PHILIPPINE PORTS AUTHORITY

DEC 2 1 2018

PHILIPPINE PORTS AUTHORITY RECEIVED TIME: 1:00 p.m. DATE: 12-27-18 BY:

PPA MEMORANDUM CIRCULAR NO. 25 - 2018

TO : **All PPA Officials and Employees Others Concerned**

SUBJECT : **Updated PPA Information and Communication Technology (ICT) Security Policy**

1 PURPOSE

This Memorandum Circular (MC) aims to provide a comprehensive Information and Communication Technology (ICT) Security Framework for the Philippine Ports Authority (PPA) and extend support to the State's policy as envisioned and articulated in the National Cybersecurity Plan 2022.

The PPA ICT Security Policy covers established guidelines, procedures, and requirements for the compliance of all concerned to effectively ensure the maintenance of a safe and secure PPA ICT domain as well as to capably preserve and sustain the Agency's information systems' operability and integrity.

2 COVERAGE

This policy applies to all internal and external PPA ICT Users, (i.e., PPA Officials and Employees, clients, contractors, third-party service providers and any other information systems Users).

3 OBJECTIVES

The PPA ICT Security Policy is explicitly designed to:

3.1 Equip PPA's ICT systems, services, facilities and infrastructure with essential protection and unified management from internal and external security threats

3.2 Allow PPA, its officials and employees, to send and receive securely via online transmission of official/confidential information, materials, and documents with sufficient provision for backup storage.

3.3 Enable PPA clients to engage securely in online business transactions with PPA.

3.4 Ensure the uninterrupted and authorized access to PPA's ICT systems, services, facilities and infrastructure.

3.5 Capacitate PPA in maintaining an accurate and up-to-date inventory of all its technology assets, whether connected to the organization's network or not, with the potential to store or process information.

4 GENERAL PROVISIONS

It is the policy of PPA that each of its officials and employees, as a User of PPA ICT Services, Facilities and Infrastructure, as well as the port clientele it serves, is responsible for the security and protection of the Agency's electronic information resources over which he has control. These resources include networks, computers, software, and data. He shall safeguard the resources against threats such as unauthorized intrusions, malicious misuse, or unintentional compromise and shall report immediately to the proper authority any such or similar threats of violation.

5 DEFINITION OF TERMS

To attain a singular and clear understanding of the textual content of the different provisions of the PPA ICT Security Policy, the definition of terms used the drafting of this document is adopted and hereto attached as Annex "A".

6 PPA ICT SECURITY AREAS OF RESPONSIBILITY

To ensure that PPA ICT security is properly safeguarded, specific policy provisions for each area of PPA ICT security are circulated for the awareness and strict observance of all concerned as indicated in the attached annexes listed below:

ANNEX	Item No.	PPA ICT SECURITY AREA OF RESPONSIBILITY
B	6.1	Access Control
C	6.2	User Account Management
D	6.3	Server Security
E	6.4	Data Center Security
F	6.5	Database Security
G	6.6	Information Classification
H	6.7	Request for System Update
I	6.8	Information Security Incident

ANNEX	Item No.	PPA ICT SECURITY AREA OF RESPONSIBILITY
J	6.9	Electronic Mail
K	6.10	Internet Security
L	6.11	Virtual Private Network (VPN)
M	6.12	Firewall Security
N	6.13	Remote Access
O	6.14	Audit
P	6.15	Acceptable Use of Computer Equipment

7 SPECIFIC ROLES IN THE PROVISION OF ICT SECURITY

7.1 Information and Communication Technology Department (ICTD)

ICTD shall be responsible for establishing, maintaining, and administering organization-wide Information and Communications Technology security policies, standards, guidelines and procedures. It shall, therefore, be responsible for activities related to these policies such as:

- Information systems risk assessment
- Preparation of information systems security action plans
- Evaluation of information security products
- Conduct of investigations into any alleged computer or network security compromises, incidents or problems

7.1.1 Network/Systems Administrators

Network and Systems Administrators shall:

7.1.1.1 act as information security coordinators and implement appropriate User privileges, monitor access/system control logs related to network administration.

7.1.1.2 be responsible for reporting all suspicious computer and network security-related activities to the ICTD Manager. Whenever system security has been compromised or even if there were justifiable reasons to believe it has been compromised, the Systems/Network Administrator concerned must immediately do any or all of the following:

7.1.1.2.1 Reassign all relevant Passwords.

7.1.1.2.2 Compel every Password on the affected system to be changed at the time of the next login. If this were not possible, a broadcast message must be sent to all Users instructing them to change their respective Passwords.

7.1.1.2.3 Review immediately all changes to User

privileges taking effect since the time of the suspected compromise for any unauthorized modifications.

7.1.2 Database Administrators

Database Administrators for both development and production areas shall:

7.1.2.1 act as information security coordinators and implement appropriate User privileges, monitor access/system control logs related to database administration.

7.1.2.2 be responsible for reporting all suspicious database security-related activities to the ICTD Manager. Whenever database security has been compromised or even if there were justifiable reasons to believe that it has been compromised, the Database Administrator concerned must immediately do any or all of the following:

7.1.2.2.1 Reassign all relevant Passwords.

7.1.2.2.2 Compel every Password on the affected system to be changed at the time of the next login. If this were not possible, a broadcast message must be sent to all Users instructing them to change their respective Passwords.

7.1.2.2.3 Review immediately all changes to User privileges taking effect since the time of the suspected compromise for any unauthorized modifications.

7.2 Responsibility Center (RC) Heads

All RC Heads shall be responsible for ensuring that appropriate Information and Communications Technology security measures are observed in their respective areas. They shall also be responsible for ensuring that all Users within their respective jurisdictions are aware of and compliant with PPA's security policies.

7.3 Users

Users shall be responsible for complying with the herein stated policies and all other PPA policies defining computer and network security measures. They shall report immediately to ICTD any violations to said policies and associated procedures.

8. REPORTORIAL OBLIGATIONS

8.1 It shall be the obligation of every PPA Official and Employee to report to ICTD any violations to the guidelines and procedures set forth in the PPA ICT Security Policy.

8.2 It shall also be every PPA Official's and Employee's responsibility to report any threat to the security, unauthorized intrusion, malicious or unintentional compromise of the PPA ICT resources, including actual or verifiable suspicion of loss or disclosure of sensitive and/or confidential information or data.

8.3 PPA Users shall notify immediately the ICTD of any unusual systems behavior such as missing files, frequent system crash, misrouted messages and other similar occurrences.

9. VIOLATION OF POLICY

Any violations to the provisions set forth in this PPA ICT Security Policy shall not be tolerated and, after proper investigation, may be considered cause for disciplinary action.

10. REPEALING CLAUSE

All issuances inconsistent with the provisions of this Memorandum Circular are hereby modified accordingly. This Memorandum Circular shall take effect immediately.

For implementation, guidance and compliance.

JAY DANIEL R. SANTIAGO
General Manager

Annex A

4.0 DEFINITION OF TERMS

To attain a singular and clear understanding of the textual content of the different provisions of the PPA ICT Security Policy, the definition of terms used in the drafting of this document is, thus, adopted as follows:

TERM	DEFINITION
Active Directory Server	a computer that stores log-in names and Passwords of Users for ensuring system's security
Anti-Virus	a software package designed to identify and remove known or potential computer viruses or any associated software containing, but not limited to, virus definition files
Circuit	method of network access, whether it is through traditional Services Digital Network (ISDN), Frame Relay, etc., or via Virtual Private Network (VPN)/Encryption technologies
Credentials	something you know (e.g., a Password or pass phrase), and/or something that identifies you (e.g. a User name, a fingerprint, voiceprint, retina print), that are presented for authentication
Cybersecurity	the ability to protect or defend an enterprise's use of cyberspace from an attack, conducted via cyberspace, for the purpose of: disrupting, disabling, destroying, or maliciously controlling a computing environment/ infrastructure; or, destroying the integrity of the data or stealing controlled information (as defined by the Committee on National Security Systems (CNSS-4009); the process of protecting information by preventing, detecting, and responding to attacks, (according to the National Institute of Standards and Technology); also termed as cyberspace security, which refers to the preservation of confidentiality, integrity and availability of information in the Cyberspace, (per definition of the International Organization for Standardization or ISO)
Cyberspace	the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form (ISO)

Data Center	a restricted facility used to house computer systems and associated components, such as telecommunications (server) and storage systems. It generally includes redundant or backup power supplies, redundant data communications connections, environmental controls (e.g. air conditioning, fire suppression) and various security devices
Electronic Mail or Email	an electronically transmitted mail. It allows the exchange of electronic messages through the Internet
Encryption	method or process of encoding message or information in such a way that only authorized parties can access it
Executable File	contains a program that is capable of being executed or run in the computer
Firewall	may be hardware devices, software programs or combination of the two for the purpose of protecting a computer network from unauthorized access; typically guards an internal network against malicious access from the outside; may also be configured to limit access of internal Users to the outside
Gateway	a network point that acts as an entrance to another network; it may also be any machine or service that passes information from one network to another network across the Internet
Information and Communication Technology (ICT)	the totality of the means employed to systematically collect, process, store, present and share information. It encompasses computers, telecommunications and office system technologies as well as accompanying methodologies, processes, rules and conventions; (SOURCE: NCC Memo Circular 2001-01: Guidelines in Leasing Hardware, Software, Network and Solution-based ICT Resources)
Information Security Incident	a suspected, attempted, successful or imminent threat of unauthorized access, use, disclosure, breach, modification, destruction of information or an interference with information technology operations
Internet	in generic term, this refers to networks bridged or connected to each other. In more specific term, Internet is a global network of computers that communicate with each other via Transmission Control Protocol/Internet Protocol (TCP/IP) and is publicly accessible and administratively uncontrolled
Internet Hosting	a business of housing, serving and maintaining files for one or more websites
Internet Services	cyber/digital utilities/services running through devices that are reachable from other devices across a network. Major internet services include Domain Name System (DNS),

	File Transfer Protocol (FTP), HyperText Transfer Protocol (HTTP), etc.
Intranet	a company-wide web accessible only to an organization's members, employees or others with such given authorization
Mailbox	storage space that contains an individual's electronic mail messages
Operating System	commonly abbreviated as either *OS* or *O/S* and described as an interface between hardware and User; is responsible for the management and coordination of activities and the sharing of the resources of the computer. OS acts as a host for computing applications that are run through the machine. As a host, one of the purposes of an operating system is to handle the details of the operation of the **hardware**
Risk	any factors that could affect confidentiality, availability, and integrity of an organization's key information assets and systems
Router	a physical device that joins multiple networks together
Sensitive Information	any data, materials or facts that could be considered as damaging to the PPA or its customers' peso value, reputation, or market standing
Server	computer or device on a network that manages network resources such as storing files, managing one or more printers, managing network traffic or processing database queries
Spam	any unsolicited bulk messages received through the Internet that may include chain letters, items for sale/advertisements, get-rich-quick scams or any other unwanted emails that people often receive
Third Party	an entity that markets an accessory hardware product for a given brand of computer equipment or provides services/solutions for addressing ICT issues/concerns. This may also be referred to as the contractor, vendor or application service provider
User Authentication	a method by which the User of a wireless system can be verified as a legitimate User independent of the computer or operating system being used
Web Browser	a software used to make contact with websites. Examples are the Internet Explorer, Mozilla Firefox, etc.

Annex B

6.1 ACCESS CONTROL

PPA ICT Services, Facilities and Infrastructure shall be accessed for official business purposes only, and should not be used for any unlawful activities or for any personal and financial gains by both its authorized internal Users, (officials and employees), and external Users, (clients and other interest groups).

The exercise of IT-related access control in PPA currently covers two responsibility areas, namely: ICT Systems and ICT Network. The pertinent provisions in this regard are as follows:

6.1.1 Access to ICT Systems

Access to PPA ICT Systems, inclusive of all electronic information, shall be appropriately secured against breaches of confidentiality and integrity of information or interruptions as to their availability. Access mechanism must incorporate authentication controls using a unique Username/User ID and Password assigned to each authorized User. The following guidelines are, thus, provided:

6.1.1.1 Username/User ID must uniquely identify a single User. On a per system/application basis, re-use of Username/User ID by a different User and/or assignment of multiple Usernames/User IDs to a single User are disallowed and strictly prohibited.

6.1.1.2 Naming standards for each application/system shall be used and documented.

6.1.1.3 Users shall be responsible for all activities, known or unknown, related to the use of their respective IDs.

6.1.1.4 A completely accomplished and signed User Account Request or UAR, (see Annex A – ICTD Form 001) and Request for System Update or RSU (see Annex B – ICTD Form 002), must be submitted for all requests concerning authorization on the corresponding roles/privileges of a new Username/User ID. These forms, as with the case of ICTD Forms 003 and 004, are downloadable from the PPA website at ***www.ppa.com.ph***.

6.1.1.5 Anonymous Username/User ID will not be allowed.

6.1.1.6 Passwords must be sufficiently complex (avoid names, places, birthdays, company slogans, dictionary words, etc.) and must

bear/comply with the following:

6.1.1.6.1 the minimum Password length employed on all accounts should be eight alphabetic and non-alphabetic characters (numeric or symbol).

6.1.1.6.2 the system shall require Password changes for a minimum period of one month and a maximum of six (6) months.

6.1.1.6.3 Passwords must contain both upper and lowercase characters.

6.1.1.7 Users shall be compelled to change their Password upon initial use/receipt and upon Password reset.

6.1.1.8 User Password must not be scripted nor hard-coded (i.e. placed in a function key, macro, or using "Save Password on next connect").

6.1.1.9 Users shall change their Passwords immediately in case the Password has been compromised.

6.1.1.10 Users shall not ask for or provide Password disclosure for any accounts managed by the PPA Systems.

6.1.1.11 Users must be cautious in writing Passwords and leaving them where others could discover them, an action that is strictly prohibited.

6.1.1.12 All default Passwords provided by software or hardware must be changed once implemented on production systems or development systems attached to the network or internet.

6.1.1.13 Users and System Administrators who maintain multiple accounts must use different Passwords for each account.

6.1.1.14 The number of consecutive unsuccessful access attempts will be limited to only three. Once locked out, only the System Administrator can unlock the account.

6.1.1.15 Successful logons shall display the date and time of the last logon to the User.

6.1.1.16 Users shall not leave a terminal that has an active log-on session connected to it unattended and unprotected.

6.1.2 **Access to ICT Network**

6.1.2.1 Only authorized Network Administrators shall do all network configurations. Likewise, access to all network devices shall be strictly limited to authorized technical personnel only unless unrestricted access is granted approval by ICTD to an external party.

6.1.2.2 A completely accomplished and signed RSU should be submitted to the Operations Resources and Services Division (ORSD) for all changes to computer networks, (including, but not limited to loading new communications software, changing network addresses, reconfiguring routers and the like). All emergency changes to the network must only be made by and reported immediately to the authorized personnel/ Network Administrators.

6.1.2.3 All internal network devices, (i.e., routers, firewalls, access control servers, etc.), shall have unique Passwords kept in a secure encrypted form or other access control mechanisms.

6.1.2.4 PPA's information and communication systems shall restrict access to the computers that Users can reach over the PPA's networks. These restrictions shall be implemented via routers, gateways and other network devices.

6.1.2.5 Devices considered or known generally for undesirable/malicious transmissions are to be blocked from access to the PPA network.

6.1.2.6 The PPA reserves the right to audit networks and systems on a periodic basis to ensure compliance with the above-stated policy.

6.1.2.7 The Network Administrators shall maintain a current inventory of PPA's network facilities including network phones, intranets and internet. All interfaces between PPA and third party networks shall be secured according to the requirements of the external access procedure (see Section 6.13 of PPA ICT Security Policy).

6.1.2.8 All connections to the internal computer data network shall employ User authentication.

6.1.2.9 Firewall(s) must be in place such that access to connected systems shall be restricted to authorized Users only. All devices hosted on or connected to the PPA network must meet the security requirements of this policy and associated policies and procedures

of the ICT Security framework (Section 6.12).

6.1.2.10 Routers, hubs, modems, and other networking hardware should be strategically located so that these may not be easily tampered with by unscrupulous persons.

6.1.2.11 The Human Resource Management Department (HRMD) is required to submit every 5th day of the month to ICTD a list of personnel who were transferred to another unit as well as those who are no longer connected with the PPA due to retirement, resignation, termination, extended leave of absence or absence without leave (AWOL). Systems/network access rules may be cautiously revised/modified in support to the ever-changing operational and business needs/demands.

6.1.2.12 Each router/switch must have the following statement posted:

"THIS IS A PROPERTY OF THE PHILIPPINE PORTS AUTHORITY. UNAUTHORIZED ACCESS IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged; and violations of this policy may result in disciplinary action and may be reported to law enforcement. There is no right to privacy on this device."

Annex C

6.2 USER ACCOUNT MANAGEMENT

This is a critical component of system administration within an organization. The User Account is designed to provide basic permissions for completing common daily tasks such as allowing users to launch system applications, create new documents, modify basic system configuration settings, etc. Essentially, these operations are, therefore, user-specific and affect only the user who is logged on to the system network. Unless the user is given the authorization to do so, these functions, generally, do not include system-wide changes such as the installation of new applications. Regardless of the purpose of a particular User Account, there are security-related considerations that should be observed. The following guidelines are, thus, provided to ensure PPA of the proper maintenance and security of this area of responsibility:

6.2.1 For access to PPA domain and corporate email, new users shall submit an accomplished and signed UAR to ICTD Helpdesk, which will be the basis in evaluating the granting of access to the PPA domain as specified in the request.

6.2.1 For access to PPA computerized application, new users/transferees to other RCs/those with changed roles shall submit completely accomplished and signed UAR and RSU. These documents will be referred to in granting access to the PPA System/s as specified in the request.

6.2.2 Administrative/Super User Accounts shall be limited in number.

6.2.3 Users with administrative accounts shall use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.

6.2.4 User Accounts and Passwords shall be distributed to employees in a secure manner.

6.2.5 ICTD shall periodically validate User Accounts and privileges. Any inactive accounts shall be disabled and removed after a period of one month.

6.2.6 Accountability and traceability to individuals shall be maintained for all privileged system commands/actions on critical systems.

6.2.7 Users shall be notified that their actions may be monitored and recorded when using PPA systems.

6.2.8 Users shall not use any other User's account with or without the User's permission.

6.2.9 ICTD shall configure systems to issue a log entry and alert when an account is added to or removed from any group-assigned administrative privileges.

6.2.10 Logging of privileged account actions and relevant security events shall be employed on all systems including sufficient data to support security audits, (e.g., User logon information, access to privileged resources and changes to production information).

6.2.11 Audit logs containing security relevant events must be retained off-line for a period of one year.

6.2.12 Audit logs shall be resistant to attacks including attempts to deactivate, modify, or delete the logging software and/or the logs themselves.

6.2.13 Mechanisms for time synchronization for accurate logging of events on the network shall be employed and managed.

6.2.14 Monitoring of static web pages shall be employed to ensure that web page defacement attempts are corrected in real-time.

6.2.15 The right code of conduct of decency and courtesy in using shared resources over the network must be observed by officials and employees of all departments.

6.2.16 Permission in writing must be obtained from the Manager in case of urgent need to access the department's specific network resource such as file/folder.

6.2.17 It is the user's responsibility to ensure that files/folders are shared only to the intended recipient/s. Department heads must be aware of these shared network resource to properly advise their personnel on sharing vital or confidential information.

6.2.18 Anyone with knowledge of violations or suspected violations as regards user access whether on shared or non-shared resources must report this information to ICTD.

Annex D

6.3 SERVER SECURITY

This area of concern is a very important part of organizational computer security since most operational and financial data are stored in servers that could be compromised if servers were not properly configured, updated, and monitored. The firm implementation of pertinent policies is, therefore, necessary to provide basic standards for servers and network equipment to keep them secure at all times. Hence, stringent compliance to this policy will help avert security incidents, compromise of data, and possible damage to the organization. The specific PPA policy provisions on this aspect of ICT security are as follows:

6.3.1 Servers shall be documented with the following minimum information:

6.3.1.1 Server contact(s) and location, and a backup contact

6.3.1.2 Hardware and Operating System/Version

6.3.1.3 Main functions and applications, if applicable

6.3.2 The most recent security patches must be installed on the system as soon as possible; the only exception is when immediate application would interfere with business requirements.

6.3.3 To perform a function, standard security principles of least required access should always be used.

6.3.4 Do not use powerful accounts, (such as ‘administrator’ account), when a non-privileged account will do.

6.3.5 For practical purposes, services and applications that will not be used must be readily disabled.

6.3.6 Trust relationships between systems are security risks and their use must be avoided. Do not use or resort to Trust relationship when some other methods of communication will do.

6.3.7 Servers should be physically located in an access-controlled environment such as a Data Center, which requires a much greater level of security and control than normal office spaces.

Annex E

6.4 DATA CENTER SECURITY

The overall maintenance of the PPA Central Facility Data Center's physical security is the responsibility of the ICTD Manager, who shall ensure full compliance with the following expressed rule of order:

6.4.1 The following procedures apply in granting access to the Data Center:

6.4.1.1 Only PPA Responsibility Centers (RCs)/ Contractors/ Companies/Government Agencies with legitimate business in the Data Center may request access to the said facility by submitting a completely accomplished and signed Data Center Access Request or DCAR (see Annex C – ICTD Form 003) to ICTD Helpdesk.

6.4.1.2 Upon approval by the ICTD Manager/designated representative, the designated ORSD personnel will immediately inform the requesting entity regarding the access request approval.

6.4.1.3 Access permission commences and ends based on the specified duration period granted by the ICTD Manager/designated representative per approved access request.

6.4.2 The following rules apply regarding access level to the PPA Data Center:

6.4.2.1 **General Access** – only persons authorized to have free access to the Data Center, such as in the case of designated ICTD personnel whose job responsibilities require unrestricted entry into/exit from the area, will be granted this type of access.

6.4.2.2 **Limited Access** – granted to persons who do not qualify for General Access but have legitimate business in the Data Center that justifies their unsupervised access to the said area such as in the case of Administrative Services Department (ASD) personnel designated to undertake maintenance services of telephone facilities in the switch/hub room. Persons with Limited Access cannot authorize others to be granted unsupervised access to the Data Center.

6.4.2.3 **Escorted Access** – a closely monitored access provided to persons with needs for infrequent access to the Data Center due to legitimate commitments to be delivered. The incidence of "infrequent access" is generally limited to less than 15 days per year. Permission to this type of access is only granted by the Operations Resources Services Division (ORSD) Manager or his authorized representative. Persons given Escorted Access must be under the direct supervision of a person with General Access standing. They must provide positive identification upon demand and must leave the area when requested to do so.

6.4.3 Once the ICTD personnel, who has authorized access to the Data Center, terminates his employment or transfers from ICTD to another Responsibility Center (RC), his access rights to the Data Center shall be automatically revoked/cancelled.

6.4.4 To further ensure security maintenance of the Data Center, all doors to the Data Center must remain locked at all times and may only be temporarily opened for periods not to exceed what is minimally necessary to:

6.4.4.1 allow officially approved and logged access (entry/exit) of authorized individuals.

6.4.4.2 permit the transfer of supplies/equipment as directly supervised by a person with General Access to the area.

6.4.4.3 increase airflow into the Data Center in case of an air conditioning failure that at times there might be the need to prop open the facility's door. In this kind of situation, the personnel with General Access must be present and should limit access to the Data Center.

6.4.5 All infractions committed against the Data Center's physical security guidelines and procedures shall be reported to the ICTD Manager involving the following instances:

6.4.5.1 In case of warranted violation, (e.g., emergency, imminent danger, etc.), the port police/security guard should be notified by the authorized ICTD-ORSD personnel as soon as reasonably possible.

6.4.5.2 Any unauthorized access to the Data Center must be reported immediately to ICTD-ORSD. The unauthorized person/transgressor should be readily escorted out from the Data Center. A full written Incident Report should be immediately submitted to the ICTD Manager and the appropriate Security Office.

6.4.6 The ICTD personnel, with General Access to the Data Center, is obligated to monitor the area and cause the removal of any individual who appears to be compromising either the security of the area and attendant activities therein or who causes disruption to its operation. It is particularly crucial that the designated personnel take utmost initiative in monitoring and maintaining the security of the Data Center.

Annex F

6.5 DATABASE SECURITY

The policy provisions for this PPA ICT area of responsibility are as follows:

6.5.1 Database accounts shall integrate authentication with the operating system. Non-technical Users shall have no direct access to the operating system.

6.5.2 Access privileges of Users shall be on a role-based scheme wherein Users have access to resources based on the User's role. Access rights shall be grouped by role/job designation, and access to resources is restricted to Users who have been authorized to assume the associated role/job designation. Each User may be assigned one or more roles, and each role may be assigned one or more access privileges.

6.5.3 Any requests for creation of database link on the production servers shall require approval of the ICTD Database Administrator.

6.5.4 A User allowed to grant roles and privileges shall not grant, in any manner, his/her existing system privilege to other Users without the approval of the ICTD Database Administrator.

Annex G

6.6 INFORMATION CLASSIFICATION

All PPA Officials and Employees shall share in the responsibility of ensuring that corporate information assets receive an appropriate level of protection by observing the following Information Classification policies:

6.6.1 Managers or information 'owners' shall be responsible for assigning classifications to information assets according to the standard information classification.

6.6.2 Whenever practicable, the information category shall be embedded in the information itself.

6.6.3 All PPA Employees shall be guided by the below-given matrix on Information Category in their security-related handling of the Agency's information:

Information Category	Description	Examples
Public/Unclassified	Information is not confidential and can be made public without any implications for PPA. Loss of availability due to system downtime is an acceptable risk. Integrity is important but not vital.	• Brochures • Information available in the public domain, including publicly available PPA website areas • Downloadable Forms • Reports/Data required by regulatory authorities
Proprietary	Information is restricted to approved internal access and protected from external access. Unauthorized access could compromise PPA's operational effectiveness, cause an important financial loss or cause a major drop in customer confidence. Information integrity is vital.	• Passwords and information on PPA's security procedures • Standard Operating Procedures used in all parts of PPA's business systems • PPA's developed software code

Client Confidential Data	Information received from clients in any form for processing in production by PPA. The original copy of such information must not be changed in any way without written permission from the client. The highest possible levels of integrity, confidentiality, and restricted availability are vital.	• Client's Data • Electronic transmissions from clients
Company Confidential Data	Information collected and used by PPA in the conduct of its business. This includes personal data from employees. Access to this information is very restricted within the company. The highest possible levels of integrity, confidentiality, and restricted availability are vital.	• Salaries and other personnel data • Accounting data and internal financial reports • Confidential customer business data and confidential contracts • Non-disclosure agreements with clients\vendors • PPA's business plans • Drafts/copies of investigation reports

Annex H

6.7 REQUEST FOR SYSTEM UPDATE

The creation/filing of a Request for System Update (RSU) is requisite in facilitating system maintenance/fine-tuning and/or change in the Application System that includes Reference Data, System Development and Maintenance**,** and System Administration.

6.7.1. The nature of issues encountered in the use of PPA systems and services is generally of two types, namely:

6.7.1.1 **Program/Module Creation/Update-Related Issues**

6.7.1.1.1 In this kind of request, particular procedures are done through any of the following three layers of support process/task:

6.7.1.1.1.1 **First Level Support**

6.7.1.1.1.1.1 ICTD Helpdesk receives Incident Report/query by phone call, email/chat and/or facsimile from PPA User.

6.7.1.1.1.1.2 If Incident Report was received by phone call and can be easily resolved, Helpdesk readily provides the appropriate solution.

6.7.1.1.1.1.3 After having provided the first level support to the PPA User concerned, ICTD Helpdesk logs the valid Incident Report as User Support Request (USR).

6.7.1.1.1.1.4 ICTD Helpdesk conducts further monitoring by coordinating closely with the PPA User concerned, verifies the workability and effectiveness of the recommended solution.

6.7.1.1.1.1.5 ICTD Helpdesk closes the USR as “done” if the

recommended solution has been verified as workable and effective. The PPA User concerned is given a maximum of three days to respond to the verification process and if no response was received after the given period, ICTD Helpdesk considers the USR as "closed".

6.7.1.1.1.2 **Second Level** Support – if the issue remained unresolved at the First Level Support, ICTD Helpdesk escalates the matter to second level of support, which comprises the PPA Implementation Support Team, (i.e., Application Development Team, Data Conversion Team, Technical and Operations Team).

6.7.1.1.1.2.1 PPA Implementation Support Team conducts further incident analysis and investigation.

6.7.1.1.1.2.2 Once the recommended solution has been determined, the PPA Implementation Support Team prepares the RSU for submission to the ICTD Helpdesk to be logged as USR.

6.7.1.1.1.2.3 PPA Implementation Support Team implements the recommended solution.

6.7.1.1.1.2.4 ICTD Helpdesk informs the PPA User concerned of the implemented solution for verification.

6.7.1.1.1.2.5 ICTD Helpdesk tags the USR as "closed" if the recommended solution was verified effective. The PPA User concerned is given a

maximum of three days to respond to the verification process and if no response was received after the given period, ICTD Helpdesk tags the USR as "closed".

6.7.1.1.1.3 **Third Level** Support - if the problem were yet unresolved at the Second Level Support, it is elevated to third level of support to be attended to by the External Support Group (i.e., PPA IT Consultants, Network/Internet Providers and Oracle Support Group).

6.7.1.1.1.3.1 The External Support Group investigates the issue at hand to come up with the recommended solution.

6.7.1.1.1.3.2 PPA Implementation Support Team validates the workability and effectiveness of the recommended solution.

6.7.1.1.1.3.3 Once validation is completed, the PPA Implementation Support Team prepares the RSU for submission to the ICTD Helpdesk to be logged as USR.

6.7.1.1.1.3.4 PPA Implementation Support Team implements the recommended solution.

6.7.1.1.1.3.5 ICTD Helpdesk informs the PPA User concerned of the implemented solution.

6.7.1.1.1.3.6 ICTD Helpdesk tags the USR as "closed" if the recommended solution was workable and effective. The PPA User concerned is given a maximum of three days to respond to the verification process and if no response was received after the given

period, ICTD Helpdesk tags the USR as “closed”.

6.7.1.1.1.3.7 If the issue was not resolved by the third level of support, the PPA Implementation Support Team elevates the matter to the ADSD-ICTD Manager for further advice/plan of action.

6.7.1.2 **Set-Up Data-Related Issues**

6.7.1.2.1 This type of concerns usually covers the following areas:

6.7.1.2.1.1 Vessel Registration

6.7.1.2.1.2 Customer Registration

6.7.1.2.1.3 Vendor Registration

6.7.1.2.1.4 Chart of Accounts

6.7.1.2.1.5 Tariff Rates

6.7.1.2.1.6 Port Site

6.7.1.2.1.7 Commodity Registration

6.7.1.2.1.8 User Account Registration/Updating in the PROMPT/Oracle System

6.7.1.2.2 Steps to be undertaken for this kind of concern are as follows:

6.7.1.2.2.1 The PPA User concerned accomplishes completely the RSU **including pertinent documents as given below per type of concern area** and submits to the designated ICTD personnel either through email at ***helpdesk@ppa.com.ph*** or via facsimile through FAX No. (02) 301-9455:

- Vessel Registration – accomplished Vessel Information Sheet (VIS), Marina Certificate/International Tonnage Certificate (ITC)
- Customer Registration - accomplished Customer Registration Form (with valid TIN)
- Vendor Registration – accomplished Vendor Registration Form (with valid

TIN)

- Chart of Accounts - List of Chart of Account from COA/Additional Account from Controllership, if available
- Tariff Rates – Schedule of Restructured Cargo Handling Tariff from CSD
- Port Site – may concern any one of the following ports:
    - On-line Private Port - accomplished Port Code Template and Berthing Set-up Template (both to be obtained from ICTD via email or downloaded from PPA website)
    - Off-line Private Port - accomplished Port Code Template (from ICTD)
- Commodity Registration - List of Purchase Order Items to be added to the database
- User Account Registration/ Updating – accomplished User Account Request (UAR) Form (from ICTD)

6.7.1.2.2.3 If submitted documents were incomplete, ICTD Helpdesk advises the PPA User concerned regarding the lacking documents.

6.7.1.2.2.4 If the documents submitted were complete, ICTD Helpdesk validates the information in the PROMPT/Oracle System and asks for confirmation from the PPA User on the changes to be made in the PROMPT/Oracle System.

6.7.1.2.2.5 The designated ICTD personnel registers/sets-up/updates the corresponding record in the PROMPT/Oracle System.

6.7.1.2.2.6 Once the above-mentioned task has been properly executed, the ICTD Helpdesk logs the RSU as USR in the Helpdesk System.

6.7.1.2.2.7 The ICTD Helpdesk informs the PPA User concerned of successful changes/updates in the PROMPT/Oracle System.

Annex I

6.8 INFORMATION SECURITY INCIDENT

The systematic and expeditious handling of Information Security Incidents is crucial in minimizing their impact on the confidentiality, integrity, and availability of the Agency's systems, applications, data and network infrastructure. It is essential that such information is promptly communicated to appropriate PPA Officials for early resolution. While information security incidents are not always preventable, proper procedures for incident detection, reporting and handling, combined with education and awareness, can minimize their frequency, severity, and occurrence of potentially negative individual, operational, legal, reputational, and financial consequences.

6.8.1 Examples of Information Security Incident are as follows:

6.8.1.1 Computer system intrusion.

6.8.1.2 Unauthorized or inappropriate disclosure of sensitive institutional data.

6.8.1.3 Suspected or actual breaches, compromises, or other unauthorized access to PPA systems, data, applications, or accounts.

6.8.1.4 Unauthorized changes to computers or software.

6.8.1.5 Loss or theft of computer equipment or other data storage devices and media used to store private or potentially sensitive information, (e.g., laptop, USB drive, personally owned device used for work-related needs).

6.8.1.6 Denial of service attack or an attack that prevents or impairs the authorized use of networks, systems, or applications.

6.8.1.7 Interference with the intended use or inappropriate/improper usage of information technology resources.

Exceptions: Occurrences involving incidental access by PPA Employees or other trusted persons in which no harm is likely to result are not usually considered as Information Security Incidents.

6.8.2 Types of Information Security Incident are given below:

6.8.2.1 Serious – one that may pose substantial threat to PPA resources, services and/or confidentiality of stakeholders' personal/business profiles. An incident is categorized as serious if it meets one or more of the following criteria:

6.8.2.1.1 Involves potential, accidental, or other unauthorized access or disclosure of sensitive institutional information

6.8.2.1.2 Involves legal issues, including criminal activity that may be used as basis for litigation or regulatory investigation purposes

6.8.2.1.3 Causes severe disruption to mission-critical services

6.8.2.1.4 Involves active threats

6.8.2.1.5 Widespread

6.8.2.1.6 Likely to be of public interest

6.8.2.1.7 Likely to cause reputational harm to PPA

6.8.2.2 Sensitive – unauthorized disclosure that may bear serious adverse effect on PPA's reputation, resources, services or to individuals. Information protected under government regulations due to proprietary, ethical, or privacy considerations will typically be classified as sensitive; also includes personally identifiable information.

6.8.3 The scope of potentially affected entities covers the following:

6.8.3.1 All PPA Officials and Employees

6.8.3.2 Third-party vendors who collect, process, share or maintain PPA's institutional data, whether managed or hosted internally or externally

6.8.3.3 Users of personally owned devices, which access or maintain sensitive institutional data

6.8.4 Guidelines/procedures in handling/reporting Information Security Incidents:

6.8.4.1 All Users of PPA ICT resources must report in writing as Incident Report all Information Security Incidents to the ICTD Helpdesk, who will course the matter to the ICTD Manager.

6.8.4.2 Incident reporting, from identification to reporting to the ICTD Helpdesk, should be undertaken within 24 hours from occurrence and even during off-regular hours or weekends.

6.8.4.3 Based on the Incident Report submitted, the ICTD Manager will cause the conduct of an incident assessment and the coordination with the entities concerned for the proper and expeditious resolution of the information security case at hand.

6.8.4.4 To avoid inadvertent violations of government rules and regulations, individuals and RCs concerned should not release details of the Information Security Incident and affected electronic devices or electronic media to any outside entity, including law enforcement organizations, prior to the release of proper notifications on the completed conduct of resolution to the information security case under investigation.

6.8.5 Governing Roles and Responsibilities are as follows:

6.8.5.1 The ICTD Manager is the ultimate authority to render final interpretation to the above-stated guidelines and shall cause their implementation as well as initiate coordination on the handling of serious Information Security Incidents.

6.8.5.2 It is incumbent upon the PPA Management and Staff, and all Outsourced Personnel to report serious Information Security Incidents to the ICTD Helpdesk within 24 hours of becoming aware of the said incident.

6.8.5.3 The reporting requirements and procedures covered in the above-mentioned guidelines shall apply also to all third parties, (i.e., vendors, contractors and consultants), who are contractually bound to limit the access, use, or disclosure of PPA information assets. These third party entities shall report potential or actual incidents to PPA, through the ICTD Helpdesk.

For purposes of clarification, PPA has ownership and stewardship of, and custodial rights over all its ICT files, data and information assets, regardless of how or where these are stored, transmitted or processed.

Annex J

6.9 ELECTRONIC MAIL

For its official email system, PPA has adopted Office 365 (O365), which is the brand name Microsoft uses for a group of subscriptions that provide productivity software and related services. The subscription also allows the use of Microsoft Office apps on Windows, macOS, iOS, Android and Windows 10 Mobile and provides storage space on the OneDrive. In addition, for business Users like PPA, O365 also provides the following service subscriptions to satisfactorily address the information transmission/connectivity needs of the Agency in its day-to-day operation, administration and management endeavors: e-mail and social networking services through hosted versions of Exchange Server, Skype for Business Server, SharePoint and Office Online, integration with Yammer. This last related service is a "freemium" enterprise social networking service used for private communication within organizations.

6.9.1 Only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers.

6.9.2 The following rules apply to the use of PPA's O365 and related activities:

6.9.2.1 O365 shall be used for official activities only. Users shall not use the said facility for unlawful activities or for personal/financial gain.

6.9.2.2 Passwords shall never be shared or exposed to anyone besides the authorized Users. Unauthorized use of email accounts other than those assigned to a particular User is strictly prohibited. Passwords that are lost or are suspected to be lost, stolen or disclosed shall be reported immediately to ICTD.

6.9.2.3 PPA cannot provide absolute guarantee that electronic communications will be private. Users should be aware that electronic communication can, depending on the technology used, (e.g., hackers), be accessed, forwarded, intercepted, printed, and stored by others.

6.9.2.4 Users shall not use vulgar, obscene or insulting remarks in e-mail messages.

6.9.2.5 PPA's sensitive information must not be forwarded outside the PPA without prior approval of the General Manager or his designated PPA official.

6.9.2.6 Executable file attachments shall be automatically rejected to prevent the spread of virus invasion. Such type of attachments may, however, be allowed on a case to case basis.

6.9.2.7 Email messages which are no longer needed for business

purposes shall be regularly purged by Users from their personal email account to simplify and ease records management and retrieval.

6.9.2.8 Forwarding of chain letters and other *spam* mails is strictly prohibited to prevent virus proliferation.

6.9.2.9 Users are prohibited from allowing anyone else to use/access their electronic mail account.

6.9.2.10 Users are prohibited from reading or attempting to read any other User's electronic communications.

6.9.2.11 A legal recipient disclaimer will be automatically added to all external electronic mail messages.

6.9.2.12 Users shall not misrepresent or falsify their identity on the Internet or in any PPA communications. The User name, organization and other company-specific information shall be included in the message or posting.

6.9.2.13 Users shall refrain from opening electronic mail or suspect attachments from unknown senders or when the subject of the message seems inappropriate.

6.9.2.14 Official company records communicated/transmitted through electronic mail shall be identified, managed, protected, and maintained as long as they are needed for ongoing operations, audits, legal actions, or any other known purpose.

6.9.2.15 Transmission of any material, document, information that is confidential in nature, in violation of any of the existing policies of the PPA, is prohibited.

Annex K

6.10 INTERNET SECURITY

The following policy provisions on Internet Security are intended, foremost, to protect the "live" computer against today's diverse range of threats and unauthorized intrusions, which may include viruses, malware, hackers, etc.; and, additionally, to prohibit PPA Users from committing cyber technical and ethical infractions, which may wrought damage to the organization:

6.10.1 The PPA's internet facility shall only be used for official activities.

6.10.2 Downloading and use of unlicensed software is prohibited.

6.10.3 Users should assume that all materials on the internet are copyrighted unless specific notice states otherwise.

6.10.4 Users shall not save permanent Passwords in their web browsers because this practice may allow anybody who has physical access to their workstations to access the Internet with their identities.

6.10.5 Unless approved by ICTD, Users must not establish Internet or other external network connections that could allow unauthorized Users to gain access to PPA's systems and information.

6.10.6 Unauthorized internet hosting is strictly prohibited.

6.10.7 Users using PPA's resources must not connect/surf to web sites that contain sexually explicit, racist, violent, or other potentially offensive material.

6.10.8 Use of Chat Software, e.g., Yahoo, MSN Messenger and other forms of real-time communication software and devices, which make use of the Internet and its related technologies, is strictly prohibited unless authorized by the RC Head. On-line Internet games and gambling are strictly prohibited.

6.10.9 When Users provide information on public forums such as chat sessions, bulletin boards, etc., they must also clearly indicate that the opinions expressed are their own and not necessarily those of PPA.

6.10.10 PPA reserves the right to block access to sites deemed inappropriate.

6.10.11 Users of PPA's Internet connection should realize that their communications are not automatically protected from viewing by third

parties. Unless encryption and/or other approved security practices are employed, Users shall not send/post information if they consider it to be private and/or confidential.

6.10.12 PPA reserves the right to examine electronic mail messages, files on personal computers, web browser cache files, web browser bookmarks and cookies, logs of web sites visited, and other information stored on or passing through PPA computers.

6.10.13 All software used to access the World Wide Web must be approved by ICTD and must incorporate all appropriate/approved vendor-provided security patches.

6.10.14 Access to internal services from the Internet shall be via a secure (encrypted) login process. Subsequent transaction processes shall be secure as well.

6.10.15 All connections to and from the Internet shall be authenticated through a corporate-approved firewall.

6.10.16 Documentation, software, and other intellectual property must not be sold or otherwise transferred to any non-PPA User unless authorized.

6.10.17 Security credentials such as logins and Passwords shall only be sent via the Internet through secured, encrypted means. Approval from Management must be secured first for the use of other similar transmission processes.

6.10.18 ICTD Manager shall approve the hosting of all web pages on PPA-owned or operated systems. Any requests for the posting of data/information to the PPA website must be done through the submission to the ICTD Helpdesk of a completely accomplished and signed Website Posting Request or WPR (see Annex D – ICTD Form 004), which will be the referred to in assessing the granting of the said request.

6.10.19 Any files downloaded over the World Wide Web shall be scanned for viruses, using approved virus detection software.

6.10.20 All representations on behalf of PPA must first be cleared with the PPA FOI (Freedom of Information) Officer.

6.10.21 Users should not misrepresent or falsify their identity on the Internet or in any PPA communications. In official company communications, the User's name, organization and other company specific information shall be included in the message or posting.

6.10.22 Copying of software in a manner that is not consistent with the vendor's license is strictly forbidden. All licensed software shall be monitored and controlled by ICTD. Likewise, installation and update of software shall be done by an authorized/designated ICTD personnel.

6.10.23 If sensitive, confidential, and/or private information were lost or suspected to be lost or disclosed to unauthorized parties, ICTD shall have to be notified immediately by the User/RC Head concerned.

6.10.24 If unauthorized use of PPA information system has been done or is suspected to have taken place, ICTD shall have to be notified immediately by the User/RC Head concerned.

6.10.25 All unusual systems behaviour such as missing files, frequent system crashes, misrouted messages, and other similar occurrences/incidents must be reported immediately to ICTD.

6.10.26 The specifics of any possible security problems shall be kept confidential to the immediate management and security personnel.

6.10.27 Users shall not test security mechanisms at either PPA or other Internet sites nor use and/or possess tools for cracking information security unless prior written permission has been obtained from ICTD.

Annex L

6.11 VIRTUAL PRIVATE NETWORK (VPN)

VPN is a technology that creates a safe and encrypted connection over a less secure network such as the internet. It was primarily installed in the PPA ICT system to allow remote users and branch offices such as the Port and Terminal Management Offices (PMOs/TMOs) to securely access corporate applications and other resources as well as to enable PPA Users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. The following ICT security policies concerning VPN are, thus, prescribed for full adherence by all concerned:

6.11.1 It is the responsibility of ICTD to ensure that unauthorized Users are not allowed access to PPA's networks.

6.11.2 VPN use is to be controlled using strong passphrase.

6.11.3 When actively connected to the network, VPNs will force all traffic to and from the PC over the VPN tunnel; all other traffic will be dropped.

6.11.4 VPN gateways will be set up and managed by ICTD.

6.11.5 All computers connected to PPA internal networks via VPN or any other technology must use the most up-to-date anti-virus /anti-malware software to continuously monitor and defend each of the organization's workstations and servers.

6.11.6 Users with VPN connectivity shall be automatically disconnected from the PPA's network after thirty minutes of inactivity. The User must then logon again to re-connect to the network. Pings or other artificial network processes are not to be used to keep the connection open.

6.11.7 Only PPA-approved VPN clients may be used.

6.11.8 By using VPN technology with personal equipment, Users must understand that their machines are a de facto extension of the PPA's network, and as such are subject to the same rules and regulations that apply to PPA-owned equipment, i.e. their machines must be configured to comply with the PPA's security policies.

Annex M

6.12 FIREWALL SECURITY

The following policy provisions on Firewall Security are intended which will monitor and control incoming and outgoing network traffic based on PPA-predetermined security rules. A firewall provides protection to PPA's internal network from unauthorized users and safeguards data from attack

6.12.1 ICTD shall secure the configuration of PPA's network devices such as firewall, routers and switches.

6.12.2 All internet connectivity path and internet services must pass through firewalls for security, control and restrictions.

6.12.3 The PPA firewall filters packets of data to monitor it these meet certain security criteria and blocks or allows the data to pass through the network

6.12.4 All firewall appliance/servers must be placed in a physically secured area accessible only to authorized personnel.

Annex N

6.13 REMOTE ACCESS

6.13.1 It is the responsibility of employees, contractors, vendors and/or solution providers with remote access privileges to PPA's corporate network to ensure that their respective remote access connection is given the same consideration as the User's on-site connection.

6.13.2 Secure remote access must be strictly controlled. Control will be enforced via one-time Password authentication or public/private keys with strong pass-phrases.

6.13.3 At no time should any employee provide his login or email Password to anyone, not even to family members.

6.13.4 Employees and third party with remote access privileges must ensure that their PPA-owned/personal computer or workstation, which is remotely connected to PPA's corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the User.

6.13.5 All hosts that are connected to PPA's internal networks via remote access technologies must use the most up-to-date anti-virus software.

6.13.6 Personal equipment that is used to connect to PPA's networks must meet the requirements of PPA-owned equipment for remote access.

Annex O

6.14 AUDIT

6.14.1 ICTD shall ensure that local logging has been enabled on all systems and networking devices as well as appropriate logs are being aggregated to a central log management system for analysis and review.

6.14.2 ICTD shall secure the maintenance of its Data Recovery Capability by ensuring that all system data are automatically backed up on regular basis.

6.14.3 All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:

6.14.3.1 All security-related logs will be kept for a minimum of five (5) years for both Accounting and Finance Management System (AFMS) and Port Operations Management System (POMS).

6.14.3.2 Weekly full data storage backups of logs will be retained for at least one (1) week for AFMS and two (2) weeks for POMS.

6.14.3.3 Daily incremental data storage backups will be retained for at least one (1) week for AFMS and two (2) weeks for differential data storage backups for POMS.

6.14.4 When requested and for the purpose of performing an audit, any systems access needed will be provided to members of the Audit Team.

6.14.5 Database Administrators shall continuously monitor/audit access to sensitive objects as well as actions on the database.

6.14.6 During the audit period, such logs or backups must be secured in a manner that they cannot be modified and can be read only by authorized PPA personnel. The security-related logs are important for error correction, security breach investigations, and any other related tasks.

Annex P

6.15 ACCEPTABLE USE OF COMPUTER EQUIPMENT

6.15.1 Employees shall be responsible for the proper use of ICT equipment.

6.15.2 The RC Head shall request ICTD any addition of Personal Computer (PC) or laptop to the network.

6.15.3 For security and network maintenance purposes, ICTD shall monitor equipment, systems, and network traffic at any time.

6.15.4 All PCs, laptops, and workstations should be secured with a Password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when the host will be unattended.

6.15.5 Changes in configuration and settings in all equipment shall only be done by authorized ICTD personnel.

6.15.6 Data storage devices containing information for upload to/from the database shall be secured under locks as controlled by the Systems Administrator.

6.15.7 Only the Systems Administrators are authorized to retrieve data storage devices.

6.15.8 Disabling of any monitoring tool/facility installed on any system network shall be done only by authorized ICTD personnel.

.