SPICE EduGuide EG0009
Instant Messaging (IM) Secure Use

This SPICE EduGuide applies to HSC users of Instant Messaging (IM) services. An IM service can be an effective communication tool when expedient delivery of a message is important. However, IM client software products (the user workstation piece) and message transmission (the network component) present risks to our HSC information and computing environment that IM users should be aware of:

Workstation/Network Outage – IM client software is an effective conduit for malicious software such as viruses, spyware and worms. They can enter our network undetected through an IM service particularly when IM is used to exchange files. Unwitting installation or imprudent use of IM client software can cause problems as minor as causing a user's workstation to crash often, to major incidents such as a network wide 'denial of service' attack – basically a network outage.

Compromise/Data Theft – IM client software products commonly reveal important security information such as the IP address of a user workstation, and user logon id and password. These are the keys that hackers look for and use to directly access a user workstation for purposes such as data theft or illegal distribution of copyright material.

Disclosure of Restricted Information – Some free and commercial IM services send user logon id and password, and user messages in clear text over networks. In addition, content of IM messages may be stored on servers on the internet whose security is unknown or untrusted.

Safeguard Requirements and Guidance

- Commercial IM services (YAHOO, AOL, MSN, etc.) lack HSC required safeguards, therefore, are strongly discouraged.
- The UF supported IM service jabber.ufl.edu. can be configured securely, and is encouraged.
- Users must notify their Unit ISM prior to installing IM client software on their computer, and should consult with their IT workstation support service provider to ensure the workstation is protected:
  - Antivirus software on the workstation is up to date, and scanning per Unit requirements
  - Workstation firewall protections should be in place
  - File transfer feature(s) of the IM client software should be turned off if it can be
- If the IM service is to be used for transmission of **Restricted** information, only IM software authorized by the Unit ISM may be used and the following additional safeguards are required:
  - Unique user login with strong password, to access the IM service
  - Auto login may not be enabled
  - User activity must be logged
  - Encryption enabled
- When using IM:
  - **Restricted** information must be limited to the minimum necessary to accomplish the purpose of having it transmitted via IM; maintain awareness that messages can be intercepted, monitored or stored before reaching the intended recipient
  - Verify the identity of anyone you chat with or add to your buddy list; configure their full name and server name in your buddy list, for example 'John Doe, jdoe@ufl.edu' to avoid confusion
  - Do not enable automatic login or 'remember password'
  - Always reject file transfers if they are offered

Policy & Standards References:
TS0006 Electronic Communications
TS0006 Electronic Communications Software
TS0007 Malicious Software Controls