Electronic Communication & Internet Use Policy

Validated for use by

chrmp®
CERTIFIED HUMAN RESOURCE MANAGEMENT PROFESSIONAL

Table of Contents

POLICY STATEMENT:

Our organization aims to promote the secure and ethical use of electronic communication and internet resources by employees of the organization. By adhering to the guidelines outlined in this policy, employees can ensure the appropriate use of these resources for legitimate business purposes and avoid any legal liabilities, security risks, or negative consequences.

PURPOSE:

The purpose of this policy is to define the acceptable use of electronic communication and internet resources by employees of the organization.

This policy sets forth guidelines for the appropriate use of electronic communication and internet resources, including email, social media, instant messaging, and other online services.

SCOPE:

This policy applies to all employees of the organization who have access to electronic communication and internet resources in the course of their work.

It also applies to all electronic communication and internet resources owned or provided by the organization, regardless of the device used to access them.

DEFINITIONS:

- Electronic Communication: Any form of communication that is transmitted electronically, including but not limited to email, instant messaging, and social media.

- Internet Resources: Any online services, websites, or applications that are accessed through the internet, including but not limited to web browsing, search engines, and cloud-based storage services.

- Legitimate Business Purposes: Any activities related to the employee's job duties or responsibilities that are necessary for the successful operation of the organization.

- Confidential or Proprietary Information: Any information that is not publicly available and is considered confidential or proprietary to the organization, including but not limited to trade secrets, customer lists, and financial information.

- Copyrighted Material: Any works that are protected by copyright law, including but not limited to software, music, videos, and images.

- Malware or Viruses: Any software or code that is designed to harm, disrupt, or damage electronic communication and internet resources, including but not limited to viruses, worms, and Trojan horses.

ACCEPTABLE USE:

The following guidelines must be followed when using electronic communication and internet resources:

- Employees must use electronic communication and internet resources for legitimate business purposes only. Personal use of these resources is permitted only during non-working hours and should not interfere with work responsibilities.

- Employees must not use electronic communication and internet resources for illegal or unethical activities, including but not limited to harassment, discrimination, defamation, and copyright infringement.

- Employees must not use electronic communication and internet resources to share confidential or proprietary information, except as required by their job duties.

- Employees must not use electronic communication and internet resources to download or share unauthorized software, music, videos, or other copyrighted material.

- Employees must not use electronic communication and internet resources to participate in activities that waste time or distract from work responsibilities, such as playing online games or browsing social media.

- Employees must not use electronic communication and internet resources to engage in activities that could harm the organization's reputation, including making derogatory or defamatory comments about the organization, its employees, or its customers.

SECURITY AND PRIVACY:

The following guidelines must be followed to ensure the security and privacy of electronic communication and internet resources:

- Employees must use strong and secure passwords for all electronic communication and internet resources and must not share their passwords with others.
- Employees must not access electronic communication and internet resources using another employee's account without permission.
- Employees must not forward emails or other electronic communication from the organization to external parties unless they have been authorized to do so.
- Employees must not click on suspicious links or download attachments from unknown sources, as these may contain malware or viruses that could compromise the security of electronic communication and internet resources.
- Employees must not access or modify electronic communication and internet resources in ways that exceed their authorized privileges or violate the organization's security policies.
- Employees must report any suspected security breaches or privacy violations to their supervisor or IT department immediately.

ENFORCEMENT:

- Violations of this policy may result in disciplinary action, up to and including termination of employment.
- The organization reserves the right to monitor and audit electronic communication and internet resources to ensure compliance with this policy and applicable laws and regulations.

- Employees who have questions or concerns about this policy should contact their supervisor or the HR department for clarification.

Approved by:

Date of approval:

Revisions
Revision No. - Revision date - Approved by
Revision No. - Revision date - Approved by