UF Guidelines for IT Workers to Protect Restricted Data on Backup Media

UNIVERSITY of FLORIDA

Who Should Know This

These guidelines apply to all IT workers who perform backups of UF Restricted Data [2].

Definitions

Backup The copying of data for the purpose of having an additional copy of an original source. If the original data is damaged or lost, the data may be restored from the backup copy.

Purpose

These guidelines are intended to help IT Workers protect the confidentiality of Restricted Data stored on backup media.

Guidelines

Listed below are the safeguards for backing up Restricted Data.

1. For backups that contain Restricted Data, Units should document a backup policy that minimizes retention and specifies destruction of obsolete backups [4].
2. Backup media containing Restricted Data should be stored in a physically secure location with limited access.
3. Backup media containing Restricted Data transported outside of known secure facilities must be encrypted.
4. Offsite storage locations and transportation methods of backup media containing Restricted Data must be approved by the Data Principal (Dean, Director, or Department Chair) [2,3].

Bibliography

[1] UF IT Security Charter, http://www.it.ufl.edu/security/uf-it-sec-charter.html
[2] UF IT Standards for the Confidentiality of Restricted Data, http://www.it.ufl.edu/policies/security/uf-it-sec-data.html
[3] UF Privacy Office, http://privacy.ufl.edu/
[4] UF Media Reuse and Data Destruction Standard, http://www.it.ufl.edu/policies/security/documents/ITworker_draft/disposal.pdf