UF Removable Media Guidelines for Users of Restricted Data

Who Should Read This

These guidelines apply to Users who store UF Restricted Data on removable media.

Definitions

Removable media: CDs, DVDs, magnetic tapes, floppy disks, external hard drives, and universal serial bus (USB) drives also known as memory sticks, jump drives and thumb disks and other storage media intended for archive and data portability separate from the system on which it originated.

Purpose

Removable media is commonly used to transfer electronic files from one computer to another, and as a mechanism to archive data. Security controls in place on UF computer systems typically do not follow the data when it is copied to removable media. Users who place Restricted Data on removable media must be aware of the security risks and recognize their responsibility to protect the data.

Removable media is small and easily misplaced. USB drives known as memory sticks or thumb disks, are especially easy to lose track of. It's also easy to forget what data is stored on removable media. This is especially true when removable media is used for archives since they aren't used on a daily basis. Although they might initially be stored in a secure place, they are commonly forgotten resulting in a lapse of security. Because removable media is easily lost or forgotten, a high risk exists for inappropriate disclosure if they are used to store Restricted Data.

Guidelines

Listed below are safeguards to protect Restricted Data on removable media.

1. Avoid storing Restricted Data on removable media. Where no reasonable alternative exists:
    a. First obtain permission from the Data Principal [2].
    b. Minimize the amount of Restricted Data stored.
    c. Minimize the length of time that the Restricted Data is stored.
2. Before storing Restricted Data on removable media, consult your Unit Information Security Manager or local IT support staff [1,4] for:
    a. Approved media
    b. Media access restrictions
    c. Secure backups requirements [5]
    d. Encryption requirements [6]
3. Removable media containing Restricted Data should be labeled as such. Contact information should be included on the label. A label should be placed on external surface of the media and in electronic form on the media.
4. Removable media containing Restricted Data should never be left unattended, even briefly, without physically securing it. In general, it should be treated like a wallet; kept in a secure place when not in use.
5. Per UF Privacy Policy [7], removal from UF premises of Restricted Data containing personal identifiers must be authorized by your Dean, Director or Department Chair.
6. Lost or stolen removable media containing Restricted Data must be immediately reported to the Data Principal and the UF Privacy Office [7], usually through the User's supervisor, so that necessary steps can be taken to limit damage and liability.
7. Restricted Data on removable media that is being reused or disposed of must be rendered unreadable [8]. The User is responsible, but should consult their Unit Information Security Manager or local IT support staff for destruction requirements.

Bibliography

[1] UF IT Security Charter, http://www.it.ufl.edu/policies/security/uf-it-sec-charter.html

[2] UF IT Standards for the Confidentiality of Restricted Data, http://www.it.ufl.edu/policies/security/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 Level 2 Unit ISMs, http://net-services.ufl.edu/cgi-bin/subnet-form.cgi

[5] UF Guidelines for IT Workers to Protect Restricted Data on Backup Media, http://www.it.ufl.edu/policies/security/backup-support-guidelines.pdf

[6] Guidelines for IT Workers Regarding Encryption of Stored Data, http://www.it.ufl.edu/policies/security/encryption-support-guidelines.pdf

[7] UF Privacy Office, http://privacy.ufl.edu/

[8] UF IT Media Reuse and Data Destruction Standards, http://www.it.ufl.edu/policies/security/documents/ITworker_draft/disposal.pdf