## Anti-Virus and Malware

* Malicious code that attaches to operating system and user files to perform an undesirable and unauthorized action
* Virus – requires user interaction to activate the malicious code, most common security breach in the IT world.
* Worm – self replicating malicious code, does not require user interaction
* Can be distributed by email, websites, documents and even software

Antivirus management:

* Install multilayered anti-virus in condcentric circles
* Keep signatures up to date

## Trusted Recovery

* Ensures that all controls remain intact in the event of a crash.
* System should be forced to reboot in single user mode, non-privileged state
* Manual Recovery – administrator is required to perform actions to manually boot the system into secured or trusted recovery
* Automated Recovery – system is able to automatically perform trusted recovery for a single failure
* Automated Recovery without Undue Loss – like automated recovery but the system does more: verification and protection for classified objects. Can restore corrupt files, rebuild data from logs, verify integrity of key system components

## Configuration and Change Management

All changes must be tracked audited, controlled, identified and approved. Changes should be rigorously tested.

* Apply to introduce change
* Catalog intended change
* Schedule the change
* Implement the change
* Reporting change to appropriate parties

## Reusable media

Delete, erase, remove – removes the file handle, data remains. In Windows, moves to the “trash” folder

Clearing, overwriting - unclassified data (1s and 0s) are written over part or all of media, ensures data cannot be recovered by any means.

Purging – multiple overwrites, 7x to 10x overwrites

Sanitization – prepare media for destruction

Degaussing – magnetic media is subject to magnet to return media to new or original state.

Physical destruction – incineration, crushing, shredding, dissolving in acid.

### Auditing

Typical Audit record

* **Date and time** of an event
* **Who** performed the even
* **Where** the event occurred
* Terminal or workstation, IP address
* Application
* **Details** about the event
* Input data
* Old and new values
* Line number where an exception occured

Types of audit trails:

* Network layer information
* System events
* Application events
* User events: logon, logoff, use of privileges
* Keystroke

## Monitoring

**Pen Testing**

* Zero knowledge, black box testing, or closed
* Partial knowledge, information can be provided to define the boundaries for the test
* Full knowledge

**Methodology:**

* Reconnaissance / discovery (research)
* Enumeration: gain information with intrusive methods, probing
* Vulnerability analysis (threat modelling)
* Exploitation

(Note to student: Please add more content!)