UF Web Guidelines for Users of Restricted Data

UNIVERSITY of FLORIDA

Who Should Know This

These guidelines apply to all users of UF Restricted Data who use web-based services.

Definitions

Web Service — A computer service accessible from a web browser. UF examples are myUFL, ISIS, UF WebMail, WebCT Vista e-Learning and many college and department services.

Purpose

The Internet is a vast network of primarily unregulated web pages. Web pages can be easily spoofed, information from your browser can be intercepted, and vulnerabilities on your computer can be exploited to harvest information. Safeguards for web users to protect Restricted Data are presented in these guidelines.

Guidelines

1. When using the web to access or transmit Restricted Data:
   a. Use only authorized UF web services.
   b. Do not share your user identification with anyone. Use only identification that is uniquely yours to connect to web services.
   c. Use strong passwords to authenticate to web services. Safeguard your password like you would protect your wallet.
   d. Do not use the “auto-complete” features that store your username and password in the browser. Do not select check the box to save your password.
   e. Minimize the amount of Restricted Data accessed or transmitted.
   f. Do not leave your workstation unattended when connected to a Restricted Data web service.
   g. Ensure Restricted Data is encrypted when transmitting it over any wireless connection (even the UF wireless network). One way is to do this is by using the UF Virtual Private Network (VPN) [7].
   h. Ensure any computer used with web services has current updates. Select the automatic update option if available.
   i. Ensure any computer used with web services has current anti-virus protection. Configure automatic updates if available.
   j. Do not follow web links sent in email or instant messages. If you think the link is legitimate, before clicking the link, contact the sender to confirm, by phone or email.
2. Before using Restricted Data on web services, consult your Unit Information Security Manager or local IT staff [1,3]:
   a. To determine authorized web services.
   b. To determine encryption requirements.
   c. For appropriate web browser security settings.
   d. For secure workstation support [6].
3. 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 [5], usually through the User’s supervisor.

Bibliography

[1] UF IT Security Charter, http://www.it.ufl.edu/policies/security/uf-it-sec-charter.html#resource-classification
[2] UF IT Data Security Standard, http://www.it.ufl.edu/policies/security/uf-it-sec-data.html
[3] ISA/ISM list, http://infosec.ufl.edu/unit-isa-ism/
[4] UF Privacy Office, http://privacy.health.ufl.edu/
[5] UF Computer and Software Requirement, http://www.circa.ufl.edu/computers/
[6] UF IT Network and Host Security Standard: http://www.it.ufl.edu/policies/security/uf-it-sec-network.html
[7] UF VPN: http://net-services.ufl.edu/provided_services/vpn/