UF Mobile Computing Device Guidelines for Users of Restricted Data

Who Should Know This

These guidelines apply to anyone with access to UF Restricted Data who also use laptops, personal digital assistants (PDAs) and other mobile computing devices.

Definitions

Laptop A portable computer.

PDA A small, portable hand-held computing device intended for limited functions such as calendar, organization or email.

Mobile Computing Device A portable device such as a laptop, tablet PC, PDA or cell phone with computer functions that can store and/or provide access to data.

Purpose

Mobile computing devices are small and mobile, making them easy to steal or lose. They are expensive, highly functional and in great demand, creating motivation for theft. It follows that the risk of disclosure is significant when Restricted Data is used on mobile computing devices. This includes any personal identification information that might be stored on a mobile computing device including automated access to banks, email and other services.

Guidelines

Listed below are safeguards to protect Restricted Data on mobile computing devices.

1. Avoid using Restricted Data on a mobile computing device. Where no reasonable alternative exists:
    a. First obtain permission from the Data Principal [2].
    b. Minimize the amount of Restricted Data used.
    c. Minimize the length of time the Restricted Data is used.
2. Before using Restricted Data on a mobile computing devices, consult your Unit Information Security Manager or local IT support staff [1,3] for:
    a. Approved mobile computing devices.
    b. Secure configuration and maintenance [5].
    c. Secure backups [7].
    d. Encryption requirements [8].
    e. VPN requirements.
3. Mobile computing devices used with Restricted Data should be labeled as such. Contact information should be included on the label. A label should be placed on the outside of the device, and in electronic form on the device.
4. Mobile computing devices used with Restricted Data should never be left unattended, even briefly, without physically securing them. In general, mobile computing devices should be treated like a wallet; kept in a secure place when not in use.
5. Per UF Privacy Policy [4], removal from UF premises of Restricted Data containing personal identifiers must be authorized by your Dean, Director or Department Chair.
6. Lost or stolen mobile computing devices used with Restricted Data must be immediately reported to the Data Principal and the UF Privacy Office [4], usually through the User’s supervisor, so that necessary steps can be taken to limit damage and liability.
7. Restricted Data on mobile computing devices that are being replaced or retired must be rendered unreadable [6]. The user is responsible, but should consult their Unit Information Security Manager or local IT support staff for destruction requirements.
8. The following safe computing practices should be followed:

a. Use strong passwords that are difficult to guess, but easy to remember. Protect your password like you would protect your credit card.
b. Do not use computer features that remember or auto-complete your password.
c. Ensure any mobile computing device used with Restricted Data has current updates. Select the automatic update option if available.
d. Ensure any mobile computing device used with Restricted Data has current anti-virus protection. Configure automatic updates if available.
e. Configure an inactivity time-out that requires a password for re-entry. The time-out period must not exceed 15 minutes.
f. All wireless communication (i.e. Bluetooth, wifi, infra red, etc.) should be turned off when not in use.

Bibliography

[1]UF IT Security Charter: http://www.it.ufl.edu/policies/security/uf-it-sec-charter.html#resource-classification
[2] UF IT Standards for Confidentiality of Restricted Data: 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.ufl.edu/
[5] Guidelines for IT Workers Who Support Mobile Computing Devices: http://www.it.ufl.edu/policies/security/documents/ITworker_draft/mobile.pdf
[6] UF IT Media Reuse and Data Destruction Standards: http://www.it.ufl.edu/policies/security/documents/ITworker_draft/disposal.pdf
[7] UF Guidelines for IT Workers to Protect Restricted Data on Backup Media: http://www.it.ufl.edu/policies/security/documents/ITworker_draft/backups.pdf
[8] Guidelines for IT Workers regarding Encryption of Stored Data: http://www.it.ufl.edu/policies/security/documents/ITworker_draft/encryption.pdf