UF Email Guidelines for Users of Restricted Data

UF | UNIVERSITY of FLORIDA

Who Should Know This

This standard applies to all users with access to UF Restricted Data who also use electronic mail services (email).

Definitions

Email A system for sending and receiving messages electronically over a computer network in which (a) usually text is transmitted, (b) operations include sending, storing, processing, and receiving messages, (c) users are allowed to communicate under specified conditions, and (d) messages are held in storage on a server until requested by the addressee using a computer application called an email client (e.g. Outlook, Thunderbird).

Purpose

Email is popular method to expediently exchange information. It's easy to install and use. However, extreme caution should be exercised by email users with access to Restricted Data. There is a high risk of Restricted Data exposure by unauthorized email message interception, monitoring or storing. These guidelines outline safe email practices for protecting the confidentiality of Restricted Data.

Guidelines

Due to the widespread use of email, a heightened awareness of its security risks must be maintained. Restricted Data is at high risk for disclosure via email in many ways. Listed below are safeguards to protect Restricted Data when using email.

1. Avoid sending Restricted Data via email. Where no reasonable alternative exists:
    a. First obtain permission from the Data Principal (Dean, Director, or Department Chair).
    b. Minimize the amount of Restricted Data sent.
    c. Minimize the number of recipients (e.g. do not send to lists).
    d. Restrict recipients to email addresses ending with ufl.edu.
    e. Check the recipient addresses to ensure accuracy before sending.
    f. Consult your Unit Information Security Manager [4] for secure methods and approved encryption.
    g. In the body of the message, clearly identify the information in the email as Restricted Data.
    h. In the body of the message, provide handling restrictions to the recipient (e.g. 'Do not forward or duplicate this message. Printed copies of this message must be rendered unreadable prior to disposal.').
2. Use only the email technologies approved by your Unit Information Security Manager [4] for UF work-related email or for email of any kind accessed from a UF computer. A commodity email service to which you personally subscribe may not be appropriate for your computing environment at work.
3. If loss or unauthorized exposure of Restricted Data is discovered, Restricted Data Users must immediately report the incident to the Data Principal and the UF Privacy Office [3], usually through the User's supervisor.
4. The following safe email practices should be followed:
    a. Do not follow links sent in email. If you think the link is legitimate, before clicking the link, contact the sender to confirm, by phone or separate email.
    b. Delete email with attachments. If you think the attachment is legitimate, before opening it, contact the sender to confirm, by phone or separate email.
    c. Use strong passwords that are difficult to guess, but easy to remember. Protect your password like you would protect your credit card.
    d. Do not use computer features that remember or auto-complete your password.

e. Ensure any computer used for email has current updates. Select the automatic update option if available.
f. Ensure any computer used for email has current anti-virus protection. Configure automatic updates if available.
g. Consider using a spam filtering service such the one offered by UF [6].

Bibliography

[1] Acceptable Use of UF Computing Resources, http://www.it.ufl.edu/policies/aupolicy.html
[2] UF IT Standards for Confidentiality of Restricted Data, http://www.it.ufl.edu/policies/security/documents/restricted-data-standard.pdf
[3] UF Privacy Office, http://privacy.ufl.edu/
[4] Identify Unit ISA/ISM, http://net-services.ufl.edu/cgi-bin/subnet-form.cgi
[5] UF Safe Email Practices, https://infosec.ufl.edu/athome/safe-email.shtml
[6] UF Anti-spam Protection, http://www.cns.ufl.edu/spam