of, and damage to information during and outside normal working hours.
 - MbPT's resources shall not be used for commercial or personal use. Resources include but are not restricted to faxes, telephone, printers, scanners, copiers, or electronic media. The commercial and personal use includes commercial or personal advertisements, solicitations, or promotions of any outside business, political lobbying or promoting political activities, or any commercial purpose other than official MbPT's business activities.
 - Unauthorized use of photocopiers and other reproduction technology (e.g., scanners,

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	120
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

digital cameras) should be prevented.

- Documents containing sensitive or classified information should be removed from printers immediately.

Introduction of unauthorized copies of licensed software and hardware

- Introduction of unauthorized copies of licensed software and hardware (piracy/copyright and patent infringement) to MbPT information resources and the copying of such material is prohibited.
- The storage, processing, or transmittal of unauthorized copies of licensed software and hardware (piracy/copyright and patent infringement), by MbPT personnel associates is strictly prohibited.

Introduction of open-source, freeware and shareware applications

- Introduction of Open-source, Freeware and Shareware Applications whether downloaded from the Internet or obtained through any other media to MbPT information systems will be subject to a formal evaluation and approval process.
- Open-source, Freeware and Shareware Applications should be evaluated and tested by the Information Security Management Representatives and System Administrators before installation on MbPT Information Resources. They shall verify the legal implications of using the same in MbPT information systems.
- Open-source system shall be used for monitoring and reviewing any production systems after evaluation and approval of the same by the Information Security Management Representatives.

Introduction of Pornographic Material

- Introduction of pornographic material into any MbPT information systems environment is strictly prohibited. The storage, processing, or transmittal of pornographic material on MbPT information systems, by MbPT employees, contractors or associates is strictly prohibited.
- Accessing, Sharing and/or introducing any information using social media shall be as per social media policy.

Due Diligence

- Each user has the responsibility to notify the Information Security Management Representatives immediately of any evidence of or suspicion of any security violation with regard to:

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	121
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

- Unauthorized access to network, telecommunications, or computer systems.
- The apparent presence of a virus on a PC.
- The apparent presence of any information resource prohibited by this policy.
- Apparent tampering with any file for which the user established restrictive discretionary access controls.
- Violation of this policy or any other Information Security policy or procedure by another user, employee, contractor or third party service provider.
- Each user has the responsibility to prevent unauthorized access, including viewing, of information resources in his possession or control (such as portable computer, desktop terminal/computer, printouts or tape media/CD/DVD).
- Each user is responsible for providing access security against relatives, friends and neighbours, customers/clients, vendors, and unknown visitors. In situations where such people should be provided access (e.g., a vendor who has come to install a product or make repairs), then the user should oversee and monitor the actions of the individual given temporary access.

Computer games

Playing games or online computer games in MbPT premises is prohibited. Users should not install any computer games or access any online computer games using MbPT information resources.

Introduction of destructive programs

Introduction of destructive programs (e.g., viruses, self-replicating code) in order to cause intentional damage, interfere with others, gain unauthorized access, or inhibit production to MbPT's information systems, is strictly prohibited.

External services

- All users should limit their usage of external services (e.g., bulletin board, on-line service provider, Internet site, commercial data base) to authorized business purposes only in accordance with this policy, standards, and procedures regarding such usage and as approved by the user's management.
- All users should further comply with the policies, standards, and procedures of the external service (e.g., bulletin board, on-line service provider, Internet site, and commercial database) that they are using

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	122
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

b. Reporting Incidents

- Incident is defined as the occurrence of any exceptional situation that could compromise the Confidentiality, Integrity or Availability of Information and Information Systems of MbPT. It is related to exceptional situations or a situation that warrants intervention of senior management, which has the potential to cause injury or significant property damage. Software malfunctions, virus, theft, etc. and any violations of MbPT's security policies and procedures shall also be considered an incident.
- If any user comes across any exceptional situation as mentioned above he/she should immediately inform the Information Security Management Representatives ISC.
- The reporter's details should be kept strictly confidential and should not be revealed.
- The users should not try and test the weaknesses, since it might be interpreted as misuse of the system.

All the incidents should be escalated as per the defined Incident Management policies and procedures.(refer incident management Policy for more details)

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	123
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

c. Password policy

- Users shall be responsible for all activity performed with their personal user IDs. Users shall not permit others to perform any activity with their user IDs or perform any activity with IDs belonging to other users.
- All user-level passwords (e.g., email, web, desktop computer, etc.) shall be changed periodically (at least once every three months). Users shall not be able to reuse previous passwords.
- Password shall be enforced to be of a minimum length and comprising of mix of alphabets, numbers and characters.
- Passwords shall not be stored in readable form in batch files, automatic logon scripts, Internet browsers or related data communication software, in computers without access control, or in any other location where unauthorized persons might discover or use them
- All access codes including user ID passwords, network passwords, PINs etc. shall not be shared with anyone, including personal assistants or secretaries. These shall be treated as sensitive, confidential information
- All PINs (Personal Identification Numbers) shall be constructed with the same rules that apply to fixed passwords
- Passwords must not be communicated through email messages or other forms of electronic communication such as phone to anyone.
- Passwords shall not be revealed on questionnaires or security forms.
- Passwords of personal accounts should not be revealed to the controlling officer or any co-worker even while on vacation unless permitted to do so by designated authority.
- The same password shall not be used for each of the systems/applications to which a user has been granted access e.g. a separate password to be used for a Windows account and an UNIX account should be selected.
- The "Remember Password" feature of applications shall not be used.
- Users shall refuse all offers by software to place a cookie on their computer such that they can automatically log on the next time that they visit a particular Internet site
- First time login to systems/services with administrator created passwords, should force changing of password by the user
- If the password is shared with support personnel for resolving problems relating to any service, it shall be changed immediately after the support session.
- The password shall be changed immediately if the password is suspected of being disclosed, or known to have been disclosed to an unauthorized party.

Password Policy: For designers/developers of applications/sites

- No password shall be traveling in clear text; the hashed form of the password should be used. To get around the possibility of replay of the hashed password, it shall be used along with a randomization parameter
- The backend database shall store hash of the individual passwords and never passwords in

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	124
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

readable form.

- Password shall be enforced to be of a minimum length and comprising of mix of alphabets, numbers and characters.
- Users shall be required to change their passwords periodically and not be able to reuse previous passwords.
- For Password Change Control, both the old and new passwords are required to be given whenever a password change is required.
- Policy for constructing a password: All user-level and system-level passwords must conform to the following general guidelines described below.
- The password shall contain more than eight characters.
- The password shall not be a word found in a dictionary (English or foreign).
- The password shall not be a derivative of the user ID, e.g. 123.
- The password shall not be a slang, dialect, jargon etc.
- The password shall not be a common usage word such as names of family, pets, friends, co-workers, fantasy characters, etc.
- The password shall not be based on computer terms and names, commands, sites, companies, hardware, software.
- The password shall not be based on birthdays and other personal information such as addresses and phone numbers.
- The password shall not be a word or number pattern like aaabbb, qwerty, zyxwvuts, 123321, etc. or any of the above spelled backwards.
- The password shall not be any of the above preceded or followed by a digit (e.g., secret1, 1secret).
- The password shall be a combination of upper and lower case characters (e.g. a-z, A-Z), digits (e.g. 0-9) and punctuation characters as well and other characters (e.g., !@# \$%^&*()_+|~-=\`{}[]:;'\<>?,./).
- Passwords shall not be such that they combine a set of characters that do not change with a set of characters that predictably change.

Suggestions for choosing passwords:

- Passwords may be chosen such that they are difficult-to-guess yet easy-to remember. Methods such as the following may be employed:
- String together several words to form a pass-phrase as a password.
- Transform a regular word according to a specific method e.g. making every other letter a number reflecting its position in the word.
- Combine punctuation and/or numbers with a regular word.
- Create acronyms from words in a song, a poem, or any other known sequence of words. Bump characters in a word a certain number of letters up or down the alphabet. Shift a word up, down, left or right one row on the keyboard.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	125
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Responsibilities:

- All individual users having accounts for accessing systems/services in the domain, and system/network administrators of servers/ network equipment's shall ensure the implementation of this policy.
- All designers/developers responsible for site/application development shall ensure the incorporation of this policy in the authentication modules, registration modules, password change modules or any other similar modules in their applications.

Compliance:

- Personnel authorized as Internal Audit shall periodically review the adequacy of such controls and their compliance.
- Personnel authorized as Application Audit shall check respective applications for password complexity and password policy incorporation.

Refer: MbPT ISMS -L2 – ISMS control Policy – Access Control Policy – System and application access control.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	126
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

d. Virus protection policy

- Users should not open any files attached to an e-mail from an unknown, suspicious or untrustworthy source.
- Users should not open attachments that are from an unknown or non-trusted source. Attachments with extensions such as '.exe', '.vbs', etc should be blocked by the anti-virus engine.
- Users should not open any files attached to an e-mail whose subject line is questionable or unexpected. If there is a need to do so, they should always save the file to the hard drive before doing so.
- Users should delete chain/junk e-mails and not forward or reply to any of the chain/junk mails. These types of e-mail are considered Spam, which is unsolicited and intrusive that clogs up the network.
- Users should exercise caution when downloading files from the Internet, and should download only from a legitimate and reputable source. Verify that an anti-virus program checks the files on the download site. If you're uncertain, don't download the file at all.
- Users should back up the files on a regular basis. If a virus destroys the data files, they can be replaced with the back-up copy. The backup files should be stored in an off-site location.
- When in doubt, always follow on the side of caution and do not open, download, or execute any files or e-mail attachments.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	127
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

e. Physical security

- Users should not allow any unauthorized person to enter MbPT network switch room.
- Users should not enter into MbPT without ID badges and they should always display their ID badges within MbPT.
- Users should disclose voluntarily all their belongings while entering and going out of MbPT to the security personnel.
- Smoking, drinking alcohol is strictly prohibited inside MbPT.
- Users should not take in or out any equipment from MbPT, without authorization.
- Users should adhere to all physical security standards to be followed in MbPT

Controls for infrastructure facilities and physical assets

- The facility chosen to locate information assets will be suitably protected from physical threats aimed at unlawful or unauthorized access, manmade disasters like vandalism or theft, natural disasters like fire, flood etc., and will ensure adequate infrastructure availability and allow for capacity expansion.
- Controls specified for public areas will include:
 - Security Guard to discourage vandalism.
 - External people will be allowed to enter in the premises only with authorized permission and it will be documented in the register maintained by the security guards.
- Controls specified for Restricted Areas will include:
 - A 24 x 7 human security guard will be kept posted to control access of the building premises.
 - The network cabinets / closets and server racks will be locked at all times.
 - The console port access to networking equipment will be secured at all times.
 - Access permissions shall be provided on approval as per company MbPT policy.
- Additional controls for critical assets:
 - The network switch room or any other critical assets will not be located in the basement of the building.
 - Electronic storage or transmitting devices will not be permitted within such facilities without prior permission.
 - The use of hard disks/ CDs /flash drives /recording devices will be restricted and logged within such facilities.
 - A contact list of essential resources and services will be prepared and maintained up-to-date. The list will be posted in clear view at the critical facilities. The list will include:
 - Details of the critical staff and support teammembers
 - Local police

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	128
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

- Local fire department
- Local Hospital
- Contact numbers of IT services provider

Visitor restrictions

- Access to visitors will be logged and kept with the Security.
- It is desirable that visitors /Contractors be restricted at the reception area only. If that is not feasible, the visitors /Contractors will be escorted at all times.

Visitor access shall be provided on Approval as per MbPT Visitor access policy

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	129
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

f. Handling confidential information

- Confidential/restricted information transmitted over any communication network should be sent in an encrypted form.
- Confidential information not being actively used, when stored or transported in computer-readable storage media (such as magnetic tapes, floppy disks or CDs), shall be encrypted.
- The strength of the encryption algorithm to be used in a given situation should be based on the classification of the data to be encrypted. (**Refer:** MbPT ISMS - L2 - Policy - 1 - Asset Management Policy)
- Use of electronic signatures on critical documents should be done with extra care and diligence. Employee handling the task should be responsible for the authenticity and integrity of the information carrying electronic signatures.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	130
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

g. Use of office equipment

Telephone

- Employees should not reveal sensitive or classified information over the telephone unless the telephone lines have been specifically secured for this purpose – for example through the use of encryption.
- Employees should not enter into the conversation or reveal any information over the telephone where the identity of the caller cannot be determined.
- Employees should not discuss confidential matters or reveal confidential/ classified information in public places and/or outside MbPT premises.
- Employees should not reveal or store confidential messages on answering machines or voice-mail services.
- All parties on a telephone call should be notified in advance if the call is to be recorded.

Fax Machines

- Sensitive or confidential information should be faxed only, when a more secure means of communication is not available. Both the sender of the information and the intended recipient should authorize the transmission of the information before the transmission.
- All fax messages should be classified as per Asset Classification guidelines and should be handled accordingly.
- Users who are responsible for receiving confidential fax messages should co-ordinate with the sender to ensure that they are present at the machine at the time of delivery.
- Users should not leave the fax messages near the fax machine or near desktops unattended.
- Any fax received in error should be destroyed and its sender notified, wherever possible.

Modems/Data Cards

- Modems should not be attached to workstations.
- Laptop users should not connect to the public domain using the internal modems in laptops or data cards and be connected to MbPT network at the same time. The internal network connectivity should be disconnected before the modem/data card is enabled.
- No data transfer should take place via a modem/data card when connected to MbPT networks

Desktops and Laptops

- In events where confidential or restricted data needs to be stored on laptops, the data on laptop hard disks should be kept encrypted using at least 128 bit encryption application.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	131
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

- PCs with Confidential data and all laptops will have a power-on password when initially "booting-up" the system, wherever possible.
- Laptops should not be left unattended. They should be kept locked to the desk or under lock and key when user has to leave office without laptop.
- The folders or disk drives in individual PC's or laptops should not be shared unless authorized. All PCs and laptops, containing confidential data should not have any open shared folders.
- Use of CDs, DVDs, USB drives, floppies and other removable media on laptops and desktops should be disallowed by default and enabled only on authorization from the Department Head.
- The virus definition files on all desktops and laptops should be kept updated.
- Users need to return the desktop/laptop to Department Head/ IT team on their separation or retirement and should not handover it to anyone else within the department/organization.
- All data on desktops or laptops should be erased in the event of change of desktop or laptop custodians unless authorized by Team Lead.
- The Laptop/Desktop should not be used for personal profit or commercial activities.
- Physical Sharing of Laptop is strictly prohibited.
- Each user will be responsible for the applications or services used through his / her Laptop/Desktop.
- Installing any software by user is strictly disallowed / prohibited. In the event or requirement, user should take the prior permission of Department Head before installing any utility software.
- Upon delivery of the laptop, it becomes the user's personal property although MbPT will maintain general warranty support such as deemed by the manufacture.
- User shall not be allowed to upgrade the Laptop/Desktop without the knowledge of Department Head.
- Each User is responsible for any loss or damage to the laptop computer and software.
- If the laptop malfunctions, the user has to contact Department Head. The User should not attempt to repair the laptop or sending it to any vendor for repair.
- Users should lock their Laptops/Desktops while leaving the workstation.
- Users should not intentionally write, generate, compile, copy, collect, propagate, execute or attempt to introduce any computer code designed to self replicate, damage or otherwise wilfully commit fraud and hinder

the performance of or access to MbPT 's information system assets.

- Users shall not download any shareware or freeware directly from the Internet without the

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	132
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

prior approval from Department Head. After approval, users shall scan the software for virus, prior to its use.

- Users should always switch off their Laptops/Desktops (instead of ‘Hibernate/Standby’) before leaving the office and should always carry them in Laptop Bags provided with the Laptop.

Handheld devices

- Department Head will supply the Hand Held devices and is responsible for managing the security of the devices.
- Upon delivery of the devices, it becomes the user’s responsibility although MbPT will maintain general warranty support such as deemed by the manufacturer.
- Physical sharing of devices is strictly prohibited.
- The User is responsible for any loss or damage to the devices. The User is required to pay all repair/replacement charges that are the result of the above mentioned loss or damage.
- If the device malfunctions, the user has to contact Department Head. The User should not attempt to repair the hand held device or send it to any vendor for repair.

Printer and photocopying machine usage

- Making additional copies of or printing of extra copies of secret, confidential, or private information shall not take place without the advance permission of the information owner.
- Whenever additional copies of sensitive information are made the number of copies and recipients of these copies shall be recorded in a log.
- Each of the recipients shall be informed that further distribution or additional copying may take place only after the information owner’s permission has been obtained.
- Printing excess photo copies of documents, files, data, or programs should be avoided.
- If a printer/ photocopying machine jams or malfunctions when all users are making copies of secret information, they shall not leave the machine until all copies of the information are removed from the machine or destroyed beyond recognition.
- Waste papers containing confidential data shall be destroyed using the paper shredder.
- Prior to sending any secret, confidential or private information to a third party for copying, printing, formatting, or other handling, it shall be ensured that the third party signs a non-disclosure agreement.
- Private and confidential information shall be shipped or sent through internal or external mails in a sealed opaque envelope marked “To be opened by Addressee only”.
- The Peripherals (like Printers, Scanners, etc) should strictly be used for Official purpose only.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	133
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

- Peripherals shall be located where they will be free from damage by water, fire or other disasters.
- Only authorized persons will be given access to the peripherals.
- Each Department would be responsible for peripheral allocated to them.
- If any peripherals malfunction, the user has to contact Department Head. The User should not attempt to repair the peripheral themselves or send it to any vendor for repair.

Unattended user equipment

- Users should lock the terminals when they are away from the desks.
- Screen savers should be set to activate within 3 minutes of inactivity.
- The users before leaving for the day should ensure that they have logged off all servers and have shut down their equipment/desktop.
- Users should not remove and dump the Desktops/Laptops etc if not used. The same should be surrendered

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	134
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

h. Inappropriate Internet use

- The use or attempt to initiate such activities using MbPT 's computing facilities or equipment leading to abusive, unethical or “inappropriate” use of the Internet are considered grounds for disciplinary, legal and/or punitive actions, including termination of employment. Examples of prohibited employee Internet use include, but are not limited to, the following:
 - Introduce material considered indecent, offensive, or is related to the production, use, storage, or transmission of sexually explicit or offensive items on the company's network or systems, using Internet.
 - Conduct illegal activities, including gambling, access or download pornographic/illegal material.
 - Solicit for any purpose which is not expressly approved by MbPT management.
 - Use MbPT logos or materials in any web page or Internet posting unless it has been approved, in advance, by MbPT management. Reveal or publicize proprietary or confidential information. Represent personal opinions as those of the company.
 - Use software files, images, or other information downloaded from the Internet that has not been released for free public use.
 - Use of any Internet software (Instant Messengers, Download tools, Online Music software, etc.) that are not approved by management for use.
 - Upload or download commercial software in violation of its copyright.
 - Make or post indecent remarks like “Flaming” (e.g. malicious written attacks directed at someone) or similar written attacks.
 - Download any software or electronic files without reasonable updated virus protection measures in place.
 - Intentionally interfere with the normal operation of any MbPT Internet gateway.
 - Attempt to gain illegal access to remote systems on the Internet.
 - Attempt to inappropriately Telnet to or port scan remote systems on the Internet.
 - Establish Internet or other external network connections that could allow non-MbPT users to gain access into MbPT's systems and information assets.
- Spoofing the identity of another user on the Internet or on any of MbPT communications system is forbidden.

Implied restrictions on Internet

- Users using MbPT's computers on discovering that they have connected with a web site that contains potentially offensive material should immediately disconnect from that site.
- Users should be aware that MbPT accepts no liability for the exposure to offensive material that they may access via the Internet.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	135
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

The ability to connect with a specific web site does not in itself imply that users of MbPT's systems are permitted to visit that site.

i. Review by Management

- At any time and without prior notice, MbPT's Organization reserves the right to examine electronic mail messages, personal files on computers, web browser cache files, web browser bookmarks, and other information stored on or passing through the company's computers. All transactions done over the Internet will be logged. These logged transactions will be used for analysis and may be audited.

j. Restrictions on posting MbPT information on social media

- At Users should not place the company's information or material (software, internal memos, etc.) on any publicly accessible Internet computer, which supports anonymous FTP or similar services, unless the CISO has first approved the posting of these materials.

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	136
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

k. Violations

- All users shall adhere to their security responsibilities as outlined in this document and in the IT Security procedures. They are expected to make themselves familiar with the policies, procedures, standards and guidelines that are applicable to them. All violations of any policy shall be reported to the Information Security Management Representatives. He shall classify the violation, coordinate with appropriate personnel and take necessary action on the concerned person.

Violation classification

- Violations shall be categorized into three levels as follows:
 - **High Severity:** The security violations, which can compromise, the security of critical IT/Non-IT equipments or confidential information assets or, to the extent that it can cause devastating impact to the operations of the organization is classified as High Severity violation.
 - **Medium Severity:** The security violations, which can compromise, the security of critical IT/Non-IT equipments or restricted information assets or, to the extent that it can cause significant impact to the operations of the organization is classified as Medium Severity violation.
 - **Low Severity:** The security violations, which can compromise, the security of non-critical IT/Non-IT equipments or internal information assets or, to the extent that it can cause nuisance impact to the operations of the organization is classified as Low Severity violation.

Disciplinary action

- A staggered approach shall be followed in taking disciplinary action against the employee on non-compliance. Employees shall initially be let off with a lighter penalty (e.g., a reprimand) till the security culture is established in MbPT. Implementation may thus be done in the following three steps:
 - Step 1 (1st 6 months): Counselling
 - Step 2 (Next 3 months): Verbal Reprimand and Written Memo
 - Step 3 (Subsequently): Any of the punitive actions mentioned below
 Punitive actions shall be taken according MbPT's Organization Conduct Rules

l. Execution responsibilities

The users of MbPT who are using information resources are responsible for implementing these policies and procedures mentioned in this section

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	137
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

Social Media Policy

Policy

This policy provides guidance for employee use of social media, which should be broadly understood for purposes of this policy to include blogs, wikis, microblogs, message boards, chat rooms, electronic newsletters, online forums, social networking sites, and other sites and services that permit users to share information with others in a contemporaneous manner.

Scope and Applicability

The information security policy applies to all MbPT employees & employees of enabling functions including Network and Data Centre Operations, Application development and testing, Human Resource, CISO, Facility team and Internal Audit at MbPT, regardless of position.

The policy shall also be applicable to all external/ third party personnel (i.e. vendors, third party resources, consultants, interns, contractors employed with MbPT and clients/ customers visiting MbPTs office locations who engage in work and have access to MbPT's information or information processing facilities.)

Procedures

The following principles apply to professional use of social media on behalf of MbPT as well as personal use of social media when referencing MbPT.

1. Employees need to know and adhere to the [MbPT Code of Conduct, Employee Handbook, and other company policies] when using social media in reference to MbPT.
2. Employees should be aware of the effect their actions may have on their images, as well as MbPT image. The information that employees post or publish may be public information for a long time.
3. Employees should be aware that MbPT may observe the content shared and information made available by employees through social media. Employees should use their best judgment in posting material that is neither inappropriate nor harmful to MbPT, its employees, or customers.
4. Although not an exclusive list, some specific examples of prohibited social media conduct include posting commentary, content, or images that are defamatory, pornographic, proprietary, harassing, libelous, or that can create a hostile work environment.
5. Employees are expected not to publish, post or release any information that is considered confidential or not public. If there are questions about what is considered confidential, employees should check with the Human Resources Department and/or supervisor.
6. Social media networks, blogs and other types of online content sometimes generate press and media attention or legal questions. Employees should refer these inquiries to authorized MbPT

 MUMBAI PORT AUTHORITY	Department	MANAGEMENT	Page No.	138
	Title	IMS APEX MANUAL	Date	03-02-2020
	Section 5	INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES	Revision	00

spokespersons.

7. If employees encounter a situation while using social media threatens to become antagonistic, employees should disengage from the dialogue in a polite manner and seek the advice of a supervisor.
8. Employees should get appropriate permission before referring to or posting images of current or former employees, members, vendors or suppliers. Additionally, employees should get appropriate permission to use a third party's copyrights, copyrighted material, trademarks, service marks or other intellectual property.
9. Social media use shouldn't interfere with employee's responsibilities at MbPT. MbPT computer systems are to be used for business purposes only. When using MbPT computer systems, use of social media for business purposes is allowed (ex: Facebook, Twitter, blogs and LinkedIn,Whatsapp), but personal use of social media networks or personal blogging of online content is discouraged and could result in disciplinary action.
10. Subject to applicable law, after-hours online activity that violates the company's Code of Conduct or any other company policy may subject an employee to disciplinary action or termination.
11. If employees publish content after-hours that involves work or subjects associated with MbPT, a disclaimer should be used, such as this: "The postings on this site are my own and may not represent MbPT positions, strategies or opinions."
12. It is highly recommended that employees keep MbPT related social media accounts separate from personal accounts.

Note No. #1

MUMBAI PORT AUTHORITY
Mechanical and Electrical Engineering Department
Materials Management Division

Sub: MbPT Apex Manual for ISO 9001:2015 QMS, IS
14001:2015 EMS and ISO 27001:2013 ISMS

MbPT Apex manual for ISO 9001:2015 QMS, ISO 14001:2015 EMS and ISO 27001:2013 ISMS is attached herewith.

2. Proposal for approval of MbPT Corporate Quality Objectives for the year 2021-22 has already been put up in E-office through file no. 7663 initiated on 17.05.2021. Currently, the E-office file is with GAD since 31.05.2021. Upon approval by the Chairman, the same will be incorporated in the Apex Manual.
3. Only after the approval of Apex Manual and Corporate Quality Objectives for the year 2021-22, internal audit and Management Review can be conducted. Before conducting the stage-II external audit for awarding ISO certifications, approval of Apex Manual is necessary.
4. In view of above, the combined Apex Manual for ISO 9001:2015 QMS, ISO 14001:2015 EMS and ISO 27001:2013 ISMS is submitted herewith for approval of the Chairman.
5. After incorporation of the approved MbPT Corporate Quality Objectives for the year 2021-22 and approval of Apex Manual in E-office, physical signature of the respective Management Representatives and the Chairman will be obtained on the Apex Manual for uploading in the website.

Materials Manager	Harbour Master	Jt.
Director		
(ISO 9001:2015 QMS)	(ISO 14001:2015 EMS)	(ISO 27001:2013 ISMS)

Chief Mechanical Engineer

Dy. Conservator

Dy. Chairman

Chairman



16/06/2021 4:03 PM

VINAY PRAKASH DUBE
(ASSTT. EXE. ENGINEER MEED)

Note No. #2

18/06/2021 4:34 PM

R. VENKATSUBRAMANIAN
(SR. DY. MATERIALS MANAGER MM)

Note No. #3

Apex Manual recommended for approval.



23/06/2021 12:12 PM

A.R. HAZARNIS
(MATERIALS MANAGER MM)

Note No. #4

Recommended for approval

30/06/2021 5:22 PM

BALASAHEB VINAYAK PAWAR
(HARBOUR MASTER MARINE)

Note No. #5

The Apex Manual comprises of

Section 2 - Common Procedures [\(Page 12 -31 \)](#)

Section 3 - Quality Specific Policies and Procedures ([Page 32-44](#))

Section 4 - Environment Specific Policies and Procedures ([Pg 45](#) - 62)

The Header will be replaced as Section 4 "Environment Specific Policies and Procedures " instead Section 5 "INFORMATION SECURITY SPECIFIC POLICIES & PROCEDURES"

Section 5 - Information Security Specific Policies & Procedures ([Pg 63-206](#))

- Information Security Org structure, Roles and responsibilities (Governance Structure [Pg 68 - 73](#))
- Information Security Policy ([Pg 74](#))
- Information Security Objective ([Pg 75](#))
- Information Security Management System (ISMS) Scope of application ([Pg 76](#)) ,Exclusions are ([Pg 77](#)) Information Assets ([Pg 79](#))

The Procedure for Information Risk assessment and Treatment ([Pg 80-85](#)) >the Statement of Applicability ([Pg 86 - 106](#))

Information is an asset which, like other important business assets, has a value to the organization and consequently needs to be protected. Therefore, MbPT recognizes its information assets as a significant and valuable resource. The MbPT, information security policy provides management direction and support to ensure protection of MbPT's information assets, and to allow access, use and disclosure of such information in accordance with appropriate standards and laws. The information security objectives for MbPT and its enabling functions. This Policy document will be reviewed at least annually by the Leadership and CISO or in events of any significant changes (i.e. change in operations change in technology, regulatory changes, major security incidents) in the existing information security environment affecting policies and procedures. The policy owner will be responsible to make the changes to

the policy document.

The ISC will be responsible to approve the changes to the policy. The Information Security Policies like [Mobile Device Policy](#) , Human resource Security ([Pg 114 - 118](#)) , Asset Management ([Pg 119 - 126](#)) , Access Control ([Pg 127 - 144](#)) , IT Hardware Management ([Pg 145 - 166](#)) , System acquisitions development and maintenance ([167 - 169](#)) . Secure system engineering principles (Outsourcing , Testing , Incident Reporting , other Policies [170-206](#))

The Stage 2 audit for ISMS is Scheduled on 12th of July 2021 .

Approval of Chairman is requested to the [Para 5 Note #1](#)

05/07/2021 10:43 AM



V.B.S. VENKATESHWARA RAO
(JT.DIRECTOR_PNR)

Note No. #6

Recommended for approval please.



08/07/2021 10:53 AM

MANAS MANDAL
(CHIEF MECHANICAL ENGINEER MEED)

Note No. #7

Approved as proosed



12/07/2021 3:13 PM

RAJIV JALOTA
(CHAIRMAN MBPT)

Note No. #8

12/07/2021 4:58 PM

MANAS MANDAL
(CHIEF MECHANICAL ENGINEER MEED)

Note No. #9

13/07/2021 1:43 PM

A.R. HAZARNIS
(MATERIALS MANAGER MM)

