| | | |
|---|---|---|
| MAYNILAD | INFORMATION SECURITY POLICY | |
| | Policy No.: PS-ITS-004-2023 | Effective Date: August 31, 2023<br>Revision No.: 0 |

## I. PURPOSE AND SCOPE

The purpose of this Policy is to safeguard information belonging to Maynilad and its stakeholders (third parties, clients or customers, and the general public) within a secure environment. This Policy informs all Maynilad employees and other individuals entitled to use Maynilad facilities, information, or data on the principles that govern the holding, use, and disposal of information.

## II. DEFINITION OF TERMS

1. **ACCESS CONTROL** – The selective restriction of access to a place or other resource.

2. **ANTI-VIRUS SOFTWARE –** Designed to detect and remove viruses from computers and can also protect against a wide variety of threats, including other types of malicious software such as keyloggers, browser hijackers, Trojan horses, worms, rootkits, spyware, adware, botnets, and ransomware.

3. **ANTI-MALWARE SOFTWARE –** A type of software program designed to prevent, detect, and remediate malicious programming on individual computing devices and IT systems.

4. **AUTHORIZATION –** Specifying access rights to resources related to information security and computer security in general and to access control in particular.

5. **AVAILABILITY –** Ensuring that authorized parties are able to access the information when needed.

6. **CONFIDENTIALITY** – Protecting the information from disclosure to unauthorized parties.

7. **ENDPOINT –** any device such as a PC, laptop, tablet, or smartphone that is connected to the Maynilad network.

8. **ENCRYPTION –** is a process of converting data into a coded or scrambled form in order to prevent unauthorized access, tampering, or interception during transmission or storage.

9. **INTEGRITY –** Protecting information from being modified by unauthorized parties.

10. **MALWARE** – Software that is intended to damage or disable computers and computer systems.

11. **PHISHING** – Unsolicited email that scammers use to collect personal information from unsuspecting users.

12. **REMOTE ACCESS –** Terminal emulation to remotely control a computer system.

13. **SECCAB (Security Change Advisory Board) –** A change management for security-related controls or any change in configuration that has security implications.

14. **SECURITY INCIDENT** – refers to any event or occurrence that poses a potential threat to the security of an organization's information systems, data, or network infrastructure.

15. **VIRTUAL PRIVATE NETWORK (VPN)** – is a technology that creates a secure and encrypted connection between your device and the internet.

## III. GENERAL POLICY STATEMENT

Maynilad (or the "Company") establishes and enforces security over its network system and corporate data to protect it against all forms of threats or intrusion, whether deliberate or accidental, thus preserving the company's information and system resources' availability, confidentiality, and integrity.

It is the goal of Maynilad that:

- Information will be protected against unauthorized access or misuse.
- Confidentiality of information will be secured.
- The integrity of the information will be maintained.
- The availability of information and information systems are maintained for service delivery.
- Business continuity planning processes will be maintained.
- Regulatory, contractual, and legal requirements will be complied with.
- Physical, logical, and communications security will be maintained.
- Disposal of information that is no longer in use will be done in a suitable manner.
- All information security incidents will be reported to the IT Security Head and investigated through the appropriate management channel.

It is the Company's policy to provide the most appropriate and effective means and levels of security—encompassing physical, technological, or logical/system access provisions—to protect the company's system resources and information. Complementary to this is the responsibility of all employees, including contractors and service providers who are engaged by Maynilad, to preserve the company's information from any unauthorized disclosure or transmission.

## IV. DISTRIBUTION

This policy shall apply to all individuals authorized by Maynilad to use and access IT resources, which include regular and project-based employees, service providers, contractors, and other third parties.

## V. POLICIES AND STANDARDS

### A. Organization of Information Security Policy

Information Security governance and compliance are the responsibility of the IT Security Head, which directly reports to the Chief Information Officer ("CIO") of Maynilad.

Maynilad has established a Security Council with security responsibilities and roles shared across the Information Technology Services ("ITS") Division.

### B. System Security Policy

#### 1. User Access Management

a. ITS grants and maintains user access to any Maynilad operational systems and other critical non-productive systems. This includes the enablement of endpoint devices that may be allowed to connect to the Maynilad intranet network and their associated assets.

b. ITS shall ensure that user access control procedures for each application and information system are documented, implemented, and kept up-to-date. Authorization shall only be provided based on the level of access required to perform their duties in conformity with the defined roles/functions in the approved business process. Refer to the *Access Privilege Matrix* for the specific roles and access per system.

c. Employees availing of early retirement, extended or prolonged leave of absence, or resignation shall conform to clearance procedures to remove their access to the different Maynilad systems. A list of employees who have resigned, retired, or are on AWOL (absence without official leave), including those transferred or realigned due to organizational changes/restructuring shall be made available by Human Resources ("HR") to ITS for the necessary updating of user access.

d. ITS, on the other hand, shall provide the following list of user accounts to HR every month:

(i) without any activity for the last 30 days for deactivation
(ii) without any activity for the last 90 days for deletion

HR shall review and confirm within the prescribed period the necessary action for the submitted list of user accounts.

## 2. Network Administration and Firewall Mangement

a. All end-users, including service providers, contractors, project-based employees, OJTs (on-the-job trainings), and employees of subsidiaries who need to access the Maynilad network shall be required to have an AD (active directory) account.

b. ITS shall ensure that the appropriate firewall infrastructure and technology are in place to protect the company's systems and information. All of Maynilad's laptops and desktops should have their firewall enabled and be properly configured and maintained. A review of firewall security settings and Maynilad's Firewall Policy shall be performed by ITS on a regular basis.

## 3. Password Management

A strong password should be registered and used by the end-users. The password should comply with the AD password complexity policy and the *IT Security Guidelines*. End-users are ultimately responsible for the safeguarding of their passwords.

## 4. Protection from Virus

All servers and computer equipment attached to the Maynilad network must have standard, supported anti-virus and anti-malware software installed. This software must be active to perform virus checks at regular intervals and have its virus definition files kept up-to-date. End-users are prohibited from bypassing, disabling, or tampering the installed security and antivirus systems managed by ITS.

## 5. Confidential Information or Documents

a. End-users with sensitive and confidential information/data for transmission shall be required to secure the data.

b. All file servers shall be the responsibility of their respective owners, i.e., the Business Area or Department that requested to use them as their data repository. Any damage to or loss of data in such repository shall be their accountability.

c. Only the use of an authorized Maynilad Cloud Storage and email is allowed for file sharing and storage of critical and confidential files or data.

### 6. Physical Access to ITS Facilities

a. Only ITS authorized personnel are allowed access to critical IT facilities and equipment, such as, but not limited to, the data center/server room, servers, network switches, and network equipment. Access to any IT facility and equipment must be approved by the IT Head or IT Security Head.

b. Employees shall also be responsible for securing and protecting the IT facilities and equipment located in their respective offices. They will be held liable for any form of destruction or unauthorized access to any IT assets or facility.

## C. Server Security Policy

### 1. Physical Security

a. ITS shall ensure that all servers are placed inside a secured room, preferably a dedicated room. Each room shall have door locks or access door locks. Servers shall be configured to disable booting from optical drives, external drives, and USB devices. It is a must to make backups of important data and store the tapes in a fireproof safe, preferably not in the same location as the server.

b. Regular review of backup policies and procedures must be observed. Regular checking and review of backup restoration shall be performed by the IT Infrastructure Head to ensure that systems and data can be restored in a timely manner as needed or in the event of disasters.

c. All critical servers should be connected to a UPS to prevent improper shutdown during power outages, which may result in system failures and data corruption.

d. Refer to the *Security Procedures on Access Control (SCM-OP-ADM-SEC-01)* for other details on physical security.

### 2. Operating System (OS)

a. Critical and important security updates must be applied to the servers based on an agreed schedule to prevent software errors or unexpected behavior brought about by vulnerabilities to hackers and malicious codes. These are deployed alongside a defined rollback procedure by ITS.

b. ITS shall implement Active Directory, Group Policy and Domain security policies to secure the domain and systems. Such may include, but should not be limited to, using the appropriate server baseline configuration, complex passwords and a minimum password length, and restricting anonymous user access and shared names.

### 3. Account Security

a. Appropriate account lockout configuration due to an erroneous password should be determined and implemented by ITS to prevent dictionary attacks on all accounts (including the Administrator account).

b. All Administrator account passwords shall be complex and correspond to the prescribed minimum length of the password.

c. Each Administrator should have at least two (2) accounts, one for administrative use and one for regular usage. The administrative account shall only be used when necessary.

### 4. File Systems

a. ITS shall ensure that all hard drives follow the right partition indicated in the server security baseline. On Application servers, Programs and Data should be in different locations. Data should always be isolated from the OS and Applications and be backed up and restorable as such.

b. The root directory of a drive must never be shared. ITS is responsible to restrict the access since it is very dangerous to share the root of the drive where the OS is installed.

c. Logs must be configured and should be part of the Standard Server Build. Events to be logged must ensure that attacks, breaches, and inappropriate use can be detected. All logs must be stored and forwarded to a central logging server, including the setting up of alerts (email or SMS).

## D. Email Usage Policy

### 1. Granting of Email Accounts

a. Provision of e-mail accounts for Maynilad's Managers and above shall no longer require approval and shall automatically be configured along with the creation of an AD account. All other Maynilad employees below Managerial level shall require approval from the requesting Department Head.

b. Email naming convention shall conform to the following format:
(i) Maynilad employees:
*firstname.lastname@mayniladwater.com.ph*
*(e.g.* ***juan.delacruz@mayniladwater.com.ph****)*

(ii) Non Maynilad employees:
*initialoffirstnamelastname.department@mayniladwater.com.ph*
*(e.g.* ***jdelacruz.its@mayniladwater.com.ph****)*

(iii) Other Maynilad subsidiaries (e.g. PhilHydro):
*initialsoffirstnameandmiddlenamefulllastname@philhydro.com*
*(e.g.* ***jmdelacruz@philhydro.com****)*

(iv) Group or Shared Accounts:
*department/division.groupname@mayniladwater.com.ph*
*(e.g.* ***its.servicedesk@mayniladwater.com.ph****)*

### 2. Use of Email

a. Individual email accounts should always be kept secure and should not be shared unless it is a group email account.

b. Email account details (e.g., contact details, position, department, etc.) should always be updated. It is the employee's responsibility to inform the IT Service Desk should there be changes to be made.

c. Maynilad email account owners shall be responsible for the proper use of their email. They shall observe the prescribed company signature and disclaimer when sending or replying to emails. Sending junk emails is strictly prohibited and considered unacceptable behavior under the Maynilad Handbook.

### 3. Removal of Email Access

a. Email accounts shall be deactivated by ITS upon receipt of notice from:

(i) HR for employees' termination, resignation, retirement, or prolonged leave for more than 14 working days; or

(ii) Units concerned for the end or termination of contract agreements for service providers, contractors, or vendors with temporary business engagements with Maynilad.

b. It is the responsibility of the email account owner to backup their mailbox and make sure that proper turnover to their immediate superior has been done before the last day of the end-user's access.

c. ITS is authorized to revoke e-mail accounts should it be investigated that improper and abusive use of e-mail has been committed.

## E. IT Software Management

### 1. Software Purchase and Acquisition

a. All software and software projects to be acquired or used by Maynilad shall be evaluated for data privacy compliance by the Enterprise Risk Management and Internal Audit Division ("ERMIA") and approved by ITS. Approval of purchases shall follow the existing policy on the Procurement of Goods and Services.

b. Maynilad Employees shall conform to the use of all acquired licensed software in accordance with the software licensing agreement. Deviation from this agreement, such as copying installers for backup purposes, may be allowed provided there is concurrence by the vendor and that the copy shall only be kept and used by ITS.

c. ITS shall have custody of all the software installers, optical storage media, and license keys of all licensed software acquired, including the software licensing agreement.

2. **Software Use and Installation**

   a. Only ITS is allowed to install software or give access to a cloud/web-based application on Maynilad computers and mobile devices.

   b. As much as possible, only Maynilad-issued devices will be used when undertaking official Maynilad transactions/business. In case there is a need to use a personal device, failure to comply with Maynilad's IT Security standards and policies will hold the user liable and accountable.

   c. ITS shall ensure that only licensed or authorized software is installed. Shareware, freeware, cloud/web-based, and non-standard software that may contribute to end-users work efficiency must undergo software evaluation and approval by the IT Infrastructure Head, IT Security Head, or CIO prior to installation or use.

   d. Any software and cloud/web-based application that will process (i.e., collect, use, store, transfer, and delete) personal data shall be evaluated through the conduct of a Privacy Impact Assessment ("PIA") reviewed and approved by the Data Protection Officer ("DPO") and IT Security Head. This is also applicable should there be a change in the usage or process of the software or cloud/web-based application after it has been authorized for use.

3. **Software Maintenance**

   ITS shall ensure the following:

   a. Determine a proper rollback strategy before any software deployment is made. For security-related patches, these are immediately implemented with a rollback strategy in place.

   b. Updated software patches are applied on a regular basis to create a consistent, configured environment and reinforce security against known software vulnerabilities.

   c. Monitor the allocation and installation of all authorized licensed software. ITS shall update records of these, including upgrades and maintenance agreements.

   d. Support only authorized, licensed cloud/web-based applications. ITS may, however, still authorize the installation of unlicensed applications (including freeware or shareware), whether cloud-based or installed software, if properly justified.

4. **Software Monitoring**

   a. ITS shall maintain a list of authorized software. Any software installed or cloud/web-based application used on computers or mobile devices not included in the list or without the approval of ITS and/or the DPO is considered unauthorized. The list of authorized software shall be reviewed annually.

   b. ITS, the DPO, or Internal Audit shall conduct a random and on-the-spot check of computers and mobile devices for any unauthorized software. Those found stored shall be automatically removed or blocked from Maynilad's network.

c. Employees found installing unauthorized software shall be reported in writing to the employee's department head or immediate superior, copy furnished to the HR Division, for the appropriate sanction under the Maynilad Standards of Discipline.

### 5. Encryption Policy

a. All Company-owned laptops issued to the Top Management Team and Critical Users shall be encrypted with the minimum Advanced Encryption Standard (AES) algorithm and a 256-bit key to prevent or lower the risk of brute force attacks. It is required to be used, unless in exceptional instances where this is not deemed necessary. Any exception shall require approval from SECCAB.

b. ITS User Support shall be responsible for ensuring that all laptops and desktops are encrypted prior to the distribution to the end-user.

c. Only ITS-approved encryption solutions shall be used. All Private Keys shall be secured on an encryption server and can only be accessed by authorized ITS users.

d. Portable devices such as USB sticks, portable hard drives, and recording devices are at higher risk of loss or theft. It is the responsibility of the Critical Users to ensure that these devices are also encrypted to prevent loss or compromise of data.

e. Transfers of data done outside of the Maynilad corporate network shall only be made through Maynilad's official VPN with a minimum of AES 256 encryption.

f. All internet-facing web applications shall require an SSL certificate, and the Cipher suite should be enabled with a minimum of AES 128-bit encryption to establish a secured and private link between a web server and a browser.

## F. Security Change Management

Changes in the system, endpoints, server, and network infrastructure that may have IT security implications will require SECCAB approval depending on the requirements of the request. Refer to the *IT Security Guidelines* for details.

## G. ITS Project Management

1. During the initial assessment of the proposed ITS project, compliance with IT security and data privacy requirements should be taken into account. This forms part of the criteria for determining whether the project will proceed or not.

2. In all succeeding phases of the ITS project, from design, development, and testing, IT security and data privacy features shall be considered and incorporated.

## H. Software and Hardware End of life

ITS shall purge all information residing on the servers and systems prior to its decommissioning.

## I. Mobile Device

### 1. Device Management Configuration

a. Devices must have a strong password or passphrase, fingerprint, or facial recognition enabled for authentication.

b. Devices must be encrypted or password-protected to protect sensitive data stored on the device.

### 2. Mobile Application Usage

a. Employees should only download applications from official and trusted sources, such as authorized application stores (e.g., the App Store or Google Play). It is prohibited to download or install applications from unknown or untrusted sources.

b. When accessing the organization’s network remotely, employees should use a secure VPN connection to encrypt data transmission. Refer to the *Mobile Communication Policy* for more details

### 3. Responsibility and Accountability

The Employee shall be responsible as follows:

a. Ensure the security of his/her mobile devices (e.g., encrypted or password protected), including taking appropriate measures to protect them against theft, loss, or unauthorized access.

b. Sensitive company information should not be stored on personal mobile devices unless explicitly approved by the Division Head.

c. Adherence to the Information Asset Classification and Protection Policy when accessing, storing, or transmitting company data using mobile devices.

## J. Computer Peripherals and Other IT Equipment Policy

1. IT equipment should be identified, and an inventory of these assets should be drawn up and maintained by ITS.

2. Proper care and appropriate use of IT equipment are required from end-users.

3. Equipment such as computers, laptops, etc. should be verified to ensure that any corporate data, confidential information, and licensed software have been securely removed or overwritten prior to disposal or reuse. Confidential information stored on removable media and other storage devices should be kept safe and/or securely removed from these devices in accordance with the *Information Asset Classification and Protection Policy*.

Refer to the *Computer Peripherals and Other IT Equipment Policy* for more details.

### K. Incident Management

1. A formal incident management process should be established.

2. All employees have the responsibility to report any security incident or any observed or suspected incident.

3. Information security incidents should be responded to in accordance with the documented incident response procedures. Refer to the *Computer Security Incident Response Plan (CSIRP) Manual* for details.

### L. Clear Desk and Clear Screen policy

1. All employees must clear their workstations of any sensitive or confidential information at the end of the workday.

2. Computer screens should be locked or turned off when employees are away from their workstations.

3. Personal belongings should be kept to a minimum, and clutter should be avoided.

4. Employees should dispose of confidential documents and waste properly, using designated shredders or disposal bins.

5. Any portable storage devices (e.g., USB drives) should be stored securely when not in use.

### M. Acceptable Use of IT Resources

1. The acceptable use of computer laptops, or desktops, and all IT assets like systems, equipment, network devices, applications, or servers shall be indicated in the "important notice" screen upon the Windows OS login of the employee or any Maynilad-authorized individuals.

2. By logging in to the computer, the Employee or Maynilad authorized individual agrees to the Maynilad ITS and Data Privacy policies, including the terms and conditions on the acceptable use of IT resources.

## VI. VIOLATIONS OF THE POLICY

Any violation of this policy will merit the imposition of appropriate disciplinary action in accordance with Maynilad Employee Handbook and Standards of Discipline.

## VII. MONITORING AND REVIEW

A. ITS shall regularly review the implementation of this policy, and initiate its revisions/updating, as may be necessary under the circumstances.

B. The Internal Audit shall periodically review compliance with and/or effectiveness of this policy, and recommend necessary or appropriate changes therefor.

## VIII. REFERENCES

A. System Security Policy
B. Server Security Policy
C. Email Usage Policy
D. IT Software Management Policy
E. Encryption Policy
F. ITS Projects Policy
G. Computer Peripherals and Other IT Equipment Policy
H. IT Security Guidelines
I. CSIRP Manual
J. Supply Chain Management Security Procedures on Access Control
K. Mobile Communication Policy
L. HR Memorandum on Clean Desk and Clear Screen Policy