Secure Data Handling Standard

Revision Notes	Last Updated:	Status: APPROVED
Version 1.1 8/2017 Endorsed by ISAC, Reviewed By Cabinet Ratified	8/2017	

Table of Contents

1. Objectives ……Page 1
2. Scope Statement ……. Page 1
3. Requirements ……..Page 1
4. Definitions ……Page 5
5. References……Page 5

1. Objective:
The objective of this standard is to clearly define the requirements needed for securely utilizing institutional data including confidential and sensitive information.

This standard addresses the objectives outlined in sections 4.4.3.3, 4.4.3.4, and 4.4.3.5 of the University Information Security Policy.

2. Scope:
The standard applies to all Appalachian State University employees, students, and affiliates and all University IT services (see 4.1).

3. Requirements

3.1 Designation Of Secure Data Environments
University units that frequently manage, store, or process Confidential and Sensitive University data may be designated as a Secure Data Environment (see 4.2) by the Chief Information Security Officer.

This designation indicates that the unit has more appreciable exposure and impact associated with data risks such as data theft, data leaks, data corruption, or data loss.

This designation also brings forward the following requirements:

- All information resources used in these Department may be classified as high impact assets so that a consistent level of security controls can be applied (see Minimum Security Standard). ● All full and part-time employees within the unit may be designated as privileged users (see 4.7) to ensure that common security awareness and authentication protection measures may be applied.

- **3.2 Secure Use Of Public and Internal University Data**

As detailed in the University Data Management Standard, University Public and Internal data (see definitions below) typically do not necessitate extensive data handling requirements for secure use.

When handling both printed and/or electronic versions of Public or Internal data, the following rules must be followed:

- Public data must be reviewed to ensure that the integrity and availability of the data is maintained at an appropriate level based on the context of use and need.

- Internal data must be used in a manner that limits access to Appalachian State University employees or authorized partners with a business need to access this information.

3.3 Secure Use Of Sensitive and Confidential University Data

As detailed in the University Data Management Standard, Confidential and Sensitive data do require more extensive data handling requirements to help manage risk associated with theft, misuse, loss, or corruption.

When handling both printed and/or electronic versions of sensitive and confidential data, the following requirements must be met:

3.3.1 Creation and Identification of Sensitive and Confidential Data

Records containing Confidential and Sensitive data should only be created where there is a legitimate and justifiable business need that is authorized by the appropriate data steward (see University Data Management Standard 3.2.2).

3.3.2 Secure Storage and Sharing of Sensitive and Confidential Data

Confidential and Sensitive Data must only be stored using systems of record (see 4.6) and electronic copies must be kept to a minimum and stored in pre-approved locations or in systems that have been evaluated and approved by the Chief Information Security Officer (see tables below).

Confidential and Sensitive Data may only be exchanged using secure methods of sharing that have been approved by the Chief Information Security Officer (see tables below).

The following storage and sharing methods have been pre-approved for use with Sensitive and Confidential data:

3.3.2.1 Sensitive Data - Approved Storage + Sharing Methods

Approved Storage Locations	Approved Secure Sharing Methods	Insecure Methods Not Permitted
Electronic Records Banner Fortis uStor University owned/managed computers ASU Google Drives PeopleAdmin Printed Materials Locked Filing Cabinet, Desk, or Locked Room with Limited Access.	Filelocker	Sensitive data must not be stored or shared via: - Email, Instant Messaging, Social Networks, P2P Solutions - Removable Media (thumb-drives, ext. hard-drives) - Any Personal Cloud Storage Accounts (Google Drive, SkyDrive, Amazon Drive, Dropbox, Box, etc) - Any Personal Computer Devices (including Smartphones).

3.3.3.2 Confidential Data - Approved Storage + Sharing Methods

Approved Storage Locations	Approved Secure Sharing Methods	Insecure Methods Not Permitted

Electronic Records Banner Fortis uStor Printed Materials Locked Filing Cabinet, Desk, or Locked Room with Limited Access.	Filelocker	Confidential data must not be stored or shared via: - Email, Instant Messaging, Social Networks, P2P Solutions - ASU owned PCs or Laptops (Can be used to upload or access data but not long terms storage or direct file-sharing). - Removable Media (Thumb-drives, Ext. Hard-Drives) - Any Cloud Storage Solutions (Google Drive, SkyDrive, Amazon

		Drive, Dropbox, Box, etc) - Any Personal Computer Devices (including Smartphones).

3.2.3 Approval Required For Storage and Sharing of Confidential or Sensitive Data

The ITS-Office of Information Security must evaluate storage and sharing solutions that may be considered for use with confidential or sensitive data (including service provider hostings) based on risk, security measures, compliance obligations, and related standards. These locations must be approved by the Chief Information Security Officer prior to any use.

3.2.4 Data Disposal and Destruction of Records Containing Confidential or Sensitive Data

Media and printed materials containing confidential or sensitive data may not be surplused, repurposed, or discarded without first ensuring that confidential or sensitive data is rendered into an unreadable format. The removal of this data must conform with the University Records Retention Policy and Archives policy as well as utilize an approved method of data sanitization or destruction:

Approved methods include:

ITS Performed Data Wipes - The wipes may only be performed by authorized ITS staff using sanitization methods that meet or exceed NIST SP-800-88 guidelines. Validation

logs of wipe are maintained.

ITS Media Destruction / Degaussing - Media destruction or degaussing may only be performed by authorized ITS staff. Validations logs of destruction or degaussing activities are maintained.

Use of Paper Shredders - University owned paper shredders may be utilized for rendering printed materials with confidential or sensitive data unreadable. Cross-cut shredders are strongly recommended for units that may oversee large amounts of printed confidential or sensitive records.

3.3 Required Reporting of Potential Data Security Incidents

All University employees are required to report both suspected or validated security incidents that may pertain to any other information stored, processed or maintained to support the conduct of University business. These reports must be given to both their immediate supervisor as well as the ITS Office of Information Security. Willful failure to report security incidents could lead to

disciplinary actions up to and including termination.

3.4 Enforcement, Exemptions, and Advisement

3.4.1 Authority and Enforceability - This standard is established under the authority of the Chief Information Security Officer (Information Security Policy 4.3.3). In the event of violation of this standard, the Chief Information Security Officer may require that non-compliant University IT services be disconnected or temporarily suspended until the minimum security controls (see section 3.3) are established and/or verified.The Office of Human Resources or Academic Affairs may be consulted to see if further disciplinary actions should be considered.

3.4.2 Exemptions - Exemptions to this standard must be undergo a formal risk evaluation and receive signed approval by the University Chief Information Officer.

3.4.3 Review and Advisement - Collaborative advisement concerning these standards are provided by the University IT Security Liaisons Group and Campus Information Security Advisory Committee.

4. Definitions

4.1 "IT Services" - IT services refers to the application of business and technical expertise to enable the creation, management and optimization of or access to information and business processes and includes business process services, application services and infrastructure services.

4.2 "Secure Data Environments" - Campus division/units where Information Security risks are known to be higher due to requisite use of Confidential (data breach risks) or Sensitive information (reputational risks).

4.3 “Privileged User” - Privileged users are individuals who conduct University business and hold service accounts that meet one of the following criteria:

- Utilize an account that has elevated rights that allow for actions that can alter the performance, security, or operation of University systems and services and impact other users.
- Utilize an account that allows access to read, copy, or modify Confidential University Data (see Data Management Standard).
- Routinely perform work for a University unit that has been designated as a Secure Data Environment.

4.2 “Endpoint” - An endpoint is defined as any laptop or desktop, used to support or conduct official University business.

4.3 “Server” - A server is defined as a host that provides a network accessible service.

4.4 “Application” - An application is defined as software running on a server that is remotely accessible.

4.5 “Institutional Data” - Institutional data refers to one or more data elements that meets one or more of the following criteria:

- Any Data that originates in an academic or administrative system.
- Any Data contained within the University data warehouse.

4.6 “System of Record” - An information storage system (commonly implemented on a server running a database management system) that is the authoritative data source for a given data element or piece of information.

5. REFERENCES

5.1 University Information Security Policy

5.2 University Data Management Standard

5.3 University Statement of Confidentiality

5.4 University Identity Theft Prevention Plan

5.5 University Payment Card Services Policy