COMPUTING SERVICES
Section: 135-7 SUPPLEMENT II
Effective: 09/15/2003
Supersedes: N/A
Review Date: TBD
Issuance Date: 09/15/2003
Issuing Office: Administrative Computing & Telecommunications (ACT)

SUPPLEMENT II

LOGICAL SECURITY

Authentication and Authorization

Access to *Restricted* Electronic Information Resources must be limited to authorized users. Authentication methods must be periodically reviewed in light of current technological advances.

For each *Restricted* EIR procedures must be in place that address the following issues:

- How is an authentication token (account) granted? When? Who authorizes new authentication tokens? Are "temporary" tokens permitted?
- How is authentication revoked? Under what circumstances may this happen?
- How often are authentication tokens audited?

Strong authentication methods have at least two of the following three properties:

- something the entity has (e.g. a hardware token which will generate a password)
- something the entity knows (e.g. a password)
- something the entity *is* (e.g. fingerprint)

Currently, the general authentication mechanism tends to be login name/password combinations, which really use only the second property. Until circumstances change, therefore, passwords must be carefully constructed to make them difficult to guess. Password-based authentication mechanisms must possess rules which enforce selection of strong passwords. Passwords must be kept securely; they should not be written down.

Authentication tokens for *Restricted* or *Essential* data should not be shared between entities. If it is imperative that such sharing occur, a special token must be constructed, and the use of this token monitored.

The Principal Holder of the EIR will specify authorization procedures.

"Superuser" accounts often possess the ability to circumvent established authentication and authorization schemes on locally kept data. The following guidelines must be enforced:

- access to superuser accounts must be limited to personnel whose job duties require them.
- provide superusers with less powerful accounts to use when not performing system administration tasks.
- superuser accounts should not be used for other than authorized purposes.
- activities performed using a superuser account must be securely logged, and those logs reviewed periodically.

Revision Control

Development and maintenance of administrative applications performed by University personnel or performed by any vendor engaged by University personnel must conform to the specifications of BFB IS-10, Systems Development Standards.

Logging

Activity logging is an important tool for logical security. Where ever possible, logs should be made recording:

- system access
- authentication (especially failed authentication attempts)
- data access
- software or data modification
- elevation of privilege

Logs, once made, should be monitored for anomalies, preferably by automated means (to protect authorized user privacy, where applicable, and also to provide timely notification of potential problems). Systems containing Restricted EIRs must log, and those logs must be closely monitored. All logs must be retained according to defined data retention schedules; must be backed up following the most stringent requirements governing the criticality and/or sensitivity of the EIRs involved in the logged activity.

As logs themselves may contain sensitive information (account names, passwords, individual usage patterns), they must be kept securely, ideally on a separate machine dedicated to logging (secured against unauthorized access) and/or on write-once media.

Backup

The purpose of Backup (as distinct from Archive) is to protect the system from unintentional loss or catastrophic system failure. Most EIRs will require some sort of regularly scheduled backup; *Restricted* and *Essential* EIRs must have a clearly defined schedule and procedure.

Backups must be treated according to requirements of the most critical/sensitive data contained therein; if an EIR is in the *Restricted-Essential* category, guidelines for scheduling of backups and storage of media must be consistent with the corresponding Disaster Recovery Plan. In any event, backups must be periodically verified by performing test restores – the time to find out that things are not working is not when the data has gone missing.

Physical security of backup media must be consistent with requirements for the EIRs backed up.

An acceptable backup plan will address the following issues:

- how often are backups performed?
- Who is responsible for ensuring that backups are done?
- How is the media labeled?
- Where is the media stored?
- How often is the backup process verified (by performing a test restore), and whose responsibility is the verification?
- When is the media eligible for reuse?

Privacy

All access to *Restricted* data must be restricted to authorized entities only. This implies that proper access controls be in place on any system on which such data resides, and any place it might pass in transit. *Restricted* data

- Must be encrypted whenever it is transmitted (encryption accomplished either by the medium

or at the endpoints of the transmission)
- Must be stored in a manner consistent with its sensitivity (servers must be secured against unauthorized use)
- Must not be kept in insecure circumstances (unencrypted on a desktop, for example)

In defining data privacy standards, the following questions must be addressed:

- How is the data access authorization defined? How is it maintained?
- How is access to the server containing the data appropriately controlled?
- What logging is in place to guard against unauthorized access?
- What applications access the data? If they are run from client machines, how is the privacy of the data in transit maintaineSd?
- What procedures are in place to prevent unauthorized “caching” of the data in non- secure environments (office desktops, for example)