UF Guidelines for IT Workers Who Support Restricted Data Users That Use Instant Messaging Services

Who Should Read This

This standard applies to UF IT Workers who support instant messaging (IM) services.

Definitions

Instant Messaging Service	Instant messaging or IM is a form of electronic communication that involves immediate or real time correspondence between two or more users who are all online simultaneously.

Purpose

IM is expedient and popular. It's easy to install and use. However, extreme caution should be exercised by users with access to Restricted Data. There is a high risk of Restricted Data exposure by unauthorized IM message interception, monitoring or storing.

Guidelines

1. For users that must use IM 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 IM.
    c. Counsel users to never use commercial IM services, such as Yahoo, AOL, or MSN, to transmit or receive UF Restricted Data.
2. Any host that is used to transmit or receive Restricted Data via IM should be maintained according to the UF Network and Host Security Standard [3].
3. Any IM client software used to transmit or receive Restricted Data should be configured with the following safeguards.
    a. Users should be provided unique IM authentication credentials that are not shared with other users.
    b. Strong passwords should be required to access IM services.
    c. Automatic login to IM client software should be disabled.
    d. User connections to IM should be logged and the logs should be retained for at least six months.
    e. Encryption should be enabled.
    f. The IM file transfer feature should be disabled.
4. If IM 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. The UF Jabber IM service (jabber.ufl.edu) meets all the safeguards listed above and is recommended for users that must transmit or receive Restricted Data using IM.
    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 Instant Messaging Guidelines for Users of Restricted Data [5].
8. For the purpose of communicating security alerts and investigating unauthorized disclosures, IT Workers should maintain records of Restricted Data Users who also use IM.

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-im-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