## DOCUMENT REVISION HISTORY

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Author(s)</th>
<th>Revision Notes</th>
<th>Reviewed by</th>
<th>Approved by</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0</td>
<td>31-Dec-2013</td>
<td>Mr. Rajesh S. Chandragade</td>
<td>Initial</td>
<td>Mrs. Anuradha H. Sharma, Director/ MR</td>
<td>Mr. T. S. Balasubramanian Member (Finance)</td>
</tr>
<tr>
<td>0.1</td>
<td>28-Aug-2014</td>
<td>Mr. Rajesh S. Chandragade</td>
<td>Updation of 4) Information Security Objective 5) Communication of Information Security Policy.</td>
<td>Mrs. Anuradha H. Sharma, Director/ MR</td>
<td>Mr. T. S. Balasubramanian Member (Finance)</td>
</tr>
<tr>
<td>0.2</td>
<td>28-Dec-2015</td>
<td>Mr. Rajesh S. Chandragade Assistant Director-IT.</td>
<td>Yearly Review – revised objectives for year 2016</td>
<td>Mrs. Anuradha H. Sharma, Director/ MR</td>
<td>Mr. T. S. Balasubramanian Member (Finance)</td>
</tr>
<tr>
<td>0.3</td>
<td>18-Jul-2016</td>
<td>Mr. Rajesh S. Chandragade Assistant Director-IT.</td>
<td>Continual Improvement added in first para.</td>
<td>Mrs. Anuradha H. Sharma, Director/ MR</td>
<td>Mr. T. S. Balasubramanian Member (Finance)</td>
</tr>
<tr>
<td>0.4</td>
<td>06-Jul-2017</td>
<td>Mr. Rajesh S. Chandragade Assistant Director-IT.</td>
<td>Yearly Review – At Para 4 revised objectives and their completion dates for the year 2017.</td>
<td>Mrs. Anuradha H. Sharma, Director/ MR</td>
<td>Mr. T. S. Balasubramanian Member (Finance)</td>
</tr>
<tr>
<td>0.5</td>
<td>22-Aug-2017</td>
<td>Mr. Rajesh S. Chandragade Assistant Director-IT.</td>
<td>At Para 4.2 the VAPT date is revised to 31.12.2017</td>
<td>Mrs. Anuradha H. Sharma, Director/ MR</td>
<td>Mr. T. S. Balasubramanian Member (Finance)</td>
</tr>
</tbody>
</table>

## DISTRIBUTION LIST
- Management Representative (Master Copy)
- Others on request – Copy
**TABLE OF CONTENTS**

1  PURPOSE ..........................................................................................................................3
2  PHYSICAL ASSETS OF TAMP ..................................................................................3
3  INFORMATION ASSETS OF TAMP ........................................................................4
4. INFORMATION SECURITY OBJECTIVE .................................................................. 4
5. COMMUNICATION OF INFORMATION SECURITY POLICY .......................... 5
1. PURPOSE:

**Information Security Policy of TAMP**

TAMP is committed to ensure Confidentiality, Integrity, Availability and Security of its Physical and Information Assets and its continual improvement at all times for serving the needs of the Major Port Trusts, Private Terminal Operators thereat, Port users and Government.

Information and Information Security requirement plays an important role in realizing the organizational goal at TAMP. The Information Security Management System (ISMS) is an enabling mechanism for information sharing in a safe and secure way so as to protect Confidentiality, Integrity and Availability of the Information Asset, for electronic operations and for reducing information-related risks to acceptable levels, which are defined in the Methodology document for Risk Management.

In this policy, “information security” is defined to protect confidentiality, Integrity and Availability of all the business data including the information relating to tariff details right from drafting agenda note till notification of tariff in Gazette of India.

The terms Confidentiality, Integrity & Availability are defined as follows:

**Confidentiality:** This involves ensuring that information is only accessible to those authorized to access it and therefore to preventing both deliberate and accidental unauthorized access to TAMP’s information and proprietary knowledge and its systems including network(s), website(s), and extranet (s) systems.

**Integrity:** This involves safeguarding the accuracy and completeness of information and processing methods and therefore requires preventing deliberate or accidental, partial or complete, destruction or unauthorized modification of either physical assets or electronic data. There must be appropriate contingency included for all critical services like network(s), web site(s), extranet(s) and data backup. TAMP must comply with all relevant data-related legislation in those jurisdictions within which it operates.

**Availability:** This means that information and associated information assets shall be accessible to authorized users when required. The computer network must be resilient and the organization must be able to detect and respond rapidly to incidents that threaten the continued availability of assets, systems and information. There must be appropriate business continuity plans.

2. Physical assets of TAMP: Include (but not limited to) computer hardware, data cabling, telephone systems, filing systems and physical data files.

3. Information assets of TAMP: Include business data and information printed or written on paper, transmitted by post or shown in films, or spoken in conversation, as well as information stored electronically on servers, web site(s), extranet(s), intranet(s), PCs, laptops, mobile phones and PDAs as well as on CD ROMs, floppy disks, USB sticks, backup tapes and any other digital or magnetic media, and information transmitted electronically by any means. In this context “data” also includes the sets
of instructions that tell the system(s) how to manipulate information (i.e. the software: operating systems, applications, utilities, etc).

TAMP’s current strategic business plan and risk management framework provide the context for identifying, assessing, evaluating and controlling information-related risks through the establishment and maintenance of ISMS and to safeguard organizational information assets from potential security breach. A **Security Breach** is any incident or activity that causes or may cause a break down in the availability, confidentiality or integrity of the physical or electronic information assets of TAMP.

TAMP would consider **internal & external issues, needs & expectations of interested parties** in determining the risks and opportunities to ensure that information security management system of TAMP would achieve its intended objectives, prevent, or reduce undesired effects and achieve continual improvement.

In line with the above requirement of commitment to continual improvement TAMP has defined and established an information security objective bearing no. CP-03-ISMS taking due consideration of an internal issue identified in the document, context of organization (CP-02-ISMS) as follows:

**4. Information Security Objective:**

With reference to internal issues of ready access of Business Data to all the staff members of TAMP in the document, Context of the Organization (CP-02-ISMS).

1. To carry out ISMS Awareness Programs for all the staff members and explain them about significance of Confidentiality of Business Data and consequences of compromise of Confidentiality by December 31, 2017.
2. Vulnerability Assessment & Penetration Testing to be completed by December 31, 2017.
3. Physical Security needs to be strengthen by implementing measures such as physical access control - Installation of Biometric device in TAMP by December 31, 2017.

**TAMP would establish and maintain information security risk criteria that include risk acceptance criteria and criteria for performing information security risk assessments.**

In the process TAMP would identify risks associated with loss of confidentiality, integrity and availability of information assets under the scope of ISMS and also identify risk owners. Further TAMP would analyse/assess the potential consequences that would result in case the risks identified are materialized, assess the realistic likelihood of occurrence of risks identified and determine the levels of risk. TAMP on completion of risk analysis would evaluate the information security risks in line with the risk criteria established and arrive at the risk levels to prioritize risk treatment. Based on the risk levels so determined, TAMP may decide any of the four options of risk treatment such as apply the controls, accept the risk, avoid risk and transfer the risk.
As a result & conclusions from risk assessment aforestated, TAMP may decide to apply the controls to mitigate the risk by examining the requirements in Annex A, wherein 114 controls are suggested by ISO 27001:2013 standard. On selection of controls from the illustrative list(Annex A) and elsewhere TAMP would prepare the document, Statement of Applicability, which comprises of controls selected afresh, controls currently implements and excluded controls with due justifications.

Senior Management is responsible for approval of residual risks and the risk treatment plan based on the controls listed in Statement of Applicability.

- Additional risk assessments may, where necessary, be carried out to determine appropriate controls for specific risks. In particular, business continuity and contingency plans, data backup procedures, avoidance of viruses and hackers, access control to systems and information security incident reporting are fundamental to this policy. Control objectives for each of these areas are contained in the ISMS Manual and are supported by supporting Information Security policies and procedures.

- All employees of TAMP and external parties (Contractors and Temporary staff, Vendors and Service Providers, Customers and Visitors) are expected to comply with this policy and with the ISMS that implements this policy. All employees (including temporary staff) accessing information or information processing facilities of TAMP will receive appropriate information security awareness training and re-trainings at periodical intervals.

- The Management Representative (MR) is the Owner of this document and is responsible for ensuring that this policy document is subject to systematic, periodic reviews and subjected to continual improvement. This policy will be reviewed to respond to any changes in the risk assessment or risk treatment plan at least once in a year or in view of any change w.r.t. legal & regulatory requirements, business environment or occurrence of a major information security incident etc.

A current version of this document is available to all TAMP’s staff. It does not contain confidential information and can be released to relevant external parties in prior written consent of MR.

5. Communication of Information Security Policy:

The information security policy is placed in the website of TAMP for the purpose of communication to all interested parties such as vendors, port users, port trusts etc. who are external. The information security policy has also been circulated to all the workforce within the organization.”

Place: MUMBAI
Date: 22-August-2017

(T. S. Balasubramanian)
Member (Finance)
Tariff Authority of Major Ports