Appalachian STATE UNIVERSITY®

Data Security HandBook

Version 1.0 03/2016

ITS-Office of Information Security |
http://security.appstate.edu

1. Introduction

Appalachian relies upon the efficient use of data to accomplish our shared mission and associated objectives. However, our institutional data is often subject to security threats as well as numerous legal and contractual requirements that necessitate its protection.

To help efficiently address of these risks and compliance needs, it is essential that University employees approach data handling and security efforts in a consistent and uniform manner.

To achieve this, the University has adopted several university-wide policies and standards that define essential roles, responsibilities, and definitions related to data security. For reference, these relevant policies and standards include:

- Information Security Policy
- Data Management Standard
- Statement of Confidentiality
- Minimum Security Standard

The overall goal of this handbook is help Appalachian State University employees easily find answers to the most common data security questions within a single reference document.

Some questions this handbook addresses include:

- How can I determine if the data I'm using needs to be protected/restricted?
- What IT services are we permitted to use to copy or transmit sensitive data?

We hope you find this manual useful to help address questions regarding data security. If you have questions or are unable to find the information you are looking for please contact: ITS - Office of Information Security (security@appstate.edu Ext: 6277)

Remember - Information Security Is A Shared Responsibility!
We all have a role to play.

2. University Data Classifications

Appalachian State University recognizes **four** data classifications for institutional data including: **Confidential**, **Sensitive**, **Internal**, and **Public** Data classifications. These classifications reflect the level of sensitivity associated with types of data including the degree of access restrictions and level of negative impact the University could experience if this data is subject to common threats.

It is important to note that all University data records whether encoded in electronic or physical forms can be directly associated with one of these classifications.

Confidential Data - "Red Data"

Confidential data is information whose unauthorized disclosure and/or loss of control would reasonably result in significant financial losses, unacceptable risks, criminal liability, or impairment to the efficient conduct of the University mission.

Confidential Data often have these attributes:

- Protection of this data is prescribed within legal and/or contractual requirements.
- Confidential data is usually not considered a public record subject to disclosure (NCGS-132), but even if the data would be releasable under the public records act it may still be protected under other state or federal laws
- The handling of this data is often addressed by detailed data security requirements.

Sensitive Data - "Amber Data"

Sensitive data is considered private and must be protected, but has a lesser degree of impact associated with unauthorized disclosure and/or loss of control versus confidential data.

Sensitive Data often have these attributes:

- Protection measures are either not prescribed by legal or contractual requirements or may be significantly less stringent that those for confidential data due to a lower risk of harm if the data is disclosed.
- Access rights established around identified processes and needs.
- Handling of this data requires elevated data security requirements.

Internal Data - "Green Data"
Internal data is often proprietary or produced only for use by members of the University community who have a legitimate purpose to access such data.

Internal Data often have these attributes:

- Access established for fulfillment of daily University business requirements.
- Handling of this data requires general security requirements.
- Institutional information that has few restrictions or is intended for public use.

Public Data - "White Data"
Public Data is meant for broad consumption with little to no restrictions on access or use.

3. Default Data Classification For Institutional Data

The default data classification for ASU institutional data is **Internal.** In the absence of any explicit data classification or labeling, all Institute data shall be presumed to be **Internal** and should be protected as such. This means that this data should not be shared with third parties without formal authorization.

4. List Of Confidential and Sensitive Data Elements

The following table lists individual data elements that must be treated as **Confidential** or **Sensitive** Data due to Appalachian's legal, contractual, and risk based objectives. If you are dealing with one of these data elements and evaluating new processes or storage and sharing options, then you need to contact the ITS Office of Information Security for review and assistance.

Appalachian State University
Confidential & Sensitive Data Elements
03/15/2016

Data Element	FERPA	GLBA	PCI-DSS	HIPAA	NCID Theft	NC Public Record	NC HR Act	FTC Red Flag	AppState Selected (Other)	ASU Classification Level and Justifications
Alien or Immigration ID	X FERPA (if student)	X GLBA			X NCID Theft		X NC HR Act	X FTC Red Flag		Confidential **Legal/Contractual Issues:** Data protection and breach notice requirements. **Info. Risks**: Fiscal and Reputational risks from unauthorized disclosure, modification, or loss.
Attorney Client Relationship						X NC Public Record			X Appstate Selected	Sensitive **Legal:** Potential misdemeanors for inappropriate access or sharing. **Risk**: Reputational risks from unauthorized disclosure.
Bank Account Number		X GLBA		X HIPAA	X NCID Theft		X NC HR Act			Confidential **Legal/Contractual Issues:** Data protection and breach notice requirements. **Info. Risks**: Fiscal risks from unauthorized disclosure, modification, or loss.

Banking Account Password	**X** FERPA	**X** GLBA		**X** HIPAA	**X** NCID Theft	**X** NC Public Record	**X** NC HR Act	**X** FTC Red Flag		**Confidential** **Legal/Contractual Issues:** Data protection and breach notice requirements. **Info. Risk**: Fiscal risks from unauthorized disclosure, modification, or loss
Beneficiary Information					**X** NCID Theft		**X** NC HR Act			**Confidential** **Legal/Contractual Issues:** Data protection and breach notice requirements. **Info. Risk**: Fiscal risks from unauthorized disclosure, modification, or loss
Biometric Information					**X** NCID Theft					**Confidential** **Legal/Contractual Issues:** Data protection and breach notice requirements. Risk: Fiscal risks from unauthorized disclosure, modification, or loss.
Birthdate	**X** FERPA	**X** GLBA		**X** HIPAA			**X** NC HR Act	**X** FTC Red Flag		**Confidential** **Legal/Contractual Issues:** Data protection and breach notice requirements. Risk: Fiscal risks from unauthorized disclosure, modification, or loss.

Criminal Investigation Report or Police Record.	X FERPA					X NC Public Record * (NCGS 132-1.4)	X NC Personnel Act			**Confidential** **Legal/Contractual Issues:** Data protection and breach notice requirements. Risk: Fiscal risks from unauthorized disclosure, modification, or loss.
Dependents (relationship to individual or employee)							X NC HR Act			**Sensitive** **Legal:** Potential misdemeanors for inappropriate access or sharing. **Risk**: Reputational risks from unauthorized disclosure.
Disability Information	X FERPA			X HIPAA			X NC HR Act		X AppState Selected	**Confidential** **Legal:** Data protection and breach notice requirements. **Risk:** Fiscal risks from unauthorized disclosure, modification, or loss.
Driver's License Number	X FERPA				X NCID Theft			X FTC Red Flag		**Confidential** **Legal**: Data protection and breach notice requirements. **Risk**: Fiscal risks from unauthorized disclosure, modification, or loss.
Employee HR file info (e.g., performance, benefit, financial,		X GLBA					X NC HR Act			**Confidential** **Legal**: Data protection and breach notice requirements. **Risk:** Fiscal risks from unauthorized

medical)										disclosure, modification, or loss.
Fingerprints					X NCID Theft					**Confidential** **Legal**: Data protection and breach notice requirements. **Risk:** Fiscal risks from unauthorized disclosure, modification, or loss.
Home Address	X FERPA						X NC HR Act	X FTC Red Flag		**Sensitive** **Legal:** Potential misdemeanors for inappropriate access or sharing. **Risk**: Reputational risks from unauthorized disclosure.
Marital Status or Effective Date	X FERPA	X GLBA					X NC HR Act			**Sensitive** **Legal**: Potential misdemeanors for inappropriate access or sharing. **Risk**: Reputational risks from unauthorized disclosure.
Medical Records (including medical ID number (PHI)	X FERPA (Students Only)			X HIPAA			X NC HR Act			**Confidential** Legal: Data protection and breach notice requirements. Risk: Fiscal risks from unauthorized disclosure, modification, or loss.
Mothers Maiden Name	X FERPA (Students Only)	X GLBA		X HIPAA	X NCID Theft					**Confidential** Legal: Data protection and breach notice requirements.

										Risk: Fiscal risks from unauthorized disclosure, modification, or loss
Passport Number	X FERPA	X GLBA			X NCID Theft		X NC HR Act	X FTC Red Flag		**Confidential** Legal: Data protection and breach notice requirements. Risk: Fiscal risks from unauthorized disclosure, modification, or loss.
Payment Card Number (PAN)			X PCI-DSS							**Confidential** Legal: Data protection and breach notice requirements. Info Risks: Fiscal and reputational risks from unauthorized disclosure, modification, or loss
Payment card magnetic strip Info. (Not To Be Stored By AppState)			X PCI-DSS							**Confidential** Legal: Data protection and breach notice requirements. Info Risks: Fiscal and reputational risks from unauthorized disclosure, modification, or loss
Payment Card PIN			X PCI-DSS		X NCID Theft					**Confidential** Legal: Data protection and breach notice requirements. Info Risks: Fiscal risks from unauthorized disclosure, modification, or loss

Private contributor records									X ASU Selected	**Confidential** Info Risks: Fiscal risks from unauthorized disclosure, modification, or loss
Social Security Number	X FERPA	X GLBA		X HIPAA	X NCID Theft	X NC Public Record	X NC Personnel Act	X FTC Red Flag		**Confidential** Legal: Data protection required under most compliance obligations. Info Risks: Fiscal risks associated with adverse events.
Student Conduct Records	X FERPA								X ASU Selected	**Sensitive** **Legal**: Potential misdemeanors for inappropriate access or sharing. **Risk**: Reputational risks from unauthorized disclosure.
Student Loan Number	X FERPA	X GLBA			X NCID Theft					**Confidential** Legal: Data protection and breach notice requirements. Info Risks: Fiscal risks from unauthorized disclosure, modification, or loss

5. Secure Storage and File Exchange

It is important that approved technologies are used to store and exchange University data. This is particularly true for Confidential and Sensitive Data where accidental disclosure or loss can result in a potential data breach event.

The tables below summarize storage locations and file exchange methods that are approved when managing varied classifications of University data.

If you have questions or would like to determine if a particular application is appropriate for storing or sharing institutional data then please contact the ITS - Office of Information Security (security@appstate.edu   Ext: 6277)

Secure Data Storage and Sharing Methods Overview

Data Classification Level Information must be classified according to the highest (most restrictive) data classification category applicable to any individual data element in the information.		**Examples**	✓ **Secure Storage & File Exchange**
Confidential Data ***High Security***	Unauthorized disclosure and/or loss of control of confidential data may reasonably result in significant financial losses, unacceptable risks, or impair the efficient conduct of the University mission.	● Personal Identifiers: Birthdate, SSN, Driver's license number, Passport or Immigration number, and Mother's Maiden Name ● Financial Data: Credit Card Numbers, Bank Account Numbers ● Authentication Data: Biometric Information, Passwords, Digital Signatures ● Protected Health Information	**Approved Storage** ● Banner ● Fortis ● uStor **Secure Exchange** ● Filelocker
Sensitive Data ***Medium Security***	Sensitive data is private data that must be protected, but has a lesser degree of impact associated with unauthorized disclosure and/or loss of control versus confidential data.	● Personally identifiable information including home address, and marital status ● Personnel Data including beneficiary information, and dependents	**Approved Storage** ● Banner ● Fortis ● uStor ● University computers ● App State Google Drive **Secure Exchange** ● Filelocker
Internal Data ***Standard Security***	Proprietary data or information produced only for use by University members with a legitimate purpose to access such data.	● Internal policies, procedures, and memos ● Budget and salary information	Internal Data should only be stored and shared via University owned, maintained, or purchased devices, solutions, and services.
Public Data ***Minimum Security***	Institutional information that has few restrictions and/or is intended for public use.	● Directory information ● Presentations ● Press releases	There are no security restrictions or guidance needed for Public Data.

Secure Data Storage and Sharing Solutions

IT System / Solution	Confidential Data	Sensitive Data	Internal Data	Public Data	Notes
ASU Owned PCs and Laptops	STOP No Long term storage + File Sharing (see note)	✓ Yes	✓ Yes	✓ Yes	*ASU owned PCs can be used to upload or access confidential data but cannot be used for long terms storage of confidential data or direct file-sharing.*
Banner	✓ Yes	✓ Yes	✓ Yes	✓ Yes	*Banner is a "System of Record" and it is recommended not to copy data from Banner than can be manipulated directly within the application.*
Cloud Storage (Not MountaineerDrive)	STOP No	STOP No	✓ Yes	✓ Yes	*Examples: Personal Google Drive, SkyDrive, Amazon Drive, Dropbox, Box, etc.*
Filelocker	✓ Yes	✓ Yes	✓ Yes	✓ Yes	*Filelocker is the preferred application for securely sharing confidential and sensitive information:* http://support.appstate.edu/answers/filelocker
Fortis	✓ Yes	✓ Yes	✓ Yes	✓ Yes	

IT System / Solution	Confidential Data	Sensitive Data	Internal Data	Public Data	Notes
Instant Messaging	STOP No	STOP No	STOP No	✓ Yes	*Examples: Google Hangouts, Facebook Messenger, WeChat, WhatsApp, Snapchat.*
MountaineerMail (ASU Gmail)	STOP No	STOP No	✓ Yes	✓ Yes	*Note: MountaineerMail may not be used to send confidential or sensitive data. ASU Filelocker should be used instead.*
MountaineerDrive (ASU GoogleDrive)	STOP No	✓ Yes	✓ Yes	✓ Yes	*Note: MountaineerDrive may not be used to store or share Confidential data. ASU Filelocker can be used for sharing.*
Peer To Peer File Sharing Solutions	STOP No	STOP No	STOP No	✓ Yes	*Peer to peer application examples: Bittorrent applications,Gnutella applications, Ares, Edonkey.*
Personal Computing Devices (Including Cell Phones)	STOP No	STOP No	✓ Yes	✓ Yes	*Examples: Personally owned Mobile Phones, Tablets, Home PCs + Laptops.*
Personal Email Account	STOP No	STOP No	✓ Yes	✓ Yes	*Also please see guidance here on conducting Univ. business via personal email.*

IT System / Solution	Confidential Data	Sensitive Data	Internal Data	Public Data	Notes
Removable Media	STOP No	STOP No	✓ Yes	✓ Yes	*Examples: External Hard Drives, Thumbdrives, SIM cards, Optical Media (Bluray, DVD, CDR)*
Social Networks	STOP No	STOP No	STOP No	✓ Yes	*Examples: Facebook, Twitter, Flickr, Google+,*
uStor	✓ Yes	✓ Yes	✓ Yes	✓ Yes	*This is listed as the M drive for most University PCs*.

6. Classifying Aggregate Data and Data Views.

Aggregate data repositories or data views must be classified with the highest (most restrictive) categorization applicable to any individual data element contained therein. For example, on a repository, form, or screen displaying both **Internal** and **Confidential**, the data shall be entirely classified as **Confidential**.

7. Classifying Document Groups and Collections of Records.

In a similar fashion to data views (see above), electronic and printed records often contain a variety of data elements belonging to several data classification levels. Documents and records collections must be classified according to the highest (most restrictive) data classification category applicable to any individual data element contained therein. For example, an individual document or collection of documents that contains both **Internal**, **Sensitive**, and **Confidential**, would be entirely classified as **Confidential**.

8. Addressing Open Records Requests

As part of the the University of North Carolina System, Appalachian State University is subject to the North Carolina Public Records Act (NCGS Chapter 132) which provides a method for third parties to request records associated with the public business of all state agencies. The North Carolina Public Records Act includes requirements involving the exclusion of certain material from these requests. While the data classifications contained in this manual address some relevant aspects of the NC Public Records Act, they should not be considered comprehensive. If your office receive a public records request, then your should contact the Office of General Counsel before responding to this request.
The University's policy regarding Public Records Requests can be found in the University's policy manual in Policy # 105.6.

9. Data Labeling

University Records, including printed materials, may employ data labels to quickly indicate that the type of information they contain. The table below lists the approved label graphics that can be used to indicate data classification levels as well as a summary of associated security and access control levels.

Data Labels with Security + Access Levels

Data Classification	Data Label	Security Level	Access, Storage, and Sharing
Confidential	RED DATA	**Level 1- "High Impact"** Systems that transmit, store, or manage this data require substantial security controls and measures.	**Highly Restricted** Access is tightly restricted to only those with need to know and frequently reviewed. Sharing and storage solutions are limited to high security systems only.
Sensitive	AMBER DATA	**Level 2- "Medium Impact"** Systems that transmit, store, or manage this data may require additional security controls and measures.	**Restricted** Access is tightly restricted and frequently reviewed. Sharing and storage solutions are limited to high security systems only.
Internal	GREEN DATA	**Level 2- "Medium Impact"** Systems that transmit, store, or manage this data must meet relevant University minimum security requirements.	**Standard** Access to this data is most often limited to employees. Many systems can be used to store/share data.
Public	WHITE DATA	**Level 3 - "Low Impact"** Systems that transmit, store, or manage this data must meet baseline requirements.	**Unrestricted** Access to this data is most often unrestricted and can be accessed by anyone.