EMAPTA

Internet and Email Usage Policy

PROTECTED

DOCUMENT CONTROL NO.: EVSI.ITD.24.00PM
EFFECTIVITY DATE: May 2024

TABLE OF CONTENTS

1. OVERVIEW 3

2. OBJECTIVE 3

3. SCOPE 3

4. DEFINITION OF TERMS 3

5. ROLES AND RESPONSIBILITIES..4

6. IMPLEMENTING GUIDELINES..4

7. PERMITTED USES 5

8. LIMITED PERSONAL USE..5

9. PERMITTED EXTENDED PERSONAL USE 6

10. UNACCEPTABLE USE..6

11. COMPLIANCE..6

12. REPORTING VIOLATIONS 7

13. DOCUMENTATION AND COMPLIANCE..7

14. POLICY REVIEW..7

15. EFFECTIVITY 8

1. OVERVIEW

1.1. Emapta recognizes the pivotal role that email systems and internet access play in facilitating the efficient and professional delivery of services by our employees. We affirm our support for employees' rights to engage in reasonable personal use of internet and email communications within the workplace environment.

2. OBJECTIVE

2.1. This policy serves to establish clear and comprehensive guidelines for the acceptable use of the computer network, internet, and email by all employees of Emapta. The primary objective of providing internet and email access to our employees is to empower them in the effective discharge of their job responsibilities while maintaining a conducive work environment.

3. SCOPE

3.1. This policy applies to the appropriate utilization of any internet and email communication transmitted through Emapta's network and email addresses. It extends to encompass all employees, vendors, and individuals operating on behalf of Emapta, thereby ensuring uniformity and consistency in our approach to internet and email usage.

4. DEFINITION OF TERMS

4.1. **Access Credentials:** Usernames, passwords, and other forms of authentication that allow employees to access Emapta's email systems and internet resources.

4.2. **Limited Personal Use:** Occasional and brief use of internet and email resources for personal activities that do not interfere with work responsibilities or Emapta's operations.

4.3. **Permitted Extended Personal Use:** Personal use of internet and email resources that extends beyond occasional and brief use, requiring prior notification and negotiation with the respective manager.

4.4. **Unauthorized Activities:** Actions that violate this policy, including but not limited to generating offensive content, accessing objectionable material, sharing confidential information without authorization, and engaging in illegal activities.

4.5. **Monitoring and Enforcement:** The process by which the Information and Cybersecurity department reviews internet and email usage to ensure compliance with this policy.

4.6. **Compliance Measurement:** Methods used to assess adherence to this policy, including walk-throughs, video monitoring, business tool reports, audits, and feedback mechanisms.

4.7. **Non-Compliance:** Failure to adhere to this policy, which may result in disciplinary action, including termination of employment.

5. ROLES AND RESPONSIBILITIES

5.1. **Employees**:

5.1.1. Ensure that internet and email usage comply with this policy.

5.1.2. Participate in training sessions and stay informed about updates to the policy.

5.1.3. Report any suspected policy violations to their immediate supervisor, HR department, or the Information Security department.

5.1.4. Use internet and email resources responsibly, maintaining productivity and security.

5.2. **Managers**:

5.2.1. Communicate the policy to their teams and ensure understanding and compliance.

5.2.2. Monitor their teams' internet and email usage to ensure adherence to this policy.

5.2.3. Address and report any suspected violations of the policy within their teams.

5.3. **Information Security Manager**:

5.3.1. Oversee the implementation and enforcement of this policy.

5.3.2. Approve any exceptions or deviations from the policy.

5.3.3. Coordinate with other departments to ensure policy compliance and address violations.

5.4. **Information Security Department**:

5.4.1. Monitor internet and email usage across the organization.

5.4.2. Investigate any violations or suspicious activities.

5.4.3. Provide technical support and assistance to employees regarding policy compliance.

5.4.4. Conduct periodic reviews and updates of the policy to ensure its effectiveness.

5.5. **Human Resources Department**:

5.5.1. Maintain records of employee training sessions, policy acknowledgments, and disciplinary actions.

5.5.2. Ensure that all employees receive the necessary training and understand the policy.

5.5.3. Support the Information Security department in investigating and addressing policy violations.

5.6. **IT Department**:

5.6.1. Provide employees with access credentials and necessary resources.

5.6.2. Support the implementation of the least privilege access principle.

5.6.3. Assist employees with technical issues related to internet and email usage.

6. IMPLEMENTING GUIDELINES

6.1. **Provision of Access:** Emapta's IT department will be responsible for providing employees with access to the company's email systems and internet resources.

Access credentials will be issued to employees upon completion of the necessary onboarding procedures. Access will be granted according to the least privilege access principle, aligning with employees' roles and responsibilities within the organization.

6.2. **Monitoring and Enforcement:** The Information and Cybersecurity department will monitor internet and email usage to ensure compliance with this policy. Monitoring activities may include the review of network traffic, email content, and website access logs. Any violations or suspicious activities will be promptly investigated, and appropriate action will be taken in accordance with this policy.

6.3. **Employee Training:** All employees will receive comprehensive training on the provisions of this policy during their onboarding process. Additionally, regular refresher training sessions will be conducted to reinforce understanding and compliance with the policy guidelines.

6.4. **Communication of Policy Changes:** Any updates or amendments to this policy will be communicated to all employees via email or through the company's internal communication channels. Employees will be required to acknowledge receipt and understanding of the updated policy provisions.

6.5. **Assistance and Support:** Employees who require clarification or assistance regarding any aspect of this policy are encouraged to contact the IT Helpdesk or their immediate supervisor for guidance. The IT department will provide technical support and assistance as needed to ensure employees can adhere to the policy requirements effectively.

6.6. **Documentation and Record-keeping:** Records of employee training sessions, policy acknowledgments, and any disciplinary actions taken in response to policy violations will be maintained by the HR department in accordance with company policies and regulatory requirements. These records will be made available for audit purposes as necessary.

7. PERMITTED USES

7.1. Employees are granted permission to utilize Emapta-provided internet and email access for the following purposes:

7.1.1. Conducting work-related activities and tasks.
7.1.2. Engaging in limited personal use, as outlined below.
7.1.3. Participating in extended personal use under specific circumstances.

8. LIMITED PERSONAL USE

8.1. Limited personal use of internet and email resources is permissible under the following conditions:

8.1.1. Occasional and brief usage.
8.1.2. Non-interference with the duties of the employee or their colleagues.
8.1.3. Non-disruption of Emapta's operational activities.
8.1.4. Preservation of the security integrity of Emapta's systems.

8.1.5. Absence of adverse impact on Emapta's electronic storage capacity or network performance.
8.1.6. Compliance with prescribed Email Maintenance and Archiving Procedures and adherence to the current IT Security Standard and Requirements.
8.1.7. Absence of any additional financial burden on Emapta.
8.1.8. Conformance to all applicable laws and regulations, as well as to Emapta's confidentiality requirements.

8.2. Examples of reasonable personal use encompass activities such as:
8.2.1. Initiating brief online banking transactions.
8.2.2. Settling personal bills.
8.2.3. Sending concise personal emails or making brief personal phone calls.

9. PERMITTED EXTENDED PERSONAL USE

9.1. In exceptional circumstances necessitating extended personal use, employees must adhere to the following expectations:
9.1.1. Prior notification and negotiation with the respective manager regarding the intended use.
9.1.2. Compensation for the time spent on personal internet usage by either replacing break time or adjusting timesheets accordingly.
9.1.3. Dispensation from the requirement to notify or negotiate with the manager for personal use deemed to be of a limited nature.

10. UNACCEPTABLE USE

10.1. Employees are prohibited from utilizing Emapta-provided internet or email access for the following purposes:
10.1.1. Generating or exchanging offensive, harassing, obscene, or threatening content.
10.1.2. Accessing websites containing objectionable or criminal material.
10.1.3. Sharing confidential or sensitive information belonging to Emapta, except when authorized as part of their job duties.
10.1.4. Violating copyright laws through the unauthorized downloading or uploading of commercial software, games, music, or movies.
10.1.5. Engaging in internet-enabled activities such as gambling, gaming, conducting personal business, or participating in illegal activities.
10.1.6. Distributing unsolicited or bulk email, including advertisements, solicitations, chain letters, or spam.
10.1.7. Engaging in non-work-related activities on company computers during designated work hours.

11. COMPLIANCE

11.1. **Compliance Measurement:** The Information and Cybersecurity department will monitor compliance with this policy through various methods, including periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback mechanisms.

11.2. **Exceptions:** Any deviation from this policy requires prior approval from the Information Security Manager.

11.3. **Non-Compliance:** Employees found to have violated this policy may face disciplinary action, up to and including termination of employment.

12. REPORTING VIOLATIONS

12.1. Employees are encouraged to promptly report any suspected violations of this policy to their immediate supervisor, HR department, or the Information Security department for appropriate action.

13. DOCUMENTATION AND COMPLIANCE

13.1. The policy will be communicated to all stakeholders through email notifications, internal communication channels, and regular team meetings to ensure broad understanding and engagement. Comprehensive training programs and educational resources will be provided to all stakeholders during the onboarding process and through periodic refresher courses to ensure a clear understanding of their responsibilities under the policy. Specific compliance certifications or qualifications may be required for certain roles affected by the policy to ensure adherence. To address non-compliance, the Information and Cybersecurity department will implement enforcement measures that include monitoring internet and email usage, investigating violations, and taking appropriate disciplinary actions. Penalties or sanctions for non-compliance will be enforced consistently and fairly across all stakeholders, ensuring that enforcement actions uphold the integrity of Emapta's operations and regulatory requirements.

14. POLICY REVIEW

14.1. The Internet and Email Usage Policy will undergo a comprehensive annual review to ensure its ongoing effectiveness and relevance to Emapta's operations. Monitoring and evaluation of the policy's impact and effectiveness will be conducted through various methods, including the analysis of compliance metrics, such as the number of policy violations, the frequency and outcomes of employee training sessions, and feedback from internal audits. Key indicators of success will include a reduction in unauthorized activities, increased adherence to usage guidelines, and overall employee compliance. Feedback and input from stakeholders, gathered through surveys, focus groups, and direct communications, will be incorporated into the policy to address emerging issues and improve its applicability. Evaluations will be conducted annually, with additional reviews triggered by significant incidents or regulatory changes, and the findings will inform necessary updates or amendments to maintain alignment with industry standards and regulatory requirements.

15. EFFECTIVITY

15.1. 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.24.00PM**
EFFECTIVITY DATE:	**May 2024**

	NAME / DESIGNATION	DATE
AUTHOR	**Jappy Damaso – Information Security Manager**	**April 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 20219	*Created*	*1.0*	*A policy for Internet and Email Usage is created. Reviewed and approved.* *-Justin Arrojado-*
May 2023	*Reviewed*	*1.1*	*Reviewed* *-Justin Arrojado-*
May 2024	*Reviewed and updated* *Template updated*	*1.2*	*Reviewed and added Definition of terms, Roles and responsibilities, Implementing guidelines, Compliance and Report violations.* *-Shihani Punchihewage-*