UF Guidelines for IT Workers Who Support Mobile Computing Devices Used With Restricted Data

UNIVERSITY of FLORIDA

Who Should Know This

These guidelines apply to UF IT workers who support mobile computing devices. IT workers should read and understand this document before supporting users of mobile computing devices.

Definitions

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

Untrusted Network
Any network that must traverse the Internet to reach UF. All unencrypted wireless, even UF wireless, should also be considered untrusted.

Purpose

The purpose of this document is to outline guidelines for securely managing mobile computing devices used to store Restricted Data [2]. Mobile computing devices are small and portable, making them easy to steal or lose. They can be expensive, highly functional and in great demand, creating motivation for theft. It follows that if Restricted Data is used on a mobile computing device, the risk of inappropriate disclosure is significant. To minimize the risk of exposing Restricted Data, user attentiveness and support from knowledgeable IT workers is required.

Guidelines

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

1. IT workers should maintain awareness and inform users of the risks and responsibilities of using Restricted Data on mobile computing devices. The UF Mobile Computing Device Guidelines for Users of Restricted Data [5] should be given to users. Device maintenance schedules and IT worker contact information should also be provided to users.
2. IT workers should assist Restricted Data Users [2] to determine the classification of data that will be used on their mobile computing device. The data classification determines the appropriate safeguards. This includes any personal identification information that might be stored on the mobile computing device including automated access to banks, email and other services.
3. Storage of Restricted Data on any mobile computing devices should be avoided, regardless of who owns the device. Restricted Data stored on a mobile computing device should be limited to the minimum amount of data necessary to accomplish the purpose for which the data is stored and consistent with Data Principal requirements.
4. Before storing Restricted Data on a mobile computing device, the device should be approved by the Level 2 Unit ISM or their designee, who is responsible to ensure that it is configured to satisfy the UF IT Security Regulations and Data Principals requirements.
5. Storage of Restricted Data on mobile computing devices must be consistent with limitations established by the respective Data Principal. Where applicable, location restrictions of mobile computing devices should be documented. Per UF Privacy Policy [4], removal from

UF premises of Restricted information containing personal identifiers must be authorized by your Dean, Director or Department chair or his/her designee.

6. Mobile computing devices used to store Restricted Data should be managed by UF professional IT workers or a support service approved by the Level 2 Unit ISM. The support service must understand the UF IT Security Regulations and configure devices accordingly. Level 2 Unit ISMs may approve a mobile computing device that they do not support, but they should know the support organization and have reasonable assurance that the mobile computing device is configured to comply with UF IT security regulations.
7. Restricted Data stored on a mobile computing device should not be the only copy and should not be the authoritative copy. If the authoritative copy must reside on a mobile computing device, a reliable and secure process to back up the data should be provided [8].
8. Restricted Data should not be transferred from a mobile device to any device not known to be secure, such as a user's home computer. Care should be taken that data is not inadvertently transferred via another process, such as calendar or address book synchronization.
9. A list of mobile computing devices, users, models and configurations should be maintained by the Unit for purposes of communicating important security alerts, responding quickly to a lost or stolen device, and tracking of Restricted Data. Tracking custody of mobile computing devices may be advisable in some cases, particularly for multi-user mobile devices.
10. Mobile computing devices used to store Restricted Data should have the following protections installed and enabled:
    a. A means to encrypt storage of the data [6]. Where applicable, users should be prevented from unencrypted storage of Restricted Data (e.g. use full disc encryption of all drives on the device). Ensure Users understand that Restricted Data should be stored using encryption. Ensure Users understand that care should be taken to protect access keys and pass phrases in order to recover data. If a hardware key is used or a software key is recorded, Users should be instructed on methods to protect keys.
    b. A means to encrypt transmission of Restricted Data. Transmission across untrusted networks should be secured. Examples include VPN, SSL, SSH or some similar method that not only encrypts the transmission, but verifies that the receiving end of the transmission is trusted. All wireless networks are untrusted, including UF’s wireless network. Encryption methods that ensure remote host identity are required. For example, WEP and WPA are not sufficient security for wireless transmission.
    c. Authentication that permits only authorized users to access the Restricted Data on the mobile computing device. Multi-factor authentication should be considered.
    d. An inactivity time-out that requires a password for re-entry. Time-out periods should be commensurate with risks as determined by the Level 2 Unit ISM. In the absence of a risk based time-out period determined by the Level 2 Unit ISM, 15 minutes or a time consistent with Data Principal rules must be used.
    e. An engraved, indelible or electronic label with contact information.
11. Data on mobile computing devices that are being replaced or retired must be rendered unreadable [7]. Where technology permits, enable functionality to remotely destroy Restricted Data on mobile computing devices that are lost or stolen.

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 privacy policies and procedures, http://privacy.ufl.edu/pandp.html
[5] UF Mobile Computing Device Guidelines for Users of Restricted Data, http://www.it.ufl.edu/policies/security/documents/user-mobile-device-guidelines.pdf
[6] UF Guidelines for IT Workers Regarding Encryption of Stored Data, http://www.it.ufl.edu/policies/security/documents/it-worker-encryption-guidelines.pdf
[7] UF Media Reuse and Data Destruction Standard for IT Workers, http://www.it.ufl.edu/policies/security/documents/it-worker-disposal-standards.pdf
[8] UF Guidelines for IT Workers to Protect Restricted Data on Backup Media, http://www.it.ufl.edu/policies/security/documents/it-worker-backup-guidelines.pdf