EMAPTA

Information Security Policy

PROTECTED

DOCUMENT CONTROL NO.: EVSI.ITD.11.00PM
EFFECTIVITY DATE: August 2024

TABLE OF CONTENTS

1. OVERVIEW

1.1. The Information Security Policy of Emapta establishes a set of guidelines and standards to protect the organization's information, information systems, and data for which Emapta is responsible. The policy aims to safeguard Emapta's information from unauthorized access, loss, or damage, and ensure compliance with relevant regulatory and contractual requirements. The policy supports the confidentiality, integrity, and availability (CIA) of information, applying to all forms of data—verbal, digital, and physical—whether individually controlled or shared, stand-alone, or networked.

2. OBJECTIVE

2.1. The primary objective of this Information Security Policy is to protect Emapta's information and information systems through a structured approach to information security. This includes:

2.1.1. Confidentiality: Ensuring that information is only accessible to those authorized to view it and protecting it from unauthorized disclosure.

2.1.2. Integrity: Preserving the accuracy and completeness of information by preventing unauthorized modifications.

2.1.3. Availability: Ensuring that information and critical services are accessible to authorized users when needed.

2.2. The policy aims to minimize risks related to information security and to foster a culture of security awareness and compliance among all employees and relevant external parties.

3. SCOPE

3.1. This policy applies to all Emapta employees, contractors, temporary staff, partners, and vendors who have access to Emapta's information. It encompasses all forms of Emapta information—whether verbal, digital, or physical—regardless of whether it is individually controlled or shared, stand-alone, or integrated into networked systems. The scope includes all activities related to the handling, storage, transmission, and disposal of information. Compliance with this policy is mandatory for all individuals and entities granted access to Emapta's information resources.

4. DEFINITION OF TERMS

4.1. **Acceptable Use -** Authorized and appropriate use of information assets, systems, and resources within the guidelines and policies defined by the organization.

4.2. **Authorization -** Establishing an individual's access level and/or grant access to information.

4.3. **Authorized Persons -** Means employees of Emapta that may be provided with access to Confidential Information in connection with the provision of the Services.

4.4. **Availability -** Ensuring that information is ready and suitable for use.

4.5. **Client Information -** Information that the Clients of Emapta own and have shared with only certain authorized personnel from Emapta (e.g., Offshore Talent of Client, Customer Experience Manager) for the purpose of delivering the agreed services to the Clients as part of Emapta's business model.

4.6. **Confidential Information -** Means any information, whether in physical or electronic format, disclosed, that is marked "Confidential," or would reasonably be considered to be confidential based on its nature or contents.

4.7. **Confidentiality -** Ensuring information is kept in strict privacy and protected.

4.8. **Emapta Information -** Information that Emapta owns, collects, processes, stores, shares, or destroys in carrying out Emapta's business model and providing services to Clients. This includes information contained in hard and soft copy documents or other media, communicated over voice or data network, or any form of exchanged conversation.

4.9. **Information Security -** Protection of information and information systems from unauthorized access, disclosure, alteration, destruction, or disruption in order to ensure the confidentiality, integrity, and availability of information.

4.10. **Information System -** Means any computer, server, storage device, networking equipment, or other equipment managed by Emapta and used to store, process or manage Emapta and Client Confidential Information.

4.11. **Integrity -** Ensures the accuracy, completeness, and consistency of information.

4.12. **PII (Personal Identifiable Information) -** Refers to information that can be used to identify or trace an individual's identity, such as name, address, date of birth, etc.

4.13. **Risk -** The potential for an event, action, or circumstance to have an adverse impact on an organization's objectives, including the security of information and information systems.

4.14. **Security event -** Refers to any occurrence or observable activity that has the potential to compromise the security of a system, network, or data. It includes both normal and abnormal activities that may be logged or detected by security tools or monitoring systems. Security events can serve as indicators of potential threats or vulnerabilities, but not all events result in security incidents.

4.15. **Security incident -** A security incident is anything that either already has or may immediately put Emapta information and systems at high risk of compromising their "CIA" (Confidentiality, Integrity, or Availability). Security incidents fall under the category of Major Incidents as defined in the IT Incident Management Policy.

4.16. **Sensitive Information -** Can refer to protected, confidential, or classified information.

4.17. **Sensitive PII -** Refers to personally identifiable information that is considered highly sensitive, such as financial information, medical records, biometric data, etc.

4.18. **Services -** Means all work performed by Emapta employees (i.e., Authorized Persons – see above) under the instructions provided by the Client.

4.19. **Unauthorized access -** Reviewing, copying, modifying, deleting, analyzing, looking up or handling information without authorization and legitimate business need.

5. ROLES AND RESPONSIBILITIES

5.1. Chief Information Security Officer

5.1.1. Responsible for overall information security strategy, program management, and ensuring the protection of the organization's sensitive data, systems, and infrastructure. Maintain a robust and resilient security posture and ensuring compliance with information security policies and regulations.

5.2. Chief Information Officer

5.2.1. Oversight of the company's Information Technology ecosystem and ensuring that information security is integrated within the company's technology processes and global technology services

5.3. Chief Technology Officer

5.3.1. Over-all responsible for secure development / project management / digital transformation and ensuring that all applications and systems owned by EMAPTA and used within the company adhere to strict software development standards and meet business objectives.

5.4. Information Security Department

5.4.1. Primarily responsible for enforcing compliance of in-scope individuals & entities with the company's Information Security Policy. Responsible for performing periodic checks and reviews of security controls and policies.

5.4.1.1. Develop, implement, and maintain security controls, procedures, and technical measures.

5.4.1.2. Conduct regular vulnerability assessments and penetration tests.

5.4.1.3. Manage network security, firewalls, intrusion detection systems, and antivirus solutions.

5.4.1.4. Monitor and respond to security events and incidents.

5.4.1.5. Provide security awareness training to employees.

5.4.1.6. Enforce access controls and user privileges.

5.4.1.7. Maintain and update security policies and procedures.

5.5. IT Service Center

5.5.1. Responsible for incorporating security best practices in the day-to-day IT operations and abiding by the Information Security Standards & Requirements within IT operations such as service desk, procurement & IT asset management, IT service delivery, and IT onboarding & offboarding.

5.6. IT Infrastructure

5.6.1. Responsible for secure systems & network operations, implementation of network infrastructure security controls, secure system administration practices, configuring remediation of system and network vulnerabilities, and availability of IT infrastructure components. Abide by all Security Standards & Requirements within the ISMS Manual relevant to infrastructure Department.

5.7. Global Technology Solutions Division

5.7.1. Implement secure coding practices, security project/product management practices, and follow secure software lifecycle development processes. Abide by all Security Standards & Requirements relevant to Application Security, Project Management, and Vendor Management within the Information Security Management System Manual Standards & Requirements.

5.8. Human Resources (People & Culture)

5.8.1. Responsible for screening employees, facilitating employment contractual agreements, organizational learning & development, and facilitating disciplinary process.

5.8.1.1. Implement security awareness training programs for employees.

5.8.1.2. Enforce security policies and procedures through employee onboarding and ongoing training.

5.8.1.3. Manage user access and account management processes.

5.8.1.4. Ensure compliance with security policies during employee offboarding.

5.8.1.5. Address security incidents involving employee misconduct or policy violations.

5.9. Facilities

5.9.1. Responsible for Physical and Environmental Security within Emapta premises and coordination with third-party logistics partners. Abide by Physical Security Standards & Requirements. Implement surveillance systems, alarm systems, and access control measures on premises. Monitor and respond to physical security incidents.

5.10. Legal and Compliance

5.10.1. Identification and compliance with applicable laws, regulations, and contractual obligations

5.10.1.1. Monitor and interpret applicable laws, regulations, and industry standards related to information security.

5.10.1.2. Develop and maintain policies to ensure compliance with legal and regulatory requirements.

5.10.1.3. Conduct risk assessments and audits to identify vulnerabilities and ensure compliance.

5.10.1.4. Provide guidance on legal and contractual obligations related to information security.

5.10.1.5. Coordinate response to legal and regulatory inquiries or breaches.

5.11. Marketing

5.11.1. Comply with Information Security Policy, Data Privacy Policy, and social media Policy upon producing materials available to the public or on the internet

5.12. Growth

5.12.1. Follow security rules in sharing or disclosing Emapta information to clients or prospective clients

5.13. Service Delivery

5.13.1. Client relationship management and raising information security concerns from clients and talents; partnering with key stakeholders for handling client concerns. Ensure Client’s security requirements are captured for proper implementation of security controls.

5.14. Project Managers

5.14.1. Incorporate and integrate information security within project management practices and project lifecycle

5.15. **Executive Management of Emapta**

5.15.1. Provide leadership, support, and resources for information security initiatives.

5.15.2. Approve and enforce the Information Security Policy.

5.15.3. Ensure alignment of information security with business objectives and risk management strategies.

5.15.4. Promote a culture of security awareness and compliance.

5.15.5. Promote a security-minded organizational culture and require everyone who processes Emapta and Client information to abide by Emapta's information security policy.

5.16. **All Employees and others granted use of Emapta information are expected to:**

5.16.1. Adhere to the Information Security Policy and related policies made available to them via company systems.

5.16.2. Use information systems and resources in a secure and responsible manner.

5.16.3. Understand the data classification as defined in Emapta's Information Security Policy.

5.16.4. As appropriate, classify information and apply commensurate protection to Emapta information.

5.16.5. Access, process, and store information only as needed to meet legitimate business needs.

5.16.6. Not to divulge, copy, release, sell, loan, alter or destroy any Emapta or Client information without a valid business purpose and/or authorization.

5.16.7. Protect the confidentiality, integrity, and availability of Emapta or Client information in a manner consistent with the information's classifications.

5.16.8. Handle any personal identifiable information in accordance with the Emapta Data Privacy Policy and other applicable Emapta policy and standards.

5.16.9. Safeguard any physical key, ID card, computer account, or network component that allows to access Emapta information.

5.16.10. Discard media containing Emapta information in a manner consistent with the information's classification, type and any applicable Emapta information destruction and retention requirements. This includes information contained in hard copy documents or any electronic, magnetic, or optical storage medium.

5.16.11. Contact Emapta Data Protection Officer or Information Security personnel prior to disclosing information generated or prior to responding to any litigation or law enforcement subpoenas, court orders, and other information requests from private litigants and government agencies.

5.16.12. Contact the appropriate Emapta office or department prior to responding to request for information from regulatory agencies, inspections, examiners and/or auditors.

5.16.13. Report promptly any identified or suspected security incidents via the appropriate security reporting channels

5.16.14. Ensure completion of the mandatory annual Information Security Awareness Course and Privacy Fundamentals Course

5.16.15. Create backups of official work files to authorized platforms (e.g., official company cloud drive account)

6. INFORMATION CLASSIFICATION

6.1. Emapta provides flexible, fast, efficient, and cost-effective services for a variety of clients worldwide. It is critical for Emapta to set the standard for the protection of information assets from unauthorized access, compromise, or disclosure. Emapta appropriately secures its information from unauthorized access, data loss and damages. Emapta has adopted this information classification policy to help manage and protect its information assets. (See classification table below)

Classification & Description	Examples	Business Impact
Unclassified - Information that is created within the business that does not cause damage to the company and to its employee or customer; including information deemed public by legislation or routine disclosure. Unrestricted information is available to the public, employees, and contractors working for the company.	▪ Sales materials ▪ Granted patents ▪ Job postings ▪ Published research Public announcement Press releases	▪ Minimal or no Impact. ▪ Does not contain intellectual or commercial information that gives business competitor an advantage. ▪ No risk if corrupted or modified.

Protected - Information that is sensitive outside that company and could impact service agreement or performance or may result in low levels of financial loss to individuals and/or companies. Protected information would include personal information, financial information or details concerning the effective operation of the company and its functional office. Protected information is available to employees and authorized non-employee (contractors, sub-contractors, and partners) possessing a related need to the business.	▪ Proposals and Bids ▪ Business Plans ▪ Sales Projections ▪ Documents containing personal information ▪ Internal company announcements	▪ Unfair competitive advantage ▪ Breach of statutory regulations on the information disclosure ▪ Minor infringement of the code of conduct applied ▪ Disruption to business if not available ▪ Could disadvantages the company in commercial negotiations with others ▪ Low degree of risk if corrupted or modified.
Confidential - Information that is sensitive within the company and could cause serious loss of privacy, competitive advances, confidence loss, damage to partnerships, relationships, and reputation of the company. Restricted information includes highly sensitive personal information. Confidential information is available only to a specific function, group, or role.	▪ Personnel files ▪ Salary information ▪ Industrial trade secrets ▪ Intellectual property ▪ Technical drawing and details ▪ Software Code ▪ Third Party business information submitted in confidence.	▪ Cause distress to individuals ▪ Major infringement of the applied code of conduct ▪ Loss of trade secrets/intellectual property ▪ Loss of reputation or competitive advantage ▪ Facilitation of improper gain ▪ Breaches in the confidence of information provided by third parties ▪ Loss of confidence in the company by employees, suppliers, and customers ▪ Loss personal or individual privacy ▪ Loss of opportunity (e.g. orders & customers) ▪ Financial loss High degree of risk if corrupted or modified.
Classified - Information that is extremely sensitive and could cause extreme damage to the integrity, image, or effective business performance of the company.	▪ Executive documents ▪ Management deliberations ▪ Personnel/Personal medical records	▪ Cause substantial distress to individuals ▪ Loss of jobs or livelihood ▪ Exploitation by criminal elements ▪ Significant financial loss

Extreme damage includes substantial financial loss, social hardship, major economic impact, and criminal prosecution. Secret information is available only to named individuals or specified positions on a strictly need to know basis.	▪ High level budget and business performance figures ▪ Procedural or criminal investigations ▪ Merger & acquisition documentations ▪ Information that prejudices public floatation or share price ▪ Strategic Negotiations ▪ Significant technological innovations.	▪ Substantial loss of competitiveness ▪ Compromise of legal system and board deliberations ▪ Destruction of partnerships and relationships ▪ Significant damage ▪ Sabotage/terrorism ▪ Impedes the effective operation of company policies ▪ Undermine the proper management of the company and its operations ▪ Extreme risk if corrupted or modified.

7. OVERVIEW OF TECHNICAL, PHYSICAL, AND ADMINISTRATIVE SECURITY MEASURES

7.1. Employees should protect Emapta or Client information. The following security measures should be in place in providing business services to Emapta's Clients to the extent that they're applicable:

7.2. Information Security and Data Privacy Program

7.2.1. Emapta shall maintain an Information Security Program and a Data Privacy Program ("Program"), in accordance with generally accepted industry standards and applicable privacy laws, sufficient to protect the Client's Confidential Information from disclosure to unauthorized persons, or its alteration, destruction, or loss of use. This Program will include, at a minimum, the specific security measures below for Emapta-owned assets, infrastructure, and information. Risk assessments or audits should be performed on a periodic basis to review compliance with the Information Security Program.

7.3. Access Control

7.3.1. Limit access to Emapta endpoints & Information Systems to Authorized Persons.

7.3.2. Limit access to Client Confidential Information and personal data to Authorized Persons with a business need to have access to that information.

7.3.3. Limit the types of transactions that can be performed within Emapta endpoints & systems on Client Confidential Information and personal data to those types for which the person has a business need.

7.3.4. Provide each Authorized Person authenticating to any Emapta endpoints & Information System with a unique user ID, not to be divulged to or shared with any other Authorized Person.

7.3.5. Employ the principle of least privilege, including for specific security functions and privileged accounts.

7.3.6. Employ the principle of separation of duties for access to Emapta Information Systems.

7.3.7. Remove or disable user accesses immediately within 24 hours upon effective offboarding or movement to another role.

7.3.8. Perform quarterly access management review to check appropriateness of access rights and identify accounts that should already be disabled.

7.3.9. Systems must limit unsuccessful login attempts to a maximum of 3 attempts. Account lockout policies will be implemented to prevent brute-force attacks.

7.3.10. Workstations must automatically lock after 15 minutes of inactivity to protect against unauthorized access.

7.4. Password Control

7.4.1. Password Requirements

7.4.1.1. Passwords must be at least 8 characters in length.

7.4.1.2. Passwords must include a combination of uppercase letters, lowercase letters, numbers, and special characters to ensure complexity and resistance to common attacks.

7.4.2. Password Management

7.4.2.1. Passwords must be changed at least every 60 days.

7.4.2.2. Users are prohibited from reusing the last 24 passwords.

7.4.3. Password Protection

7.4.3.1. Passwords must be stored securely using industry-standard encryption methods. Plaintext passwords are strictly prohibited.

7.4.3.2. Passwords must be hashed before storage to enhance security.

7.4.4. Authentication

7.4.4.1. Multi-Factor Authentication (MFA) is required for accessing sensitive information systems and performing critical operations, including password resets.

7.4.5. Password Recovery and Reset

7.4.5.1. MFA must be used for self-service password resets to verify the identity of the user.

7.4.5.2. The password recovery process must include secure procedures to prevent unauthorized password changes.

7.4.6. User Responsibilities

7.4.6.1. Users must create strong passwords that comply with the length and complexity requirements.

7.4.6.2. Users must not share their passwords with anyone or write them down in an unsecured manner.

7.4.6.3. Users must immediately report any suspected password compromise or unauthorized access to the IT security team.

7.4.7. Monitoring and Auditing

7.4.7.1. Logs of password changes, reset requests, and failed login attempts will be maintained and monitored for security purposes.

7.4.7.2. Regular audits will be conducted to ensure compliance with this policy and to identify any potential vulnerabilities.

7.5. Network Controls

7.5.1. Restrict physical, as well as login, access to networking equipment including routers, switches, firewalls, and access points, to staff authorized and to those who require access to this equipment based on official job responsibilities.

7.5.2. Maintain networking equipment and networking software with all vendor-recommended updates and patches.

7.5.3. Perform quarterly or as-needed vulnerability scans, firewall review, and remediations on network devices & servers.

7.5.4. Control and monitor all network access, including remote access.

7.5.5. Maintain logs of network access that are secured against tampering, alteration, deletion, or disclosure to unauthorized persons.

7.5.6. Require two-factor authentication, at a minimum, for privileged remote access.

7.5.7. Implement secure network segmentation that's separate from other network space for Tenants based on Client Account or Department.

7.5.8. Require authentications for all wireless access to networks.

7.5.9. Encrypt communications over wireless networks, using industry standard mechanisms, but in no case less secure than WPA-2.

7.5.10. Ensure that for all wireless access points, password, and encryption keys shall be changed from the default value.

7.5.11. Deploy VPN software on endpoints.

7.6. Patch Management

7.6.1. Maintain all Emapta servers and endpoints including any supporting infrastructure current with vendor recommended patches.

7.6.2. Enforce the policy for prompt application of vendor-recommended patches in accordance with their severity level and Emapta's Vulnerability Management Standards.

7.7. Configuration Management

7.7.1. Establish and maintain baseline configurations and inventories of IT infrastructure servers, endpoints, and network devices.

7.7.2. Establish and enforce security configuration settings for endpoints employed in Emapta's system via a remote monitoring & management tool.

7.7.3. Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.

7.7.4. Protect Client Confidential Information at rest using industry standard encryption mechanisms of a key length not less than 256 bits.

7.8. System and Information Integrity

7.8.1. Install and maintain anti-malware and host-based intrusion prevention system on all Emapta endpoints for detection and prevention of active exploits.

7.8.2. Configure anti-malware for automatic update.

7.8.3. Configure anti-malware with real-time detection for constantly updated threat signatures and patterns

7.8.4. Monitor all systems for unauthorized access, access attempts by authorized parties, malware incidents, and any other evidence of activity that may impair the security of Client Confidential Information and personal data.

7.9. Media Controls

7.9.1. Except as required for backup, or as agreed in writing by Client, prevent transfer of Client Confidential Information to any form of Removable Media. For purposes of this requirement, “Removable Media” means portable or removable hard disks, floppy disks, USB memory drives, zip disks, optical disks, CDs, DVDs, digital film, memory cards, magnetic tape, and all other removable data storage media.

7.9.2. Protect the confidentiality of backup of Emapta Information at secure on-premises or cloud-based locations.

7.9.3. Implement cryptographic mechanisms to protect the confidentiality of Confidential Information and personal data stored on digital media during transport, if authorized or removable media storage is agreed in writing by Client to be allowed, unless otherwise protected by alternative physical safeguards.

7.9.4. Perform secure wiping of data within storage drives upon asset recovery.

7.10. Personnel Security

7.10.1. Screen individuals prior to authorizing access to Information Systems containing Client Confidential Information and personal data. Emapta will perform employee background checks prior to any engagement of personnel to provide services to the Client.

7.10.2. Ensure that Information Systems are protected during and after personnel actions such as terminations and transfers.

7.11. Awareness and Training

7.11.1. Ensure that all personnel are made aware of their responsibilities regarding the protection of Client Confidential Information and personal data via completion of the mandatory Information Security Awareness and Privacy Training.

7.12. Physical Security

7.12.1. Secure access to all office entry & exit points and data centers for which Client Confidential Information might be stored or processed ("Work Premises") via physical security controls such as biometrics access restrictions, physical lock, CCTV monitoring, and presence of security personnel.

7.12.2. Control and manage physical access devices such as biometrics devices.

7.12.3. Escort and monitor visitors while present in any Work Premises.

7.12.4. Maintain a record of any visitors who enter the Work Premises.

7.12.5. For more information, refer to Physical Security Manual.

7.13. Incident Reporting

7.13.1. Emapta shall report to the Client immediately, in compliance with applicable contractual stipulation or breach notification protocol, any security incident that results in, or is suspected to have the effect of, exposure of Client Confidential Information and personal data to unauthorized persons, or the unauthorized deletion, modification, or denial of use to any Client Confidential Information.

7.13.2. In the event of a security incident, Emapta will take steps to immediately contain the incident, preserve logs and other evidence of the incident, to stop any further security compromise of its systems, and to take remedial steps to prevent recurrence of the incident.

7.13.3. Maintain records of all investigative, remedial, and corrective actions.

7.13.4. Promptly provide, upon Client request, documentation and supporting evidence related to the incident, its impact, and any investigative, corrective, or remedial actions taken or planned.

7.13.5. Maintain an internal Security Incident Response Playbook with periodic security response exercises.

7.14. Third Party Risk Management

7.14.1. Emapta will not engage any subcontractors, vendors, or other third parties to process services to its clients and perform processing on Client Confidential Information except if it's aligned within agreed Client Services Agreements (Master Agreements) and with explicit authorization by Clients.

7.14.2. Emapta will maintain a security process to conduct appropriate due diligence prior to utilizing any third party to provide or assist in the provision of any portion of the Service or process any Confidential Information.

7.14.3. Emapta shall ensure that all such third parties are fully compliant with the obligations under reviewed contractual obligations.

7.15. Data Privacy

7.15.1. Emapta shall maintain the function of a dedicated personnel to carry out the overall management of the Data Privacy Program. The Data Protection Officer (DPO) of Emapta shall acts as the single point of contact (SPOC) for all matters about data Privacy within Emapta including but not limited to compliance to prevailing Data Privacy regulations (e.g., General Data Protection Regulation GDPR), launch sustainable initiatives to comply with these regulations and design and implement Emapta's Data Privacy Program to uphold the data privacy rights of data subjects.

7.15.2. The DPO, in coordination with the different working groups in Emapta shall ensure that all data privacy incidents are responded to, mitigated, and analyzed to meet reporting requirements to regulators The DPO shall create, maintain, and implement training and awareness initiatives to ensure that all data subjects are made aware of their data privacy rights. This also provides an avenue to ensure that they are made aware of the contact details of the DPO for immediate action on their concerns.

7.15.3. Emapta's Data Privacy Program uphold the data privacy rights of data subjects.

7.15.4. Topic-specific Information Security and Privacy Standards & Requirements should be adhered to in compliance with this Information Security Policy. Such specific standards & requirements are found in Emapta's Information Security Management System Manual and Privacy Manual official documents.

7.15.5. For more information, refer to Data Privacy Policy.

8. DOCUMENT REFERENCES

8.1. Other documents referenced as part of Emapta's Information Security roles & responsibilities and should be complied with in accordance with this information security policy can be found within Emapta's platforms for its employees and partners. Complementary to this policy, these documents, require compliance as part of the Emapta Information Security Program:

8.2. Information Security Management System (ISMS) Manual - provides the organization's approach to information security management in accordance with ISO 27001. Provides comprehensive standards & requirements to the organization's information security policies, procedures, and controls. Includes topic-specific security/privacy standards & requirements covering the following domains:

- 8.2.1. Governance
- 8.2.2. Asset Management
- 8.2.3. Identity & Access Management
- 8.2.4. Security Events & Incident Management
- 8.2.5. Threat & Vulnerability Management
- 8.2.6. Information Protection
- 8.2.7. HR Security
- 8.2.8. Physical Security
- 8.2.9. System/Network Security and Secure Configurations
- 8.2.10. Application Security
- 8.2.11. IT Business Continuity
- 8.2.12. Supplier Relationships Security (Third Party Risk Mgmt.)
- 8.2.13. Legal & Compliance

8.3. Data Classification and Handling Policy - Rules for securely sharing information based on the sensitivity level of an information

8.4. Data Privacy Policy - Sets the tone of our commitment to protect the personal information of all our stakeholders

8.5. Data Privacy Manual - Sets approach to privacy management and the protection of personal data in accordance with ISO 27701.

8.6. Acceptable Usage Policy - Sets out the rules for appropriate & limited intended use of Emapta-provided technologies

8.7. Social Media Policy - Rules we must follow when engaging in social media to help avoid disclosure of sensitive data

8.8. Offsite Work Policy - Includes security practices that we have to follow when we're working from anywhere outside Emapta offices

8.9. Clean Desk Policy - Responsibilities for maintaining a clutter-free workspace in order to protect our assets and sensitive data

8.10. Employee Handbook – document from People & Culture that sets the responsibilities of employees

8.11. Code of Conduct – document from People & Culture that lays out ethical standards and the repercussions for violations of policies & ethical standards

8.12. Global Technology Policies – internal only within the Global Technology Division; policies and standards over Global Technologies' processes which includes the following:

8.12.1.Change Management
8.12.2.Incident Management
8.12.3.IT Asset Management
8.12.4.IT Business Continuity and Disaster Recovery
8.12.5.Global Technology Back-Up
8.12.6.Global Technology Knowledge Management
8.12.7. AI Governance

9. DOCUMENTATION AND COMPLIANCE

9.1. To maintain robust information security, all relevant policies, standards, and procedures must be thoroughly documented and securely stored. Records demonstrating compliance, such as training logs, audit results, and incident reports, must be maintained for a minimum of five years. Documentation must include version control to track updates and revisions. Compliance will be monitored through regular audits and reporting to senior management, with any non-compliance issues addressed promptly. Training programs will ensure that all employees and stakeholders are aware of and understand the policies, with refresher courses provided as needed.

10. POLICY REVIEW

10.1. This policy will undergo an annual review to ensure it remains effective and relevant in addressing current security threats and regulatory requirements. Additionally, the policy will be reviewed in response to significant changes, such as new regulations or major security incidents. A designated review committee will oversee the process, incorporating feedback from stakeholders and documenting any changes. The updated policy will be communicated to all relevant parties to ensure continued adherence.

11. EFFECTIVITY

11.1. 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.11.00PM**
EFFECTIVITY DATE:	**August 2024**

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

REVIEW AND REVISION HISTORY			
DATE:	**ACTION**	**Control No. (for Revision)**	**DESCRIPTION / COMMENT**
October 2018	*Created*	*1.0*	*A policy for Information Security is created. Reviewed and approved.* *-Patrick Sulit-*
October 2019	*Reviewed*	*1.1*	*Annual review of document was done, and no change was made. The document is still updated with current policy.* *-Patrick Sulit-*
November 2020	*Reviewed*	*1.2*	*Annual review of document was done, and no change was made. The document is still updated with current policy.* *-Patrick Sulit-*
August 2021 *November 2021*	*Template Update* *Reviewed*	*1.3*	*The document was transferred to the official Emapta template. No change was made as the information is still updated.* *-Kate Sangalang-* *Annual review of document was done, and no change was made. The document is still updated with current policy.* *-Patrick Sulit-*
July 2022	*Reviewed and updated*	*1.4*	*Revised objectives, definition of terms, roles & responsibilities, and added information security commitment, and alignment with ISO 27002:2022 security controls as an annex.* *-Justin Arrojado-*
June 2023	*Reviewed and updated*	*1.5*	*Revised Roles & Responsibilities to reflect changes on updated organizational structure, minor additions in employee responsibilities, added more documents in references, and updated the Information Security Safeguards. Moved the specific standards to the Information Security Management System Manual.* *-Justin Arrojado-*
August 2024	*Reviewed and updated* *Template Updated*	*1.6*	*Added Password Controls and Physical security manual document as a reference. The document was transferred to the official Emapta template.* *-Shihani Punchihewage-*