

AUG 10 2023

PPA MEMORANDUM CIRCULAR
NO. 012 - 2023

**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 2023.

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 system, 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 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 PROVISION

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 DEFINITIONS 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 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 ICTD SECURITY AREA OF RESPONSIBILITY
B	2	Access Control
C	3	User Account Management
D	4	Server Security
E	5	Data Center Security
F	6	Database Security

ANNEX	Item No.	PPA ICTD SECURITY AREA OF RESPONSIBILITY
G	7	Information Classification
H	8	Request for System Update
I	9	Information Security Incident
J	10	Electronic Mail
K	11	Internet Security
L	12	Virtual Private Network (VPN)
M	13	Remote Access & Collaboration Tools
N	14	Firewall Security
O	15	Audit
P	16	Acceptable Use of Computer Equipment
Q	17	Information Technology (IT) Asset

7 SPECIFIC ROLES IN THE PROVISION OF ICT SECURITY

7.1 Information and Communication Technology Department

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

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

7.1.1 Network/System Administrator

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 System/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.
- 7.1.1.2.4 May suspend system usage until the extent of the compromise has been identified and addressed. The Administrator will also declare if the affected system has been deemed safe and secure to use again after completing such activity.

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 all users within their respective jurisdictions are aware of and in compliance 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 of 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 of the guidelines and procedures set forth in the PPA ICT Security Policy.
- 8.2 It shall also be every PPA Official and Employee's responsibility to report any possible 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 but not limited to missing files, frequent system crashes,

misrouted messages, corrupted and/or tampered data, and other similar occurrences.

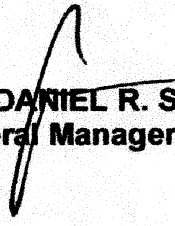
9 VIOLATIONS OF POLICY

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

10 REPEALING CLAUSE

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

For implementation, guidance, and compliance.



JAY DANIEL R. SANTIAGO
General Manager

1. 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 definitions of terms used in the drafting of this document are, thus, adopted as follows:

TERM	DEFINITIONS
Active Directory Server	A computer that securely stores user credentials such as login/usernames and passwords. The data contained on this server is used to authenticate credentials whenever a user logs in.
Anti-Virus	A software application designed to identify and remove known or potential computer viruses or similar malware before it can infect a computer system or network and potentially damage stored data or even any attached electronic device.
Backup Log	An official record of the process of duplicating data to allow retrieval of the duplicate set after a data loss.
Circuit	In the context of network topology, this refers to the method of network access, whether it is through traditional Integrated Services Digital Network (ISDN), Frame Relay, or via Virtual Private Network (VPN)/Encryption technologies
Cloud Storage	A form of electronic storage that provides System Users a method of storing data and files on a logical pool of storage media provided by a number of electronic devices across a computer network. From the User's point of view, its files are stored and grouped in one container, when in actuality such files are stored in various locations within the cloud network. User access to such files is provided via the Internet (which is the most common form of access), or via dedicated private networks.
Collaboration Tools	An application that can support at least two Users and provide methods to access common files and functions and work at the same time on the same file or function.
Credentials	Data or information which is used and presented during initial access on an electronic system for User authentication. The most common forms of user credentials are Usernames, Login IDs, and Passwords. Some information such as usernames and login IDs are unique for each User. Biometric information such as fingerprints and retina patterns are also other forms of User Credentials and can be used for authentication.

TERM	DEFINITIONS
Cybersecurity	<p>Cybersecurity is formally defined as indicated below:</p> <ol style="list-style-type: none"> 1. 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) 2. The process of protecting information by preventing, detecting, and responding to attacks, (according to the National Institute of Standards and Technology or NIST). 3. Also termed cyberspace security, which refers to the preservation of confidentiality, integrity, and availability of information in Cyberspace, (as defined by the International Organization for Standardization or ISO)
Cyberspace	As defined by the ISO, it is the complex environment resulting from the interaction of people, hardware, software, and services on the internet by means of technology devices and networks connected to it, which does not exist in any physical form.
Data Center	A restricted facility is used to host computer systems and its associated components, such as telecommunications (server) and storage systems. It generally includes redundancies such as backup power supplies, and data connections, environmental controls (such as air conditioning, and fire suppression), and various levels of security devices for personnel access.
Electronic Mail or Email	The digital equivalent of postal mail, it is a method of communication that allows stateful transmission of messages between electronic devices across a computer network.
Encryption	It is the process of encoding information from its original form, known as plaintext, to an alternate form known as ciphertext via a specific mathematical algorithm. In order to restore such information in its original form, the same specific mathematical algorithm will be used to decode the message. These mathematical algorithms are known as ciphers, which has a functional equivalence of a key in the physical world.
Executable File	An electronic file that contains a program or application that is capable of being executed or run within a

TERM	DEFINITIONS
	computer. These files will then allow an application to perform its specified operations or tasks.
File Synchronization	A process in which files that are stored in two or more locations are constantly updated in the same way in order to maintain consistency.
Firewall	In the context of computer security, it is a combination of hardware devices and software applications that protect a computer network from unauthorized access and intrusion. It also allows which user or application can access the network and works in conjunction with a network gateway (see definition below).
Gateway	It is a network device or software service that acts as a border point between one computer network to another.
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 Information & Communication Technology (ICT) Resources).
Information Security Incident	A malicious activity or event where there is a suspicion, attempt, successful or unsuccessful access to any operation, service, or device that involves information technology. Such incidents can result in unauthorized access, use, disclosure, modification, dissemination, or destruction of information.
Inter hosting	A third-party business that provides file hosting and maintenance services for one or more of its clients, usually for website content.
Internet	<p>In its basic term, it is a portmanteau for "interconnected network", or multiple smaller electronic networks connected into a singular, larger network.</p> <p>If defined in its modern context (and in its more formal and capitalized form, "Internet"), it is a global connection of various computer systems and networks linked by a broad array of electronic network technologies and protocols. The Internet has a vast range of information, resources, and services, provided by various private, public, academic, commercial, and government networks with local to global scope.</p>

TERM	DEFINITIONS
Internet Services	These are electronic services provided within the Internet that are accessible through other devices across the network. Common examples of Internet services are the World Wide Web (WWW), the Domain Name System (DNS), Internet telephony and video streaming, instant messaging, and social networking services.
Intranet	A smaller computer network designed for organizations and their respective members/personnel.
Mailbox	In the context of email, it is a software storage space provided for each email user to contain electronic messages.
One Drive	A commercial cloud storage service that was launched by Microsoft in 2007, under the "Azure" tradename. As of 2023, it is one of the "Big 3" cloud services along with Amazon Web Service and Google Cloud with a global reach.
Operating System	Commonly abbreviated OS or O/S, it is a software interface between the computer hardware and the user. This software is responsible for the management of computer resources and coordination of multiple activities that are performed by the device. It also acts as the host for other computing applications (commonly known as "programs") by providing a platform to operate or execute as such.
Remote Access	It is the ability or function to access a computer or an electronic device from a different location and gain control of its resources.
Removable Medium	A form of physical electronic storage device that is designed to be mounted/attached and removed from a computer even while the device is still running. Examples of removable media are external hard disk drives, portable solid-state USB drives (commonly known as "flash drives", "USB drives" or "thumb stick drives",) and optical media such as CDs and DVDs.
Risk	It is the condition or exposure to the chance of injury or loss. In the context of cybersecurity, it is a condition or factor that could affect the confidentiality, availability, and integrity of an organization's information assets and electronic systems.
Router	In the context of computer networks, it is an electronic device that joins multiple networks together.
Security Log	A record of security-related events or incidents that occur on a computer system, network, or application. It is used to track security-related information on a computer system. Examples of security logs include access logs, error logs, and event logs.

TERM	DEFINITIONS
<i>Sensitive Information</i>	A kind of knowledge or data that is of high value or regard by its owner or source, and any adverse event on such data will have dire consequences.
<i>Server</i>	In the context of computer networks, it is an electronic device that manages network resources with such examples as storing files, managing electronic devices such as printers, managing network traffic, or processing database queries
<i>Spam</i>	It is a derogatory term for any unsolicited bulk or junk email. This may include chain letters, items for sale/advertisements, get-rich-quick scams, or any other unwanted e-mails.
<i>SSL VPN</i>	It is an abbreviation for Secure Socket Layer Virtual Private Network. It is a network protocol that enables computing devices such as laptops, desktops, and mobile phones to establish a secure remote access connection that uses an internet connection. Once a secure connection was made between two devices, the User will now have access to the available resources in the destination network.
<i>Third-Party</i>	<p>In legal terms, it is a label to an entity or organization that is incidentally or contractually involved to an activity or undertaking.</p> <p>In the context of PPA cybersecurity, these are entities that are contracted by the Agency to provide solutions or services to address various ICT issues and concerns. These entities are also known as contractors, vendors, system integrators, or application service providers.</p>
<i>User Authentication</i>	In the context of information technology, it is the process of establishing identity and verify a user's permission level to access an electronic device or a computer network, through the use of the assigned User Credentials.
<i>Web Browser</i>	software used to access websites on the Internet. Examples are Google Chrome, Microsoft Edge, Mozilla Firefox, Apple Safari, and Opera.

2. ACCESS CONTROL

PPA ICT Services, Facilities, and Infrastructure shall be accessed for official business purposes only and should not be used for any unlawful or unauthorized 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 responsibilities areas, namely: ICT Systems and ICT Networks. The pertinent provisions in this regard are as follows:

2.1 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. The access mechanism must incorporate credential authentication controls using a unique Username/User ID and Password assigned to each authorized User. The following guidelines are, thus, provided:

- 2.1.1 A single sign-on approach will be adopted for all in-house developed systems.
- 2.1.2 Naming standards and conventions shall be observed and documented for each application.
- 2.1.3 Users shall be responsible for all activities, known or unknown, related to the use and safeguarding of their respective login credentials.
- 2.1.4 A duly accomplished and signed User Account Request (UAR), (see Annex A – ICTD Form 001), must be submitted for all requests concerning authorization on the corresponding roles/privileges for a new Username/User ID. These forms, as with the case of ICTD Forms 002, 003, and 004, are downloadable from the PPA website at <https://www.ppa.com.ph>.
- 2.1.5 Anonymous and guest credentials (Guest Usernames or User IDs) shall not be allowed.
- 2.1.6 Passwords must be sufficiently complex (avoid names, places, birthdays, company slogans, dictionary words, among others.) and must bear/comply with the following:
 - 2.1.6.1 The minimum password length employed on all accounts should be eight alphanumeric and non-alphabetic characters (numeric or symbol).

- 2.1.6.2 The system shall require password changes for a minimum period of one month and a maximum of six (6) months.**
- 2.1.6.3 Passwords must also contain at least one uppercase and one lowercase character.**
- 2.1.7 Users shall change their password immediately after the first successful login into the system, and during a Password reset request.**
- 2.1.8 User password must not be scripted nor hard-coded (i.e., placed in a function key, macro, or using "Save Password on next connect").**
- 2.1.9 Users shall change their passwords immediately in case it has been compromised and immediately report such incident to ICTD for issue tracking.**
- 2.1.10 Users shall neither ask nor disclose passwords for any accounts or systems that are either owned or managed by the PPA.**
- 2.1.11 Users must be cautious in writing down passwords and leaving them exposed which lead to its discovery. It is suggested that written passwords and other credentials should be safely stored in a non-public location. Never write down passwords or other login Credentials on small notes and put on display such that it can be easily misplaced or glanced in a public place (i.e.: post-it notes attached on a monitor or on a desktop PC).**
- 2.1.12 All default user credentials provided by software or hardware must be changed once implemented/deployed on production systems or development systems attached to the network or internet.**
- 2.1.13 Users and System Administrators who maintain multiple accounts must use different passwords for each account.**
- 2.1.14 The number of consecutive unsuccessful access attempts will be limited to only three. Once locked out, only the System Administrator can unlock the account.**
- 2.1.15 All User Login activities shall be automatically audited by the system. Recorded data shall include date and time of the last successful login and the Username of the User.**
- 2.1.16 Users shall not leave unattended any PPA electronic device currently connected or in active session. The negligence for unwarranted access thereto shall be a ground for disciplinary measure against the user and the personnel accessing it without authority.**

2.2 Access to ICT Network

- 2.2.1 Only authorized Network Administrators shall perform all of the necessary network configuration activities. Access to all network devices shall be strictly limited to authorized technical personnel only unless unrestricted access is granted to an external party after approval of and under direct supervision by ICTD.
- 2.2.2 A properly 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, and reconfiguring routers. All emergency modifications in the network must only be made by and reported immediately to authorized ICTD personnel and Network Administrators.
- 2.2.3 All internal network devices, (i.e., routers, firewalls, access control servers, etc.), shall have its respective unique passwords kept in a secure encrypted form or other access control mechanisms.
- 2.2.4 PPA's information and communication systems shall restrict access to the computers, devices, or software that users can reach over the PPA's networks. These restrictions shall be implemented via routers, gateways, and other network devices.
- 2.2.5 Devices considered or known generally for undesirable/malicious or potentially damaging transmission are to be blocked from access to the PPA network.
- 2.2.6 The PPA reserves the right to audit networks and systems on a periodic basis to ensure compliance with the above-stated policy.
- 2.2.7 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 the PPA ICT Security Policy).
- 2.2.8 All connections to the internal computer data network shall employ User Authentication.
- 2.2.9 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).
- 2.2.10 Routers, hubs, modems, and other networking hardware should be strategically to avoid tampering by unauthorized personnel.

2.2.11 The ICTD System Administrator shall disable the user account (corporate email, computerized systems, domain etc.) of PPA 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 consideration of business needs/demands.

3. USER ACCOUNT MANAGEMENT

This is a critical component of system administration within an organization. The User Account, which is comprised of various User Credential elements, is designed to provide permission and access levels to various PPA's ICT Systems for completing tasks such as launching software applications, creating new documents, or even accessing the Internet. Essentially, these tasks are user-specific and affect only the user who is logged on to the system or 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 or modifying critical settings. Regardless of the purpose of a particular User Account, there are security-related considerations that should be observed, as outlined below, to ensure PPA of the proper maintenance and security of this area of responsibility:

- 3.1 For access to the PPA network domain, corporate email, and various PPA computerized applications, new users shall submit an accomplished and signed UAR to the ICTD Helpdesk, which will be the basis for evaluating access as specified in the request.
- 3.2 For modification of an existing User Account in a PPA computerized application (i.e.: addition, deletion, or change of role, task, or site/location), the User shall submit a duly accomplished UAR and RSU. These documents will be used as references for approval or rejection as specified for such requests.
- 3.3 Administrative or "Super-User" accounts shall be very limited in number and distributed only to authorized PPA personnel.
- 3.4 Users with administrative accounts shall only use as such for elevated activities within the system, such as (including, but not limited to) performing system-wide changes or add/modify/deactivate available system functions. This account should only be used for administrative or troubleshooting activities.
- 3.5 User Accounts and Passwords shall be distributed to requesting personnel in a direct and secure manner.
- 3.6 Authorized ICTD personnel shall annually conduct user cleanup on PPA Computerized Systems to validate User Accounts and privileges and apply any necessary action.
- 3.7 Authorized ICTD personnel shall periodically validate User Accounts and privileges on Microsoft Exchange (Email). A license shall be revoked for any inactive account to be redistributed to new users.
- 3.8 Accountability and traceability to individuals shall be maintained for all

privileged system commands/actions on critical systems.

- 3.8 Users shall be notified that their actions may be monitored and recorded when using PPA systems.
- 3.9 Users shall not use any other User's account with or without the User's permission.
- 3.10 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.
- 3.11 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 login information, access to privileged resources, and changes to production information).
- 3.12 Audit logs containing security-relevant events must be retained offline for a period of one year.
- 3.13 Audit logs shall be resistant to attacks including attempts to deactivate, modify, or delete the logging software and/or the logs themselves.
- 3.14 Mechanisms for time synchronization for accurate logging of events on the network shall be employed and managed.
- 3.15 Monitoring of static web pages shall be employed to ensure that web page defacement attempts are corrected in real-time.
- 3.16 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.
- 3.17 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.
- 3.18 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 resources to properly advise their personnel on sharing vital or confidential information.
- 3.19 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.

4. 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 are 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 with this policy will help avert security incidents, data breaches, and possible damage to the organization. The specific PPA policy provisions on this aspect of ICT Security are as follows:

- 4.1 Servers shall be documented with the following minimum information:
 - 4.1.1 Server contact(s) and location, and a backup contact;
 - 4.1.2 Hardware and Operating System/Version; and
 - 4.1.3 Main functions and applications, if applicable.
- 4.2 Most recent security patches must be installed in the system except when immediate application would interfere with business requirements.
- 4.3 Standard security principles of the least required access should be used in performing a function.
- 4.4 Avoid using accounts with elevated privileges when performing standard day-to-day system functions, when a regular User account can perform the required functions. Such privileges are reserved for system troubleshooting or under extreme circumstances.
- 4.5 For practical purposes, services and applications not in use must be readily disabled.
- 4.6 Trust relationships between systems are identified security risks. Resorting to such must be avoided when other methods of communication are available.
- 4.7 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.

5. 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.

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

5.1.1 Only PPA Responsibility Centers (RCs)/ Contractors/ Companies/Government Agencies with legitimate business at the Data Center may request access to the said facility.

5.1.2 Upon approval by the ICTD Manager, the designated Operation Resources and Services Division (ORSD) personnel will immediately direct the requesting entity to accomplish an online registration form thru a QR Code or link. After the registration, the QR Code/link will issue a Guest ID that the requesting entity shall use as ID in filling out the Online Logbook for CF Data Access.

The guest/visitor is then accompanied by the assigned ORSD personnel and informed of the CF House Rules before entering the PPA CF Data Center.

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

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

5.2.1 **General Access** – granted to persons authorized to have free access to the Data Center, such as designated ICTD personnel whose job responsibilities require unrestricted entry into/exit from the area.

5.2.2 **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.

5.2.3 **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.

- 5.3 Once the ICTD personnel, who has authorized access to the Data Center, terminates his employment or transfers to another RC), his access rights to the Data Center shall be automatically revoked/canceled.
- 5.4 To further ensure security maintenance of the Data Center, all doors are equipped with an automatic door lock system and an alarm feature that is triggered after leaving the door open for 10 seconds. The authorized designated ORSD personnel may only temporarily open the door for periods not to exceed what is minimally necessary by setting the alarm system in order to:
 - 5.4.1 Allow officially approved and logged access (entry/exit) of authorized individuals.
 - 5.4.2 Increase airflow into the Data Center in case of an air conditioning failure that at times might 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.
- 5.5 The following infractions against the Data Center's physical security shall immediately be reported to the ICTD Manager:
 - 5.5.1 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.
 - 5.5.2 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.
- 5.6 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 the utmost initiative in monitoring and maintaining the security of the Data Center.

6. DATABASE SECURITY

- 6.1 Database accounts shall integrate authentication with the operating system. Non-technical Users shall have no direct access to the operating system shell. A menu-driven facility shall be made available to non-technical Users.
- 6.2 Access privileges of Users shall be on a role-based scheme wherein Users have access to resources based on the User's role. Each User may be assigned one or more roles, and each role may be assigned one or more access privileges.
- 6.3 Any request for the creation of a database link on the production servers shall require the approval of the ICTD Data Base Administrator.
- 6.4 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 Data Base Administrator.

7. 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:

- 7.1 Managers or information 'owners' shall be responsible for assigning classifications to information assets according to the standard information classification.
- 7.2 Whenever practicable, the information category shall be embedded in the information itself.
- 7.3 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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Client's Data

	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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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

8. 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.

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

8.1.1 Program/Module Creation/Update-Related Issues

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

8.1.1.1.1 First-Level Support

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

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

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

8.1.1.1.1.4 ICTD Helpdesk shall conduct further task of monitoring by coordinating closely with the PPA User concerned, verifying the workability and effectiveness of the

recommended solution.

8.1.1.1.1.5 ICTD Helpdesk shall close 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 were received after the said given period, ICTD Helpdesk shall consider the USR as "closed".

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

8.1.1.1.2.1 PPA Implementation Support Team shall conduct further incident analysis and investigation.

8.1.1.1.2.2 Once the recommended solution has been determined, the PPA Implementation Support Team shall prepare the RSU for submission to the ICTD Helpdesk to be logged on by the latter as USR.

8.1.1.1.2.3 PPA Implementation Support Team shall

then implement the recommended solution.

8.1.1.1.2.4 ICTD Helpdesk shall inform the PPA User concerned of the implemented solution.

8.1.1.1.2.5 ICTD Helpdesk shall close 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 were received after the said given period, ICTD Helpdesk shall consider the USR as "closed".

8.1.1.1.3 Third Level Support - if the problem were yet unresolved at the Second Level Support, it is then elevated to this last level of support, which is the External Support Group (i.e., PPA Consultants, Network/Internet Providers and Oracle Support Group).

8.1.1.1.3.1 The External Support Group shall further investigate the issue at hand to come up with the recommended solution.

8.1.1.1.3.2 PPA Implementation Support Team shall validate the workability and effectiveness of the recommended solution.

- 8.1.1.1.3.3 Once validation is completed, the PPA Implementation Support Team shall prepare the RSU for submission to the ICTD Helpdesk to be logged on by the latter as USR.
- 8.1.1.1.3.4 PPA Implementation Support Team shall then implement the recommended solution.
- 8.1.1.1.3.5 ICTD Helpdesk shall inform the PPA User concerned of the implemented solution.
- 8.1.1.1.3.6 ICTD Helpdesk shall close 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 were received after the said given period, ICTD Helpdesk shall consider the USR as "closed".
- 8.1.1.1.3.7 Otherwise, when no solutions recommended at this level can effectively address the standing issue, the PPA Implementation Support Team then elevates the matter to the Application Development and Support Division -

ICTD Manager for further advice/plan of action.

8.1.2 Set-Up Data-Related Issues

8.1.2.1 This type of concern usually covers the following areas:

- 8.1.2.1.1 Vessel Registration
- 8.1.2.1.2 Customer Registration
- 8.1.2.1.3 Vendor Registration
- 8.1.2.1.4 Chart of Accounts
- 8.1.2.1.5 Tariff Rates
- 8.1.2.1.6 Port Site
- 8.1.2.1.7 Commodity Registration
- 8.1.2.1.8 User Account Registration/Updating in the iPORTS/Oracle System

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

8.1.2.2.1 The PPA User concerned shall accomplish the RSU Form, which may be secured personally from the ICTD Helpdesk or downloaded from the PPA website at www.ppa.com.ph.

8.1.2.2.2 Once accomplished, PPA User concerned shall submit the RSU, including pertinent documents submitted by the Port Users, Contractors, and Third-party service providers among others as given below per type of concern area to the designated ICTD personnel either through email at helpdesk@ppa.com.ph or handed over to the helpdesk on duty.

- Vessel Registration – accomplished Vessel Information Sheet (VIS), Marina Certificate for the domestic vessels, or International Tonnage Certificate (ITC) for the foreign vessels.
- Customer Registration -

accomplished Customer
Registration Form, BIR 2303
and sample OR issued by the
customer.

- Vendor Registration –
accomplished Vendor
Registration Form, BIR 2303
and sample OR issued by the
customer.
- Vendor Registration (PPA
Employee) – accomplished
Vendor Registration Form with
TIN ID (BIR 2316 if TIN ID is not
available)
- Chart of Accounts - List of Chart
of Account from COA/Additional
Account from Controllershship, if
available
- Tariff Rates – Schedule of
Restructured Cargo Handling
Tariff from CSD
- Port Site – accomplished Port
Code Template (to be obtained
from ICTD via email or
downloaded from the PPA
website)
- Commodity Registration - List of
Purchase Order Items to be
added to the database.
- User Account
Registration/Updating –
accomplished User Account
Request (UAR) Form (to be
obtained from ICTD via email or
downloaded from the PPA
website)

8.1.2.2.3 If the documents were submitted as
complete, the ICTD Helpdesk shall
validate them in the iPORTS/Oracle
System. If found to be incomplete,
the ICTD Helpdesk shall advise the
PPA User concerned regarding the
required lacking documents.

8.1.2.2.4 When the submitted documents
have been validated as complete,
the ICTD Helpdesk shall ask for

confirmation from the PPA User on the changes to be made in the iPORTS/Oracle System.

- 8.1.2.2.5 The appropriately designated ICTD personnel shall then register/set up/update the corresponding/affected record in the iPORTS/Oracle System.
- 8.1.2.2.6 Once the above-mentioned task has been properly executed, the ICTD Helpdesk shall log the RSU as USR in the Helpdesk System.
- 8.1.2.2.7 ICTD Helpdesk shall then inform the PPA User concerned that the requested changes/updates have been successfully carried out in the iPORTS/Oracle System.

9. 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.

9.1 Examples of Information Security Incidents are as follows:

- 9.1.1 Computer system intrusion. with specific examples such as electronic packet inspection (wired or wireless), SQL injection, or brute-force attacks.
- 9.1.2 Unauthorized or inappropriate disclosure of sensitive institutional data.
- 9.1.3 Suspected or actual breaches, compromises, or other unauthorized access to PPA systems, data, applications, or accounts.
- 9.1.4 Unauthorized changes to computers or software.
- 9.1.5 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).
- 9.1.6 Denial of service attack or an attack that prevents or impairs the authorized use of networks, systems, or applications.
- 9.1.7 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.

9.2 Types of Information Security Incidents are given below:

- 9.2.1 Serious – one that may pose a 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:

- 9.2.1.1 Involves potential, accidental, or other unauthorized access or disclosure of sensitive institutional information.
- 9.2.1.2 Involves legal issues, including criminal activity that may be used as the basis for litigation or regulatory investigation purposes
- 9.2.1.3 Causes severe disruption to mission-critical services
- 9.2.1.4 Involves active threats
- 9.2.1.5 Widespread
- 9.2.1.6 Likely to be of public interest
- 9.2.1.7 Likely to cause reputational harm to PPA
- 9.2.2 Sensitive – involves unauthorized disclosure that may bear serious adverse effects 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.
- 9.3 The scope of potentially affected entities covers the following:
 - 9.3.1 All PPA Officials and Employees
 - 9.3.2 Third-party vendors who collect, process, share or maintain PPA's institutional data, whether managed or hosted internally or externally.
 - 9.3.3 Users of personally owned devices that access or maintain sensitive institutional data.
- 9.4 Guidelines/procedures in handling/reporting Information Security Incidents:
 - 9.4.1 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.
 - 9.4.2 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.
 - 9.4.3 Based on the Incident Report submitted, the ICTD Manager will direct the conduct an incident assessment and coordinate with the entities concerned for the proper and expeditious resolution of the information security case at hand.
 - 9.4.4 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 other 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.

9.5 Governing Roles and Responsibilities are as follows:

- 9.5.1** The ICTD Manager is the ultimate authority to render a 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.
- 9.5.2** 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 from knowledge of the said incident.
- 9.5.3** 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.

10. ELECTRONIC MAIL

For its official email system, PPA has adopted a cloud-powered productivity platform that uses subscriptions for software and other related services. The subscription also allows office applications on desktop, laptop, and mobile devices and provides cloud storage. In addition, this productivity platform provides services that satisfactorily address the information transmission and communication needs of the agency in its day-to-day operation, administration, and management. The productivity platform also includes online collaboration tools, social networking, that can be used for private communication within the organization. Access to these applications is determined by the user's internet access, and only PPA personnel with approved email addresses may join their respective groups or network.

The following rules apply to the use of PPA's corporate email and related activities:

- 10.1 PPA corporate email shall be used for official activities only. Users shall not use the said facility for unlawful activities or for personal/financial gain.
- 10.2 Passwords shall never be shared or exposed to anyone besides the authorized Users. The 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.
- 10.3 The contents of the email may be monitored to support operational, maintenance, auditing, security, and investigative activities. The Systems Administrator, upon approval by the ICTD Manager, may review the contents of a User's mailbox during the course of problem resolution/investigation.
- 10.4 PPA cannot provide an 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.
- 10.5 Users shall not use vulgar, obscene, or insulting remarks in e-mail messages.
- 10.6 PPA's sensitive information must not be forwarded outside the PPA without prior approval of the General Manager or his designated PPA official.
- 10.7 Email messages shall be backed up and stored in cloud storage as long as the license subscription remains active.
- 10.8 Executable file attachments shall be automatically rejected to prevent the spread of virus invasion. Such types of attachments

may, however, be allowed on a case-to-case basis.

- 10.9 Email messages which are no longer needed for business purposes shall be regularly purged by Users from their personal email accounts to simplify and ease records management and retrieval.
- 10.10 RC Heads are required to submit to ICTD a request for email accounts of their personnel as well as for email account revocation for personnel due to any of the following circumstances:
 - 6.7.10.1 User ends service to PPA (retirement or resignation).
 - 6.7.10.2 User is suspended from work.
 - 6.7.10.3 User goes on extended leave or AWOL.
- 10.11 Forwarding of chain letters and other *spam* mail is strictly prohibited to prevent virus proliferation.
- 10.12 Users are prohibited from allowing anyone else to use/access their electronic mail account.
- 10.13 Users are prohibited from reading or attempting to read any other User's electronic communications.
- 10.14 A legal recipient disclaimer will be automatically added to all external electronic mail messages.
- 10.15 Users shall not misrepresent or falsify their identity on the Internet or in any PPA communications. The Username, organization, and other company-specific information shall be included in the message or posting.
- 10.16 Users shall refrain from opening electronic mail or suspect attachments from unknown senders or when the subject of the message seems inappropriate.
- 10.17 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.
- 10.18 If sensitive, confidential, and/or private information were lost or disclosed to unauthorized parties, ICTD shall have to be notified immediately by the User concerned.
- 10.19 Users shall immediately notify ICTD, through the Helpdesk, of all unusual systems behavior, such as missing files, frequent system crashes, misrouted messages, and other similar activities.
- 10.20 Users shall not probe security mechanisms at either PPA or other Internet sites nor use and/or possess tools for cracking information security.
- 10.21 Transmission of any material, document, or information that is confidential in nature, in violation of any of the existing policies of the PPA, is prohibited.

11. INTERNET SECURITY

- 11.1 The PPA's internet facility shall only be used for official activities.
- 11.2 Downloading of evaluation/unlicensed software is prohibited, unless duly noted by the RC Head and approved by the Information and Communications Technology Department.
- 11.3 Users should assume that all materials on the internet are copyrighted unless specific notice states otherwise.
- 11.4 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.
- 11.5 As long as approved by the authorized ICTD personnel, PPA guests may be given access to PPA Guest Wifi. Access must be limited to sites allowed by the PPA's internet security policy.
- 11.6 PPA's internal systems and information must not be accessible through the PPA Guest Wifi.
- 11.7 Unauthorized internet hosting is strictly prohibited.
- 11.8 Users using PPA's resources must not connect/surf to websites that contain sexually explicit, racist, violent, or other potentially offensive material.
- 11.9 Use of Chat Software, e.g., Viber, MS Teams, FB Messenger, and other forms of real-time communication software and devices, which make use of the Internet and its related technologies, is allowed. Online Internet games and gambling are strictly prohibited.
- 11.10 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.
- 11.11 PPA reserves the right to block access to sites deemed inappropriate.
- 11.12 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.
- 11.13 PPA may keep logs and 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 pass through PPA computers.

- 11.14 All software used to access the World Wide Web must be approved by ICTD and must incorporate all appropriate/approved vendor-provided security patches.
- 11.15 Access to internal services from the Internet shall be via a secure (encrypted) login process. Subsequent transaction processes shall be secure as well.
- 11.16 The use of Terminal Network (TELNET) connection with fixed Passwords over the Internet shall be prohibited.
- 11.17 All connections to and from the Internet shall be authenticated through a corporate-approved firewall. This precludes "dialing around the company's Internet connection" or dialing into a computer from within the company.
- 11.18 Documentation, software, and other intellectual property must not be sold or otherwise transferred to any non-PPA User unless authorized.
- 11.19 Security credentials such as logins and Passwords shall only be sent via the Internet through secure, encrypted means. Approval from Management must be secured first for the use of other similar transmission processes.
- 11.20 ICTD shall approve the hosting of all web pages on PPA-owned or operated systems.
- 11.21 Any files downloaded over the World Wide Web shall be scanned for viruses, using approved virus detection software.
- 11.22 All representations on behalf of PPA must first be cleared with Management. In addition, Users shall not release company information or enter into any transactions such as contracts, including placing orders, until the identity of the individual or organization being contracted is confirmed.
- 11.23 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.
- 11.24 Copying 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 the software shall be done by authorized/designated ICTD personnel.
- 11.25 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.
- 11.26 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.

- 11.27 All unusual systems behavior such as missing files, frequent system crashes, misrouted messages, and other similar occurrences/incidents must be reported immediately to ICTD.
- 11.28 The specifics of any possible security problems shall be kept confidential to the immediate management and security personnel.
- 11.29 Users shall not test security mechanisms at either PPA or other Internet sites nor use and/or possess tools for defeating information security unless prior written permission has been obtained from ICTD.

12. VIRTUAL PRIVATE NETWORK (VPN)

- 12.1 It is the responsibility of ICTD to ensure that unauthorized Users are not allowed access to PPA's Internet networks.
- 12.2 VPN user access will be controlled using strong passphrases.
- 12.3 When a User is actively connected to the VPN, it will force all traffic to and from the electronic over the VPN tunnel; all other traffic will be dropped.
- 12.4 VPN gateways will be set up and managed by ICTD.
- 12.5 All computers connected to PPA internal networks via VPN, or any other technology must use the most licensed and up-to-date anti-virus; this includes personal computers.
- 12.6 Users with VPN connectivity shall be automatically disconnected from the PPA's network after thirty minutes of inactivity. The User must then log on again to re-connect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
- 12.7 Only PPA-approved VPN client software may be used.
- 12.8 By using VPN technology on 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 existing security policies.

13. REMOTE ACCESS AND COLLABORATION TOOLS

13.1 Remote Access

- 13.1.1 Access to PPA Systems and workstations through remote connection is allowed provided that, safety access protocols are followed.
- 13.1.2 Only those employees/consultants/contractors with approved work-from-home arrangements can connect to the networked systems of PPA.
- 13.1.3 PPA-authorized remote access shall be strictly for official use.
- 13.1.4 SSL VPN accounts shall undergo proper naming convention to determine the proper identification of remote access users.
- 13.1.5 Employees electing to use remote access shall be responsible for ensuring that their home desktop/laptop is free from viruses, malware, Trojan, and other malicious software.
- 13.1.6 Remote Access sessions to workstations requested by work-from-home personnel shall be done by the ICTD Technical team to be accompanied by an RC personnel on duty to ensure secured access to office premises.
- 13.1.7 Employees remotely accessing workstations are not allowed to make modifications of any kind to software installed in it without the express approval of ICTD.
- 13.1.8 Remote Access to workstations in the Head Office shall only be allowed from 9:00 AM until 4:00 PM from Monday to Friday to provide time for security and housekeeping protocols.
- 13.1.9 Once the Agency's desktop/workstation is successfully accessed, it is recommended that the user store or upload all needed files in PPA's Cloud Storage in Microsoft OneDrive for easier file access/retrieval. Cloud Storage is available 24/7 and can be accessed through the internet without having to connect to remote access.
- 13.1.10 Access to the workstation through remote connection shall be limited to the requesting personnel's designated computer unit only. Accessing any other workstations is prohibited unless approved by the Head of the requesting unit. The purpose for remote access should be properly indicated in the IT Service request form.

- 13.1.11 Remote access to the company's desktop/workstation shall be limited to one-time access only or unless deemed necessary especially for WFH arrangements.

13.2 Collaboration Tools

- 13.2.1 Use of collaboration tools is allowed provided that, safety access protocols, as well as online work etiquettes, are followed.
- 13.2.2 Ensure that the connecting desktop/laptop is free from viruses, malware, Trojan, and other malicious software when using collaboration tools.
- 13.2.3 Send invitations to participants through official email or direct messages on official messaging applications only to prevent unauthorized participation and compromise the web host channel.
- 13.2.4 Use a complex password or meeting identification to prevent intruders from joining when hosting a web conference or an online meeting.
- 13.2.5 Utilize the use of status indicators to inform other members of availability.

13.3 Management of Remote Access & Collaboration Tools

- 13.3.1 The ICTD Technical Group in the Head Office and designated Site Administrators at the Port Management Offices shall ensure the use of authorized remote access and collaboration tools is suitably controlled within their area of responsibility in line with the objectives of this policy.
- 13.3.2 ICTD reserves the right to implement strict technical controls whenever necessary to prevent the use of remote access and PPA-managed collaboration tools in certain circumstances.
- 13.3.3 ICTD reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of end users to transfer data to and from specific resources while connected via remote access.
- 13.3.4 ICTD shall monitor and record information as regards each user's access and/or connection to PPA's networks when remote access is detected.
- 13.3.5 ICTD, using authorized monitoring tools, shall record the dates, times, duration of access, etc. to detect unusual remote access patterns or other suspicious activity. This is done to deter unauthorized access to accounts/computers electronic devices, or networked resources. In all cases, data protection remains PPA's highest priority.

- 13.3.6** ICTD may control and administer all PPA corporate email and SSL VPN account, including modifying and terminating user access upon request of the immediate supervisor/unit head of the user or due to suspicious activity detected.
- 13.3.7** Failure to comply with these guidelines, may, at the full discretion of PPA Management, result in the suspension of any or all technology use, and connectivity privileges as well as disciplinary action when warranted.

14. FIREWALL SECURITY

- 14.1 All internet connectivity paths, and internet services must pass through firewalls for security, control, and restrictions.
- 14.2 Firewall backup files must be kept close to the server at all times.
- 14.3 All firewall servers must be placed in a physically secured area accessible only to authorized ICTD personnel.

15. AUDIT

- 15.1 When requested and for the purpose of performing an audit, any systems access needed will be provided to members of the Audit Team.
- 15.2 Database Administrators shall continuously monitor/audit User access to sensitive objects as well as actions on the database.
- 15.3 All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
 - 15.3.1 All security-related logs will be kept online for a minimum of one (1) month.
 - 15.3.2 Daily incremental data backup logs will be retained for at least one (1) month.
 - 15.3.3 Weekly full data backup logs will be retained for at least one (1) month.
 - 15.3.4 Monthly full data backup logs will be retained for a minimum of two years.
- 15.4 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. Said logs are important for error correction, security breach investigations, and any other related tasks.

16. ACCEPTABLE USE OF COMPUTER EQUIPMENT

- 16.1 All employees will only use the ICT Equipment for its authorized purposes. Use of IT equipment for personal benefit, business, or partisanship is strictly prohibited.
- 16.2 All users are required to lock their desktop computers or laptops when not in use or they are away from their desks. An automatic screen saver that can only be turned off with a password set to 10 minutes must be used when you leave your workspace.
- 16.3 Changes in configuration and settings such as installation, modification of hardware or software, and removal of software, databases, and operating system in all IT equipment shall only be done by authorized ICTD personnel.

16.4 Bring Your Own Device (BYOD)

This policy establishes the PPA ICT Policy guidelines for PPA employees, Contractors, Consultants, guests, and Third-party service providers' use of personally owned electronic devices for work-related purposes.

- 16.4.1 The following are the equipment covered by the Bring Your Own Device (BYOD) policy including but not limited to:
- Desktops, laptops, and tablet computers
 - Smartphones (defined as any cellular telephone that connects to the internet via Wi-Fi or a mobile provider network)
 - Flash, memory, and/or thumb drives, and external hard disks
 - iPods, MP3 media players, and similar entertainment and portable music devices that connect to WiFi networks.
 - Wearable devices such as watches, VR headsets, and augmented reality glasses with WiFi or Bluetooth
- 16.4.2 All Bring Your Own Device (BYOD) owners are required to have written approval from their respective supervisor before entering the office premises and will only be used for work-related activities.
- 16.4.3 Connection of BYOD to the PPA network will only be permitted with the approval of the RC department head and ICTD.
- 16.4.4 For desktop PCs, laptops, tablets, and smartphones, ICTD personnel must ensure that the BYOD device

has a licensed Operating System installed and must be equipped with an up to date Antivirus software against viruses, spyware, and other malware infections.

- 16.4.5 All BYOD Equipment is prohibited to bypass any of PPA's hardware and software security measures by using Virtual Private Network (VPN) applications and other Internet proxy sites among others that may pose a threat to the systems and networks or that could introduce application incompatibilities (any such findings should addressed first or be removed altogether before proceeding).
- 16.4.6 Upon resignation or termination of employment, or at any time upon request, the PPA employee may be asked to produce the personal device for inspection. All Agency data on personal devices will be removed by IT upon the termination of employment.
- 16.4.7 For security, data protection, and network maintenance designated ICTD personnel has the authority to access, inspect, monitor, remove, and restrict ICT resources (both PPA assets and BYOD) at any time.

17. INFORMATION TECHNOLOGY (IT) ASSET

The following are the procedures that must be observed for the effective maintenance of IT assets.

17.1 Software and Other Applications and Operating System

To minimize the risk of corruption to operating systems or Integrated applications, the controls shall include, but not necessarily be limited to, the following:

- 17.1.1 ICTD-ADSD shall retain user documentation including licenses and technical specifications of information systems software.
- 17.1.2 ICTD-ORSD and/or ADSD shall perform updating of the operating systems and program/application backups when necessary.
- 17.1.3 ICTD-ORSD and/or ADSD shall apply update patches to the operating system and/or application software only after full functionality has been verified through applicable testing methods (unit, integration, regression, etc.)
- 17.1.4 ICTD-ADSD shall ensure that change control procedures are documented and followed during the scheduled software maintenance and take into consideration the following:
 - The approval and notification process
 - Interfaces with other applications, systems, or processes
 - External agency and departmental interdependencies
 - Change categories, risks, and type.
 - The change request process
- 17.1.5 When special or emergency situations make it necessary to perform maintenance operations outside of the normal system operations schedule, these situations must be documented, and all affected users duly notified.
- 17.1.6 When maintenance support is provided by a third party, nondisclosure statements shall be signed by authorized representatives of the third party entity before any maintenance support is performed.
- 17.1.7 External Support Group/Vendor or Supplier of outsourced software shall be given physical and logical access a level supported by Service Level Agreement (SLA).
- 17.1.8 External Support Group activities shall be continuously controlled and monitored by designated ICTD personnel.

17.1.9 ICTD-ADSD shall maintain records of all updates and/or modifications performed on any in-house and outsourced software application ensuring the correct version of such software.

17.2 Hardware and Peripheral Devices

17.2.1 ICTD-ORSD shall retain user documentation and technical specifications of information technology hardware.

17.2.2 Documentation shall be secured from unauthorized use and made readily available to support system maintenance and system support staff.

17.2.3 ASD-PMD with the assistance of ICTD shall identify and record its information technology (IT) hardware assets in a formal hardware inventory/register.

17.2.4 ASD-PMD shall identify and mark all IT hardware with agency-unique physical asset tags and that the inventory/register is kept up to date.

17.2.5 The formal hardware inventory shall include all information necessary that will identify the date purchased, warranty period, serial number, location, existing user, and other relevant information.

17.2.6 ICTD-ORSD shall provide or arrange maintenance support for all critical/production IT equipment located at the Head Office, Central Facility, and Data Recovery Center that is owned, leased, or licensed by the PPA Head office.

17.2.7 The PMO through its designated Site Administrator shall provide or arrange maintenance support for all PPA IT assets and equipment located at its office, base port, and terminal ports under its jurisdiction.

17.2.8 When necessary, ICTD and PMO shall arrange support services through appropriate maintenance agreements or with qualified technical support staff.

17.2.9 When maintenance support is provided by a third party, nondisclosure statements shall be signed by authorized representatives of the third party before any maintenance support is performed.

17.2.10 ICTD-ORSD shall maintain records of all maintenance activities performed on any PPA's IT assets.

17.3 Monitoring Tools and Access Configuration

- 17.3.1 ICTD-ORSD shall use a comprehensive set of management tools (e.g., maintenance utilities, remote support, enterprise management tools, and backup software) in order to monitor and update on the current state and utilization of IT assets and facilities. (e.g., patch management processes, incremental software updates, etc.)
- 17.3.2 ICTD-ORSD shall monitor information systems (e.g., using Simple Network Management Protocol (SNMP)) so that events such as hardware failure and security incidents can be detected and responded to effectively.
- 17.3.3 ICTD-ORSD shall review maintenance records on a regular basis to verify configuration settings, evaluate password strengths and assess activities performed on the server (e.g., by inspecting activity logs).
- 17.3.4 ICTD-ORSD shall ensure that user access rights and privileges are clearly defined, documented, and reviewed for appropriateness.
- 17.3.5 ICTD-ORSD shall consider the risk of exposure when administering system resources.
- 17.3.6 ICT-ORSD shall take reasonable actions to ensure the authorized and acceptable use of data, networks, and communications transiting the system or network.

17.4 Backup Power Generators

- 7.4.1 ASD shall ensure the availability of Backup Power Generators that can provide uninterrupted electrical supply during power outages. When a backup generator is employed, ASD/PMO shall observe the following requirements.
 - Regularly inspect the generator to ensure it remains compliant with both safety and manufacturer maintenance requirements, and either has an adequate supply of fuel (for internal combustion generators) or has sufficient charge (for stored battery banks).
 - Ensure the generator has the capacity to sustain the power load required by the attached equipment for a prolonged period of time.
 - Ensure the generator is tested according to the manufacturer's specifications.

- Ensure that personnel are fully trained to operate and maintain the backup power generators to avoid the risk of fire or damage to IT facilities/equipment.
- Backup generators are usually combined with a smaller battery-based uninterruptible power supply to protect critical information technology systems that demand high availability. Such a combination supports an orderly shutdown if the generator fails, minimizing potential for equipment damage or data loss, and can also provide continuous business operations if the cutover to the generator is too slow to provide power immediately with no interruption.
- ASD shall prepare a contingency plan to be followed in the event the lockup generator fails.

17.5 Fire Suppressing Equipment

17.5.1 ASD shall ensure the availability of fire-suppressing equipment that will protect the Agency's IT assets. When a fire suppressing equipment is used, ASD/PMO shall observe the following requirements:

- Regularly inspect the fire-suppressing equipment to ensure it remains compliant with relevant industry safety standards and manufacturer maintenance requirements.
- Ensure that the fire-suppressing equipment is tested according to the manufacturer's specifications.
- Ensure that designated personnel is fully trained and knowledgeable in operating such equipment to avoid unnecessary damage to PPA IT facilities/equipment.

17.6 Disposal of PPA IT Assets and Resources

17.6.1 Based on existing inventory, ICTD shall identify all IT assets (software, software licenses, hardware, and peripherals) which have reached its end-of-life and/or end-of-support.

17.6.2 If the asset is beyond repair, such shall have to be returned to ASD-PMD for proper inventory and disposal.

17.6.3 The Site Administrator from the PMO and/or ICTD Technical Support Group shall ensure the removal of the IT asset for disposal or any of its components from the equipment.

17.6.4 The Site Administrator from the PMO and/or ICTD Technical Support Group shall sanitize the equipment to remove restricted or highly all sensitive information from

associated media, following proper procedure, when the information system or any of its components require a disposal process.

17.6.5 The PMO/RC property custodian shall accomplish a Property Return Slip and submit it to ASD-PMD together with the item/s to be returned.

17.6.6 ASD-PMD shall inspect the returned property and acknowledge receipt accordingly.

17.6.7 ASD-PMD shall update the inventory of assets and conduct an inspection of unserviceable equipment or property to verify justification for disposal.

17.6.8 ASD-PMD shall categorize each and every asset for disposal, appraise the equipment and prepare an Inspection Report which shall indicate the following information:

1 - description, quantity, and specifications of the equipment or property

2- date of purchase

3- acquisition cost

4 - physical condition

5-appraised value

6 - remarks/recommendations

17.6.9 The modes of disposal shall follow the Manual on Disposal of Government Properties, existing Commission on Audit Regulations, and other related issuances.