UF Guidelines for IT Workers Who Support Restricted Data Users That Use Email

Who Should Read This

This standard applies to UF IT Workers who support email services.

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

1. For users that must use email to transmit or receive Restricted Data, provide a secure method and:
    a. First obtain permission from the Data Principal (Dean, Director, or Department Chair).
    b. Counsel users to transmit the minimum amount of Restricted Data via email.
    c. Counsel users to never use commercial email services, such as Google, Yahoo, AOL, or MSN, to transmit or receive UF Restricted Data.
2. Any host that is used to transmit or receive Restricted Data via email should be maintained according to the UF Network and Host Security Standard [3].
3. Any email client software used to transmit or receive Restricted Data should be configured with the following safeguards.
    a. Users should be provided unique email authentication credentials that are not shared with other users.
    b. Strong passwords should be required to access email services.
    c. Automatic login to email client software should be disabled.
    d. User connections to email should be logged and the logs should be retained for at least six months.
    e. Encryption should be used.
4. If email message content containing Restricted Data is recorded, the recorded messages should be protected from unauthorized access. Retention of recorded messages should be minimized and obsolete recorded messages must be destroyed prior to disposal [4].
5. If loss or unauthorized exposure of Restricted Data is discovered, the incident must be immediately reported to the Data Principal and the UF Privacy Office [6]. For detailed incident response procedures, see the UF IT Security Incident Response Procedures, Standards and Guidelines [7].
6. UF GatorLink email service [8] meets all the safeguards listed above and is recommended for users that must transmit or receive Restricted Data using email.
    a. Authentication is by GatorLink.
    b. User connections are logged and protected.
    c. Message transmission can be optionally encrypted using transport layer security (TLS).
7. Provide to the user the UF Email Guidelines for Users of Restricted Data [5].

Bibliography

[1] UF IT Security Charter, http://www.it.ufl.edu/policies/security/uf-it-sec-charter.html
[2] UF IT Standards for Confidentiality of Restricted Data, http://www.it.ufl.edu/policies/security/documents/restricted-data-standard.pdf
[3] UF IT Network and Host Security Standard, http://www.it.ufl.edu/policies/security/uf-it-sec-network.html
[4] UF Media Reuse and Data Destruction Standard, http://www.it.ufl.edu/policies/security/documents/it-worker-disposal-standards.pdf
[5] UF Instant Messaging Guidelines for Restricted Data Users, http://www.it.ufl.edu/policies/security/documents/user-email-guidelines.pdf
[6] UF Privacy Office, http://privacy.ufl.edu/
[7] UF IT Security Incident Response Procedures, Standards and Guidelines, http://www.it.ufl.edu/policies/security/uf-it-sec-incident-response.html
[8] GatorLink Email Services, http://imap.ufl.edu/