| [Insert Company Name Or Logo] | |
|---|---|
| **Title: Internet and Email Use** | **P&P #:** |
| **Approval Date:** | **Review:** |
| **Effective Date:** | **Security Team** |

**Purpose:** To ensure that the use of email and internet activities do not negatively impact the confidentiality, availability, or integrity of [Insert Local Gov/K-12 Name]'s data and their assets and to ensure compliance with applicable federal and state laws. An authorized user's access to the Internet and/or email services for limited personal use is a privilege that, if not properly monitored and controlled, could result in harm to the organization or violations of federal or state laws. The primary use of these services is for operational purposes and need be appropriately protected.

**Scope:** This policy applies to all employees and other members of the workforce (whether paid, volunteer, or contractor) working in all facilities under the organization's ownership.

**Definitions:**

1. Sensitive Information or Data: Any information that should only be accessed by authorized personnel. It includes Protected Health Information, financial information, personnel data, trade secrets, and any information that is deemed sensitive, regulated, or confidential, or that would negatively affect [Insert Local Gov/K-12 Name] if inappropriately handled.
2. Protected Health Information (PHI): Health information, including demographic information collected from an individual and created or received by a health provider, health plan, employer or health care clearinghouse that relates to the past, present, or future physical or mental health or condition of any individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual that identifies an individual or there is a reasonable basis to believe the information can be used to identify the individual and that is transmitted or maintained by electronic media or any other form or medium. PHI does not include individually identifiable health information in education records covered and protected by the Family Educational Right and Privacy Act and employment records held by [Insert Local Gov/K-12 Name] in its role as an employer.
3. Email: The electronic transmission of information through a mail protocol such as SMTP, POP, or IMAP.
4. User: any employee or other person authorized by [Insert Local Gov/K-12 Name] to read, enter or update information created or transmitted via the electronic mail system.



This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

**Procedure:**

1. Internet Usage
    a. Users are responsible for reporting any suspected or confirmed violations of this policy to their department manager or the Security Officer.
    b. Users shall have no expectation of privacy in email and internet use. [Insert Local Gov/K-12 Name] may monitor messages and internet use without prior notice.
    c. Users shall not misuse their Internet privileges, i.e., spending excessive time on the Internet for non-work-related business or accessing inappropriate sites.
    d. Users shall not share sensitive information or PHI on public web sites (i.e., Google Apps, DropBox.com, Google Docs, iCloud, etc.).
    e. [Insert Local Gov/K-12 Name] reserves the right to block access to non-work-related material.
    f. Users shall honor all rules of copyright and personal property
    g. Users shall not knowingly download non-work-related executable files from the Internet.
    h. Users shall not establish peer-to-peer connections to external parties for file sharing, downloading music and movies, and accessing adult materials.
    i. Users shall not knowingly enable an external/remote party to gain unauthorized access or control of any device, application, or system to the data networks.
    j. The use of any software or service that hides the identity of the user or the location of the user while using the Internet is prohibited.

2. Email Usage
    a. All email messages, documents, and correspondence and data obtained via internet use are considered [Insert Local Gov/K-12 Name] property.
    b. Organization email is solely for work purposes. Do not use work email for personal reasons.
    c. Users shall not misuse their email privileges, i.e., sending and forwarding non-business-related mass emails.
    d. Users shall delete chain and junk email messages without forwarding or replying to them. Electronic chain letters and other forms of non-business-related mass mailings are prohibited.
    e. Personnel shall not use [Insert Local Gov/K-12 Name] resources to view, record, or transmit materials which violate [Insert Local Gov/K-12 Name] policies. Inappropriate messages, pictures, and/or other visual images/materials include, but are not limited to:
        i. Fraudulent messages - Messages sent under an anonymous or assumed name with the intent to obscure the origin of the message.



This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

ii. Harassment messages - Messages that harass an individual or group for any reason, including race, sex, religious beliefs, national origin, physical attributes, or sexual preference.
iii. Obscene messages - Messages that contain obscene or inflammatory remarks.
iv. Pornographic materials -This includes, but is not limited to pictures, audio/video files, literature, or newsgroups.

f. Users shall not engage in spamming activities. Electronic chain letters and other forms of non-business-related mass mailings are prohibited.
g. Users shall not forward email containing sensitive or regulated data to public email systems such as Hotmail.com, gmail.com, or other public email system services. In addition, users shall not forward sensitive or regulated data or other business information to their personal email accounts. Personal email accounts shall not be used for official [Insert Local Gov/K-12 Name] business.
h. The email message will include the following confidentiality notice:
    i. "This electronic message is intended to be for the use only of the named recipient, and may contain information that is confidential or privileged. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution or use of the contents of this message is strictly prohibited. If you have received this message in error or are not the named recipient, please notify us immediately by contacting the sender at the electronic mail address noted above, and delete and destroy all copies of this message. Thank you."
    ii. Note: This confidentiality notice can be added to the signature block of your email signature if you currently use an automated signature. [Can also make this part of the email system, that it is added to every email.]
i. Email transmission of PHI when necessary shall be conducted with the highest level of security applied and only in situations where the email is necessary for immediate business. PHI and other sensitive information shall be encrypted during transmission over the Internet (outside [Insert Local Gov/K-12 Name] networks). [Can also require PHI/FERPA/PII or sensitive information to not be sent by email if other options available.]
    i. When sending PHI/FERPA/PII or sensitive information via email certain precautions may need to be taken when using e-mail to avoid unintentional disclosures, such as checking the e-mail address for accuracy before sending.
    ii. PHI should not be transmitted in the subject line of the email message.
j. Users shall check their email regularly and delete unneeded email.
k. Users shall delete, without opening, suspicious, unsolicited email messages from outside [Insert Local Gov/K-12 Name] especially if they contain attachments with



This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

"exe" files. If a user is receiving repeat emails of this nature, the activity should be reported to the Security Officer.

l. Only individuals with administrative responsibilities (i.e., Department Managers, Directors, etc.) or their designee may be granted access to the email account of a former employee or vendor. This may require written approval from requestor's supervisor.
    i. The account shall be used only for the retrieval of existing email and shall not be used to impersonate the former personnel or send email communications.
    ii. Access shall be granted for 30 days and any extension must be approved by the designated Security Officer.

**Violations:**

Any user found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or assignment, depending on the severity of the infraction. In addition, the company may report the matter to civil and criminal authorities as may be required by law.

**Attachments: None**

**Related Policies: None**



This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.