Data Security Policy

Objectives

Auburn University has in its possession, for the express purpose of supporting the University’s mission, large quantities of computerized information relating to its employees and students. Some of this information is private and confidential and considered to be sensitive data. Sensitive data is defined as any information that could cause an individual personal financial harm if disclosed and used improperly. Examples of sensitive data include but are not limited to social security numbers, credit card numbers, computer passwords, and any personal information flagged for non-disclosure. This information must be protected against accidental disclosure and unauthorized use. The following policy is designed for this purpose.

Policy

It is the responsibility of each individual with access to sensitive data resources to use these resources in an appropriate manner and to comply with all applicable federal, state, and local statutes. Additionally, it is the responsibility of each individual with access to sensitive data resources to safeguard these resources. Methods of safeguarding sensitive data include:

1. Sensitive data should not be stored on personal desktop or laptop computers since these computers tend to reside in less secure locations than central servers.

2. Access to computers that are logged into central servers storing sensitive data should be restricted (i.e. authenticated logins and screen savers, locked offices, etc.)

3. Access to sensitive data resources stored on central servers should be restricted to those individuals with an official need to access the data.

4. All servers containing sensitive data must be housed in a secure location and operated only by authorized personnel.

5. Copies of sensitive data resources should be limited to as few central servers as possible.

6. Sensitive data should be transmitted across the network in a secure manner (i.e., to secure web servers using data encryption with passwords transmitted via secure socket layer, etc.)

7. Any accidental disclosure or suspected misuse of sensitive data should be reported immediately to the appropriate University official.

ADOPTED: May 4, 2005