EMAPTA

Acceptable Usage Policy

PROTECTED

DOCUMENT CONTROL NO.: EVSI.ITD.13.00PM
EFFECTIVITY DATE: May 2024

TABLE OF CONTENTS

1. OVERVIEW

1.1. Emapta acknowledges its responsibility in providing a diverse range of information technology resources to qualified employees and partners, recognizing that access to these resources constitutes a privilege accompanied by specific responsibilities and obligations. Users of Emapta's computers, computing systems, information, and networks, collectively referred to as information technology resources, must adhere to Emapta policies, applicable regulations, data protection standards and international laws such as GDPR, PCI, HIPAA, and ISOs. Compliance with specific policies and guidelines governing the use of these resources is mandatory, requiring responsible conduct while utilizing shared computing and network resources. This policy undergoes regular review and updates, ensuring alignment with evolving technology, industry standards, and legal or regulatory requirements.

2. OBJECTIVE

2.1. The purpose of this policy is to establish guidelines for the acceptable use of information technology resources at Emapta, with a primary objective of promoting efficient, ethical, and lawful utilization of these resources. In addition to outlining the responsibilities and obligations of users upon access, this policy aims to safeguard the interests of Emapta and its talents.

3. SCOPE

3.1. This policy applies to all individuals accessing or using information technology resources owned or managed by Emapta, including but not limited to core employees, client talent, contractors, temporary employees, volunteers, and external individuals authorized by Emapta. Information technology resources encompass all hardware, software, networks, systems, and data owned or managed by Emapta, irrespective of the ownership of the connected computer or device.

4. DEFINITION OF TERMS

4.1. **Authorized Users -** Individuals granted permission and authorized access to Emapta's information technology resources, including employees, contractors, and other authorized personnel.

4.2. **Email Usage -** Sending, receiving, and management of electronic messages (emails) through Emapta’s email systems. Email usage should adhere to the organization’s Information Security and Acceptable Usage policies.

4.3. **Data Breach -** Unauthorized access, disclosure, or acquisition of sensitive or confidential information, leading to compromise or misuse.

4.4. **Encryption -** Process of converting data into a code to prevent unauthorized access or interception during transmission or storage.

4.5. **Fair Use Share -** Each user should have access to a proportional and appropriate amount of resources without one user monopolizing or excessively consuming the resources to the detriment of others.

4.6. **Information Technology Resources -** Refers to all hardware, software, networks, systems, and data owned or managed by Emapta, including computers, servers, laptops, mobile devices, internet connections, and associated infrastructure.

4.7. **Intellectual Property -** Refers to creations of the mind, including inventions, designs, trademarks, copyrights, trade secrets, and other original works.

4.8. **Internet Usage -** Utilization of the internet for browsing websites, accessing online services, and conducting online activities in compliance with Emapta's Information Security and Acceptable Usage policy.

4.9. **Personal Use -** Limited and occasional use of information technology resources for personal purposes that do not interfere with work responsibilities or productivity. Personal use should comply with Emapta's Information Security and Acceptable Usage policies and not violate any laws or ethical guidelines.

4.10. **System & Network Monitoring -** Surveillance and analysis of system and network activities of the organization to identify potential security threats, monitor compliance with Emapta's policies, troubleshoot issues, and ensure the overall health and performance of the organization's IT environment.

4.11. **User Account -** Unique identifiers that allow you to have access to Emapta's information technology resources. User accounts are associated with individuals, and users are responsible for maintaining the confidentiality and security of their accounts and passwords.

4.12. **Incident Response -** Coordinated approach to managing and mitigating the impact of security incidents, including detection, containment, eradication, recovery, and lessons learned.

4.13. **Work-Related Activities -** Activities that are directly related to the individual's job responsibilities or tasks assigned by Emapta or its Clients. These activities support the organization's business objectives and are performed during working hours.

4.14. You may also refer to the Information Security Policy for the other definition of terms applicable to Acceptable Usage Policy.

5. ROLES AND RESPONSIBILITIES

5.1. As an employee or authorized user of Emapta's information technology resources, access is provisioned to facilitate work-related tasks and activities, while ensuring a reasonable expectation of unobstructed use, privacy, and protection from misuse. While Emapta extends access to work-related tools and activities, employees and authorized users bear the responsibility of familiarizing themselves with Emapta's regulations and policies governing appropriate use of the computing environment and resources. It is incumbent upon them to exercise good judgment and adhere to established protocols.

6. IMPLEMENTING GUIDELINES

6.1. Acceptable Use

6.1.1. Employees and authorized users must utilize only those computers, user accounts, and IT resources for which they possess authorization, ensuring the protection of user accounts and passwords from unauthorized access or sharing.

6.1.2. Employees and authorized users may not use another individual's account or attempt to capture or guess other users' passwords.

6.1.3. Employees and authorized users are individually responsible for appropriate use of all IT resources assigned to them, including the computer, the network address or port, software, and hardware. Therefore, authorized users are accountable to Emapta for all use of such resources. As authorized users of IT resources, it is forbidden to enable unauthorized users to access the network by using an Emapta computer or a personal computer that is connected to the Emapta network.

6.1.4. Emapta is bound by its contractual and license agreements respecting certain third-party resources. Employees and authorized users are expected to comply with all such agreements when using such resources.

6.1.5. Employees and authorized employees should make reasonable efforts to protect their passwords, following the password guidelines and to secure resources against unauthorized use or

access. Users are discouraged to write down or store in an unsecured manner their passwords. Users must follow secure hardware and software configurations in accordance with Emapta's Information Security Policy to reasonably prevent unauthorized users from accessing Emapta's network and computing resources.

6.1.6. Employees and authorized users must not attempt to access restricted portions of the network, an operating system, security software or other administrative applications without appropriate authorization by the system owner or administrator.

6.1.7. Employees and authorized users must comply with the policies and guidelines for any specific set of resources to which users have been granted access, such as Emapta's policy for information security. When other policies are more restrictive than this policy, the more restrictive policy takes precedence.

6.1.8. Employees and authorized users must not use Emapta IT resources in conjunction with the execution of programs, software, processes, or automated transaction-based commands that are intended to disrupt (or that could reasonably be expected to disrupt) other computer or network users, or damage or degrade performance, software, or hardware components of a system.

6.1.9. On Emapta network and/or computing systems, employees and users are forbidden to use tools that are normally used to assess security or to attack computer systems or networks (e.g., password 'crackers,' vulnerability scanners, network sniffers, etc.) unless Employee have been specifically authorized to do so by the Information Security Department

6.1.10. Employees and Users should not install unauthorized software or hardware on company systems without proper authorization by the system owner or administrator.

6.1.11. Employees and Authorized Users should promptly report any suspected security breaches, policy violations, or suspicious activities to the appropriate IT or information security or data privacy personnel.

6.1.12. Employees and Authorized Users should not attempt to access, modify, or tamper with Emapta systems & information without appropriate authorization by the system owner or administrator.

6.1.13. Employees and users are not allowed to connect their personal or unauthorized devices to Emapta's corporate network and systems unless authorization has been provided to them. It is also prohibited to store and process Emapta or Client information on personal or unauthorized platforms without authorization by the system/information owner.

6.2. Fair Use Share

6.2.1. All departments maintaining computing resources must ensure an acceptable level of performance, preventing excessive or inappropriate use by any individual to the detriment of others. Emapta IT resources, network, computer clusters, mail servers and other central computing resources are shared widely and are limited, hence requiring that resources be utilized with consideration for others who also use them. Therefore, the use of any automated processes to gain technical advantage over others within Emapta's IT resources is explicitly forbidden.

6.2.2. Emapta may choose to set limits on an individual's use of a resource through quotas, time limits, and other mechanisms to ensure that these resources can be used by anyone who needs them.

6.3. Observance with State and Local Laws

6.3.1. Employees and authorized users are required to comply with local ordinances and state laws, as well as Emapta's guidelines concerning the use of technology, which are informed by these legal considerations. This includes adherence to laws governing licensing, copyright, and intellectual property protection. Users must refrain from engaging in any illegal or unethical activities, such as unauthorized access, distribution of malware, or harassment. Compliance with local ordinances and state laws is essential, encompassing regulations related to licenses, copyrights, and intellectual property protection.

6.3.2. Emapta and authorized users of IT resources must abide by these rules:

6.3.2.1. Abide by all state and local laws.

6.3.2.2. Abide by all applicable copyright laws and licenses. Emapta has entered into legal agreements or contracts for many of our software and network resources which require everyone using them to comply with those agreements.

6.3.2.3. Observe the copyright law as it applies to music, videos, games, images, texts, and other media in both personal use and in production of electronic information. The ease with which electronic materials can be copied, modified, and sent over the Internet makes electronic materials extremely vulnerable to unauthorized access, invasion of privacy and copyright infringement.

6.3.2.4. Do not use, copy, or distribute copyrighted works (including but not limited to Web page graphics, sound files, film clips, trademarks, software, and logos) and intellectual property rights of third parties unless employee have a legal right to use, copy, distribute, or otherwise exploit the copyrighted work. Doing so may provide the basis for disciplinary action, civil litigation, and criminal prosecution. If any potential infringement or misuse of third-party intellectual property is identified, employees and users should promptly report it to the appropriate department (e.g., Legal Department).

6.4. Protection of Intellectual Property

6.4.1. Any intellectual property created by employees within the scope of their employment, or by contractors under contract with the organization, using Emapta's IT resources, shall be the property of Emapta, unless otherwise specified in a separate agreement.

6.4.2. Emapta will take reasonable security measures, in accordance with the Information Security Policy, to protect its intellectual property assets, including implementing security controls, confidentiality agreements, and appropriate registration or filing of intellectual property rights when necessary.

6.4.3. Employees and authorized users should exercise due care and diligence to safeguard intellectual property and prevent unauthorized use, disclosure, or infringement.

6.4.4. Intellectual property owned by Emapta shall be used solely for legitimate business purposes and in accordance with relevant licenses, agreements, or policies.

6.4.5. Employees and authorized users of Emapta's IT resources shall not use or disclose Emapta's intellectual property for personal gain or benefit, or for the benefit of other organizations without proper authorization.

6.4.6. Emapta retains ownership of intellectual property created using its resources, implementing security measures to protect its assets and requiring due diligence from employees and authorized users to prevent unauthorized use, disclosure, or infringement.

6.5. Privacy and Personal Rights

6.5.1. Respect for the privacy and personal rights of others is mandatory, prohibiting unauthorized access or copying of sensitive personally identifiable information (SPII) and ensuring professional conduct in all communications:

6.5.1.1. Do not access or copy any employee's sensitive personally identifiable information (SPII), where authorization is not provided without the appropriate departments (e.g., Data Protection Officer), except if required as part of day-to-day sanctioned job responsibilities.

6.5.1.2. Be professional and respectful when using computing systems to communicate with others; the use of IT resources to libel, slander, or harass any other person is not allowed and will lead to disciplinary actions as well as legal action by those who are the recipient of these actions.

6.5.1.3. Emapta reserves the right to access and review personal information under certain conditions. These include investigating performance deviations and security/privacy incidents (with reasonable cause), determining if an individual is in violation of this policy, or, as may be necessary, to ensure that Emapta is not subject to claims of institutional misconduct.

6.6. Emapta will hold and collect necessary personal data of its Employees by virtue of their employment with Emapta. This is for the purposes of employment & human resources administration, workplace management, secure employee data management, and promote efficiencies in technology services, all in compliance with applicable laws and regulations. All personal data collected by virtue of employment will be treated with the utmost confidentiality in line with Emapta's Information Security and Data Privacy policies.

6.7. Email Use and Privacy

6.7.1. Emapta reserves the right, with approval from authorized Emapta personnel (e.g., Data Protection Officer) to access, monitor, and inspect all information within Emapta-owned mail and communication repositories, as well as its IT resources. This access, monitoring, and inspection are subject to authorization from relevant personnel.

6.7.2. Email use must be limited to business purposes only.

7. DOCUMENTATION AND COMPLIANCE

7.1. All employees and authorized users of Emapta's information technology resources are required to document their activities and compliance with this Acceptable Usage Policy. This includes maintaining accurate records of access, usage, and any incidents or breaches. These records must be kept in accordance with Emapta's data retention policies and be readily available for review by authorized personnel. Compliance with this policy is mandatory, and periodic audits will be conducted to ensure adherence. Non-compliance may result in disciplinary action, including termination of access or employment, and could lead to legal consequences.

8. POLICY REVIEW

8.1. This policy will be reviewed annually or as needed to ensure its continued relevance and alignment with evolving technology, industry standards, and legal or regulatory requirements. The Information Security and Compliance team, along with other relevant stakeholders, will conduct the review process. Any changes or updates to the policy will be communicated to all employees and authorized users in a timely manner. Feedback from users will be considered in the review process to improve the policy's effectiveness and practicality.

9. EFFECTIVITY

9.1. This Acceptable Usage Policy is effective immediately upon approval by Emapta's management and remains in effect until further notice. All employees and authorized users are required to comply with the policy from the date of its effectivity. Emapta reserves the right to amend or rescind this policy at any time, with appropriate notice provided to all users. The policy's provisions apply to all current and future users of Emapta's information technology resources, ensuring a secure and compliant computing environment.

POLICY/PROCESS OWNER:	**Information Security Manager**
DOCUMENT CONTROL NO.:	**EVSI.ITD.13.00PM**
EFFECTIVITY DATE:	**May 2024**

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

REVIEW AND REVISION HISTORY

DATE:	ACTION	Control No. (for Revision)	DESCRIPTION / COMMENT
May 2023	*Created*	*1.0*	*Document creation of Emapta Acceptable Usage Policy. Updated the document based on inputs during policy review and approval with CISO and CIO.* *-Justin Arrojado-*
	Template Updated		*Reviewed and updated document based on changes made by the author. Document was transferred to official Emapta template.* *-Rence Valdenarro-*
May 2024	*Reviewed and updated* *Template Updated*	*1.1*	*Reviewed and updated the policy to include adherence to international data protection laws, data security and privacy protection, third-party vendors, expand protocols for security incident reporting, and outline disciplinary actions and escalation procedures for non-compliance.* *-Shihani Punchihewage-*