

3.1 Sensitive Information Protection Policy

POLICY:

Information systems storing or serving sensitive information should be operated on secured systems within the environment of Computer Services.

Rationale:

The rising frequency of security incidents involving network-attached devices significantly increases the probability that sensitive data if not properly authorized and protected may be exposed to unauthorized viewing or modification. Addressing the potential of identify theft of information about individuals has become an increasing concern of the institution. Established procedures for protection and release of sensitive information must be followed regardless of the platform that data is being stored or processed on.

Compliance:

Chairs and Vice Presidents are responsible for monitoring compliance by their respective users with this policy and associated standards by directing reviews of, and action on, reports related to compliance with this policy that are generated by Computer Services.

Sensitive Information on Serving Devices:

Sensitive Information is defined as any combination of the following data records:

- Social Security Account Number
- Personal identification numbers which may be used other than Social Security Number
- Information protected by the Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Information protected by the Family Educational Rights and Privacy Act (FERPA)
- Credit card account numbers
- Bank account numbers
- Lists of computer systems ids and/or passwords

Sensitive Information on Desktops/Laptops/Workstations:

Storage of sensitive information on devices that are not used or configured to operate as serving devices is discouraged and only acceptable if the user responsible for the device takes proper care to isolate and protect files containing that information from inadvertent or unauthorized access or viewing. Assistance with securing sensitive information may be obtained from Computer Services.

Alternative Locations for Serving Devices:

Alternative locations must be reviewed and approved by the Computer Services Department. Such exceptions will be made only after it has determined that the server providing sensitive information to the campus network and/or to the Internet is secured through reasonable procedures.