Augusta University
Policy Library

Electronic Data Storage Backup

Policy Owner: Information Technology

POLICY STATEMENT
In order to protect institutional data against loss or destruction, it is required that such data be created and stored within the system of record utilizing an Information Technology (IT) approved data storage device (e.g. storage area network space, a shared or home directory). All contracted service providers, personnel and students that establish or create electronic data outside of the IT storage service shall define, document, and implement a backup procedure. Department Heads will assume the role of data trustee for their department's data and will appoint a data steward and manager.

REASON FOR POLICY
Augusta University maintains a large and growing body of data stored exclusively in electronic form. Data is critical to the operation of the enterprise, and it is clear that the enterprise could suffer significant loss should an important set of data be permanently lost. The policy is intended to ensure the integrity, availability, and confidentiality of electronically maintained data, including but not limited to confidential, sensitive, or personally identifiable information, and that Augusta University business units are able to resume operation in the event of any incident that causes data loss; equipment failure, inadvertent user error, fire, flood, vandalism, etc.

AFFECTED STAKEHOLDERS
Indicate all entities and persons within the Enterprise that are affected by this policy:

☐ Alumni ☒ Faculty ☒ Graduate Students ☒ Health Professional Students
☒ Staff ☒ Undergraduate Students ☒ Vendors/Contractors
☐ Visitors ☐ Other:

DEFINITIONS
- Data trustees are executives who have overall responsibility for all the data sets maintained by the units reporting to them. The data trustees are responsible for ensuring that campus institutional data resources are used in ways consistent with the mission of Augusta University. The data trustees have the responsibility for the appointment and accountability of data stewards.
- Data stewards, or their designees, are responsible for recommending policies, and establishing procedures and guidelines concerning the accuracy, privacy and integrity of the data subsets for which they are responsible. Individually, data stewards act as advisors

to the data trustees and have management responsibilities for data administration issues in their functional areas.

- Data managers have day-to-day responsibility for managing administrative processes and establishing business rules for the transactional systems. They have operational responsibility for the data management activities related to the collection, maintenance, protection, and dissemination of data in their functional areas
- Institutional Data Information may be considered institutional data if it satisfies one or more of the following criteria:
    - Data used for planning, managing, reporting, or auditing a major administrative function;
    - Data referenced or used by a participant organization to conduct organization business;
    - Data included in an official participant organization administrative report; or,
    - Data used to derive an element that meets any of the criteria above.

PROCESS & PROCEDURES

IT provides various types of electronic storage space for faculty, staff and students. Daily backups are performed using an enterprise data backup solution that includes off-site storage.

The following file storage areas are available:

- PRIVATE - Your private file storage area. This space is for documents only. No programs or licensed applications should be stored in this area.
- SHARE - Every department has a folder in which its members can share and collaborate on their data files. Like the PRIVATE area, program files are not permitted in this storage area.
- RESEARCH DATA - Many researchers require access to large capacity, secure storage for their research data. Additional research storage space may be allocated upon request.
- BOX – Box is a secure file sharing and collaboration system that is delivered through a strategic partnership between Augusta University and Box.

Special procedures related to Box storage:

- Confidential and regulated data (Student records, Protected Health Information, etc.) may be stored within Box if there is a legitimate business need.
- Enterprise owned devices must be encrypted if they utilize the data synchronization capabilities of Box to store confidential/regulated data.
- Confidential and regulated data shall be restricted to those who have a legitimate business need to know the information using access controls available through Box including user name and passwords.

- Links that do not require authentication should never be used to grant someone access to confidential or regulated data.
- Only enterprise owned devices shall have the synchronization client installed. The synchronization client may not be installed on personally owned devices.
- Anyone who wishes to use a third party cloud application that interfaces with Box must receive prior approval through the IT procurement process.
- Box storage is to be used for legitimate University business purposes only.

Contact the IT Service Desk at 706-721-4000 for questions relating to electronic storage space.

REFERENCES & SUPPORTING DOCUMENTS
Intentionally left blank.

RELATED POLICIES
Data Management and Classification Policy

APPROVED BY:
President, Augusta University and CEO, AU Health System **Date:** 06/20/2017