Data Management, Use and Protection

I. RATIONALE AND BACKGROUND

Data, in their many forms, are one of the University's most important assets. In every area, and at every level of the campus, members of the campus community (i.e., faculty, students, staff, and agents or affiliates of the University) are managing or using campus data. Highly sensitive data is a vital resource of which is made available to all employees who have a legitimate need for it, consistent with the University's responsibility to preserve and protect such information by all appropriate means.

The purpose of this policy is to highlight specific requirements that must be met by all who handle, use, store, or otherwise manage highly sensitive university data.

II. POLICY

A) GENERAL STATEMENTS

1. It is the responsibility of each individual with access to highly sensitive data resources, as defined in the data classification policy 309.4, 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 highly sensitive data resources to safeguard these resources.

2. The University of Arkansas payment card processing and security policies (309 series) governs the handling of payment card numbers and related personally identifiable information.

3. As noted earlier, it is the responsibility of each individual to determine if they have highly sensitive data on their individual-use device(s) and media and, if so, to ensure compliance with this policy. Failure to comply with requirements of this policy will result in loss of access to the data. The Associate Vice Chancellor for Information Technology Services enforces this policy at the direction of the Vice Chancellor for Finance and Administration.

B) SENSITIVE DATA HANDLING

Methods of safeguarding highly sensitive data include:

1. Highly 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. Highly sensitive data should not be stored on individual-use, removable media, including but not limited to external hard drives, magnetic tapes, diskettes, CDs, DVDs, and USB storage devices (e.g., thumb drives).

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

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

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

6. All servers containing sensitive data must be protected by appropriate firewall rules and must undergo a regular vulnerability assessment.

7. All servers containing sensitive data must maintain authentication, security and similar system logs for no shorter than 120 days.

8. For all information system resources which contain or access data classified as "sensitive" per the data classification standard, processes must be in place to ensure the access and activity is recorded and reviewed.

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

10. Highly 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.)

C) SENSITIVE DATA STORAGE

1. All individuals must routinely inventory their respective electronic devices for highly sensitive data using processes or procedures recommended by Information Technology Services.

2. Individuals must seek written approval of the data owner and the Associate Vice Chancellor for Information Technology Services to electronically store highly sensitive data on individual-use electronic devices or electronic media in order to meet an essential business need of the college, department, or unit.

3. Highly sensitive data must be securely encrypted on the electronic device or media, according to encryption methods recommended by Information Technology Services.

4. A log-in password must be enabled for the electronic device and, if available, the electronic media. The password must meet or exceed appropriate complexity levels. The password must not be shared with anyone.

5. A password-protected screen saver, if available, must be enabled on the electronic device and set to activate after a maximum of ten minutes of user inactivity. The password must meet or exceed appropriate complexity levels. The password must not be shared with anyone.

6. At a minimum, the electronic device must employ the basic security requirements described in the "Securing Electronic Devices" process and procedures published by Information Technology Services.

7. The data must be deleted from the individual-use device or media as soon as they are no longer required using secure methods according to the Electronic Data Removal section of this policy and the Records Retention and Disposition Policy.

8. Management of the electronic device may not be outsourced to any party external to the University without written approval from the data owner and the Associate Vice Chancellor for Information Technology Services. This written request and approval/disapproval must be filed in a secure location for subsequent audit purposes.

D) ELECTRONIC DATA REMOVAL

1. All software and data files must be removed by University-approved procedures from electronic devices and electronic media that are surplused, returned to a leasing company, or transferred from one University employee to another employee having different software and data access privileges. When electronic devices are sent outside the University for repair, all data must be either encrypted or removed to the extent possible.

2. All electronic devices must be routinely scanned for highly sensitive data (as defined in the Data Classification Policy) that is not stored on University-approved secured servers and storage. Any data found must be reported to the Associate Vice Chancellor for Information Technology Services. This data must be moved to a secured location, or removed according to University-approved procedures.

E) DATA BREACH REPORTING

1. Any accidental disclosure or suspected misuse of highly sensitive data must be reported immediately to the appropriate University officials. The appropriate University Officials include the data owner (as defined in the appendix of the Freedom of Information Act policy), the Vice Chancellor for Finance and Administration, the Provost, General Counsel, Registrar's Office, Payment Card Operations (as required in Payment Card Incident Response policy 309.2) and Information Technology Services - Security Office.

F) COMPENSATING CONTROL AND EXCEPTION REQUEST

1. It is imperative that University of Arkansas faculty, staff, and students comply with this policy and any related procedures or guidelines. However, there are circumstances that fall outside the ability to comply with and/or conform to the standard. In such instances, an exception must be documented and approved by Internal Audit, and Information Technology Services - Security Office.
2. Requests for exception must include: a valid business justification; a risk analysis; compensating controls to manage risk; and technical reasons for exception.
3. Requests for exception that create significant risks without compensating controls will not be approved.
4. Requests for exceptions are reviewed for validity and are not automatically approved.
5. Requests for exceptions must be reviewed frequently to ensure that assumptions or business conditions have not changed. Exemption renewals are not automatically approved.

III. RESPONSIBILITY

This policy is applicable to all university schools, colleges, departments, and other units. The Associate Vice Chancellor for Information Technology Services, at the direction of the Vice Chancellor for Finance and Administration, is responsible for establishing appropriate information and data protection policies as well as implementing mechanisms to ensure that protection. This policy, as well as any other information technology, data protection and management, and security policies, will be updated on a regular basis and published as appropriate.

Specifically, the Associate Vice Chancellor for Information Technology Services should ensure that there is:

- Appropriate awareness among data owners, data custodians, and, insofar as possible, all data users of security processes and procedures,

- Guidelines and mechanisms for data protection practice available to University constituencies, and
- University schools, colleges and other units responsibility and responsiveness to ensure that security is effectively accomplished.

IV. DEFINITIONS

Individual-Use Electronic Devices: Computer equipment, whether owned by the University or an individual, that has a storage device or persistent memory, such as desktop computers, laptops, tablet PCs, BlackBerrys and other personal digital assistants (PDAs), and smart phones. For purposes of this policy, the term does not include shared purpose devices, such as servers (including shared drives), printers, routers, switches, firewall hardware, etc.

Individual-Use Electronic Media: All media, whether owned by the University or an individual, on which electronic data can be stored, including but not limited to external hard drives, magnetic tapes, diskettes, CDs, DVDs, and USB storage devices (e.g., thumb drives).

April 2011