EMAPTA

Data Classification and Handling Policy

PROTECTED

DOCUMENT CONTROL NO.: EVSI.ITD.00.00.00
EFFECTIVITY DATE: July 2024

TABLE OF CONTENTS

1. OVERVIEW

1.1. In today's digital age, the protection of sensitive information is paramount for businesses to maintain trust with their clients, comply with regulatory requirements, and safeguard their reputation. As such, EMAPTA has developed this Data Classification and Handling Policy to establish clear guidelines for the classification, protection, and handling of data across all levels of the organization.

2. OBJECTIVE

2.1. The objective of this Data Classification and Handling Policy is to (a) provide a framework for classifying data based on its level of criticality and sensitivity to EMAPTA and (b) establish a system for protecting this information in all its forms and media. This includes the protection of both internal and customer data, considering compliance with statutory and regulatory requirements under ISO27001, ISO27701, Philippine Data Privacy Act, Payment Card Industry Data Security Standard (PCI-DSS), General Data Protection Regulation (GDPR), among others.

3. SCOPE

3.1. This policy applies to all employees, contractors, and third-party partners who have access to data within the organization, including data in all forms and media processed by EMAPTA.

4. DEFINITION OF TERMS

4.1. **Data Classification:** The process of categorizing data based on its level of sensitivity, criticality, and regulatory requirements within an organization.

4.2. **Data Owners:** Individuals within EMAPTA who are assigned responsibility for acquiring, creating, and maintaining information and information systems within their respective areas of jurisdiction.

4.3. **Data Custodians:** Personnel tasked with the physical protection, storage, and maintenance of data according to the classification level assigned by Data Owners.

4.4. **Data Handling Matrix:** Guidelines and procedures for the treatment and handling of data according to its classification level, ensuring consistent protection measures throughout its lifecycle.

5. ROLES AND RESPONSIBILITIES

5.1. **Data Owners:**

5.1.1. **Classification:** Responsible for classifying data at the time of creation or collection based on established classification levels.

5.1.2. **Review and Re-classification:** Regularly review the classification of data and re-classify if necessary to reflect changes in business needs or regulatory requirements.

5.1.3. **Defining Protection Measures:** Once the data is classified, data owners define the protection measures that align with the classification level.

5.1.4. **Access Control:** Define access controls and permissions, ensuring that access to data is restricted based on the principle of least privilege.

5.1.5. **Compliance and Training:** Ensure that all individuals with access to their data are informed of their responsibilities under the Data Classification and Handling Policy and are adequately trained in proper data handling procedures.

5.2. **Data Custodians:**

5.2.1. **Physical Protection:** Responsible for physically protecting, storing, and maintaining data according to the classification level assigned by Data Owners.

5.2.2. **Storage and Replication:** Create data repositories and transfer procedures to protect data, accordingly, ensuring consistency in classification and protection measures.

5.2.3. **Backup and Testing:** Ensure that all appropriate data is backed up and tested periodically as part of a documented, regular process.

5.2.4. **Disposal:** Handle data backups and disposal with the same security precautions as the data itself, ensuring data is certified deleted or disks destroyed consistent with industry best practices.

5.2.5. **Implementing Protection Measures:** Data custodians are responsible for implementing the protection measures defined by the data owners. This involves configuring systems, managing access controls, and applying security patches and updates.

5.3. **Information Security Team:**

5.3.1. **Policy Development:** Develop and maintain the Data Classification and Handling Policy, ensuring alignment with regulatory requirements and industry best practices.

5.3.2. **Training and Awareness:** Conduct regular awareness campaigns to reinforce the importance of data security and compliance with the policy among EMAPTA personnel.

5.3.3. **Monitoring and Enforcement:** Monitor compliance with the policy, investigate incidents or breaches, and enforce corrective actions as necessary to maintain data security and integrity.

6. DATA CLASSIFICATION LEVELS

6.1. **EMP-Classified:** Data that would likely cause serious harm to the organization when compromised or disclosed to unauthorized individuals. Strict security controls are required.

6.2. **EMP-Confidential:** Information that, if made available to unauthorized parties, may adversely affect individuals or the business of EMAPTA. It includes data required to be kept confidential by law, regulations, or confidentiality agreements.

6.3. **EMP-Protected:** Potentially sensitive information not intended for public sharing. Disclosure may cause damage to the company.

6.4. **EMP-Unclassified:** Information that may be freely disseminated without causing significant damage to the company.

7. DATA HANDLING

7.1. Guidelines for treatment and handling of data are defined by the Data Classification and Handling Matrix.

7.2. Data classification and its corresponding level of protection should remain consistent throughout replication and organization flow.

7.3. Data custodians must create data repositories and transfer procedures to protect data accordingly.

7.4. All appropriate data should be backed up, and the backups tested periodically, as part of a documented, regular process.

7.5. Backups of data must be handled with the same security precautions as the data itself. When systems are disposed of or repurposed, data must be certified deleted, or disks destroyed consistent with industry best practices for the security level of the data.

8. TRAINING AND AWARENESS

8.1. EMAPTA conducts regular awareness campaigns to reinforce the importance of data security and compliance with the Data Classification and Handling Policy.

9. REFERENCES AND RESOURCES

9.1. EMAPTA's Data Classification and Handling Policy is informed by relevant laws, regulations, standards, and best practices in data security and privacy. The following are key references and resources:

- 9.1.1. Philippine Data Privacy Act of 2012
- 9.1.2. ISO27001 Information Security Management System
- 9.1.3. ISO27701 Privacy Information Management System
- 9.1.4. Payment Card Industry Data Security Standard (PCI-DSS)
- 9.1.5. General Data Protection Regulation (GDPR)
- 9.1.6. National Institute of Standards and Technology (NIST) Cybersecurity Framework

9.2. For further information and assistance regarding data classification and handling, personnel are encouraged to refer to the above references or contact the EMAPTA Information Security team InfoSec@emapta.com.

10. DOCUMENTATION AND COMPLIANCE

10.1. Adherence to this policy is mandatory for all employees, contractors, and third-party service providers. Violations may result in disciplinary action, including termination of employment or contracts.

11. POLICY REVIEW

11.1. This policy will be reviewed annually or as required by changes in law or business requirements to ensure effectiveness and relevance.

12. EFFECTIVITY

This policy is effective immediately upon approval and will remain in effect until modified or rescinded by the company.

POLICY/PROCESS OWNER:	**Information Security Manager**
DOCUMENT CONTROL NO.:	**EVSI.ITD.00.00.00**
EFFECTIVITY DATE:	**July 2024**

	NAME / DESIGNATION	DATE
AUTHOR	**Luis Sicat III – Chief Information Security Officer (CISO)**	**June 2024**
REVIEWED	**Henry Vassall Jones – Chief Information Officer (CIO)**	**July 2024**
APPROVED	**Henry Vassall Jones – Chief Information Officer (CIO)**	**July 2024**

REVIEW AND REVISION HISTORY

DATE:	ACTION	Control No. (for Revision)	DESCRIPTION / COMMENT
July 2024	*Created*	*1.0*	*A policy for Data Classification and Handling Policy is created. Reviewed and approved.* *-Luis Sicat III-*