Overview

The purpose of this policy is to highlight specific requirements that must be met by all users that handle, use, store, or otherwise manage "Highly Sensitive" university data. The university's responsibility is to preserve and protect "Highly Sensitive" information by all appropriate means. This policy is applicable to all university schools, colleges, departments, and other university units, and all users should be aware of their responsibilities to ensure that security is effectively accomplished.

I. Data Use

It is the responsibility of each individual with access to "Highly Sensitive" data resources to understand the definition of "Highly Sensitive" data, and to use these "Highly Sensitive" data resources in an appropriate and ethical manner. Each individual must comply with all applicable federal, state, and local statutes. It is the responsibility of each individual with access to "Highly Sensitive" data resources to safeguard these resources. Reference: Data Classification Policy.

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 Director of Information Services enforces this policy at the direction of the Vice Chancellor for Student Affairs.
Highly sensitive data will be accessed, used or disclosed only for purposes consistent with applicable law and university policy.

Access, use or disclosure of Highly Sensitive data will be limited to the minimum that is necessary to achieve the legitimate purpose for which the data was accessed.

II. Data Management

Access to "Highly Sensitive" data should be restricted to those individuals with an official need to access the data.

All servers containing "Highly Sensitive" data must be housed in a secure location and operated only by authorized personnel.

All servers containing "Highly Sensitive" data must be protected by a firewall.

All servers containing "Highly Sensitive" data should maintain authentication, security, and system logs.

For all information system resources which contain or access data classified as "Highly Sensitive," processes must be in place to ensure that access is logged, and ideally that activity is recorded and reviewed.

"Highly Sensitive" data transmitted across the network must use secure protocols such as SFTP (secure file transfer protocol), SSL (secure socket layer), SSH (secure shell), Microsoft RDP (remote desktop protocol), etc. Authentication (login) to "Highly Sensitive" data must also use secure authentication protocols.

Specific data and physical security measures that are implemented will be documented by Information Services.

III. Data Storage

"Highly Sensitive" data should not be permanently stored on personal devices, including but not limited to desktops, laptops, iPads, smart tablets, etc.

"Highly Sensitive" data should not be permanently stored on removable media, including but not limited to external hard drives, CDs, DVDs, and USB storage devices (e.g., thumb drives).

If there is a valid reason that "Highly Sensitive" data must be temporarily stored on personal devices or removable media, then the data must be securely encrypted at rest, according to encryption methods recommended by Information Services.

"Highly Sensitive" data temporarily stored as described above must be deleted immediately from personal devices or removable media as soon as they are no longer required.
All individuals should routinely inventory their respective personal or removable devices for "Highly Sensitive" data.

All software and data files must be removed by College approved procedures from electronic devices and electronic media that are surplused.

IV. Data Breach Reporting

Any accidental disclosure or suspected misuse of "Highly Sensitive" data must be reported immediately to the appropriate university officials. Appropriate university officials include immediate supervisors, the Director of Information Services, the Vice Chancellor for Student Affairs.

V. Clarifying Points

Continuous improvement. The content of this document subject to regular review based on input from UACCB Information Services staff and the campus community. Suggestions for improvement should be directed to the Director of Information Services.

Adopted: March, 15, 2023