Data Handling Procedures Related to the *Data Security and Stewardship Policy*

The requirement to follow these procedures is specified in University Policy 97, *Data Security and Stewardship*. Data at WCU is categorized in one of the five *Data Sensitivity Levels*. These procedures specify how each level of data is to be transported and stored within three security zones.

These procedures do not define what is or is not public information. The classification of data is the responsibility of the Data Steward or their designee, who should answer questions about the sensitivity level and the handling of their data.

The *Computer Security Incident Management Policy* (IT 16.1a) requires that as soon as anyone becomes aware that a compromise or disclosure of sensitive data might have occurred they must immediately notify the Office of the Chief Information Officer (CIO) and their available department manager. The CIO will assess the situation and if appropriate will call a meeting of the Computer Security Incident Response Team (CSIRT).

Data Sensitivity Levels

Sensitivity Level	Examples	Scope	Protection
Low (Green)	Publicly available data – calendar of events or schedules, sports rosters, public articles, phone directories	Intended to be shared with the general public by the official university data owners.	Does not need to be protected. End-users may share this information, but may not publish another version of it.
Guarded (Blue)	Not sensitive – internal policies or procedures, org charts, first name, last name, Email address	Access is generally limited to those whose job requires them to have access, but is not as restrictive as the higher sensitivity levels.	Should be protected from unauthorized access.
Elevated (Yellow)	Personal information, personnel data, certain intellectual property, and education records as defined by FERPA, Banner 92#	Can be accessed by authorized university personnel. This authorization must be granted and documented by the appropriate Data Steward or his/her designee or the appropriate compliance officer. For guidelines and best practices refer to the document Storing PII and FERPA Education Records	Must be protected from unauthorized access. Education records as defined by FERPA, including FERPA directory information, cannot be shared or published outside of the university by end-users[1].
High (Orange)	PII combination data records (see Appendix B). Where the combination of collected personal information, including medical and financial data, is enough that identity theft would be possible.	Can be accessed only by authorized university personnel. This authorization must be granted and documented by the appropriate Data Steward or his/her designee or the appropriate compliance officer.	Must be protected and possibly encrypted[2]; access must be re-certified; security controls must be audited periodically.
Severe (Red)	SSN, credit card info, bank account info, driver's license #, passport #, health insurance account #, export controlled data, other data when designated by agreement or the University	Can be accessed only by authorized university personnel. This authorization must be granted and documented by the appropriate Data Steward or his/her designee or the appropriate compliance officer.	Can't be placed in unmanaged or unsecured storage. Must be protected and possibly encrypted[2]; access must be re-certified; security controls must be audited periodically.

Data Handling by Security Zone - Storage

Security Zone	Definition	Requirements	Allowed Storage/Application Examples
Low	End-users have document-level access to unmanaged or unsecured storage.	• GREEN and BLUE data is allowed. • YELLOW, ORANGE and RED data are NOT allowed. • Exception: Instructors may store student data (YELLOW) for necessary course-related work on a PC local hard drive or removable storage, however it must be encrypted and removed after one year.	For GREEN and BLUE data: Non-WCU Email, Non-IT managed departmental servers, personally owned computer or mobile device NOT managed by the WCU mobile device policy, removable storage, file collaboration services NOT managed by WCU (e.g. Dropbox, Google Docs)
Medium	End-users have document-level access to IT-managed file storage.	• Storage hosted in the WCU Data Center or managed cloud hosted secure data center; appropriate contract and security for cloud hosted storage; storage cannot be in the DMZ; service must be approved by data steward. • Access must be re-certified and security controls must be audited periodically for RED and ORANGE data. • Encryption IS required for RED and ORANGE data at rest.	WCU Email (including student Email), WCU-issued personal computer, mobile devices managed by the WCU mobile device policy, WCU Intranet, Mercury file share, IT-managed departmental servers or applications, Blackboard, OnBase, file collaboration services managed by WCU (Microsoft OneDrive for Business)
High	Access to data managed by application, or by an owned AD security group.	• Application hosted in the WCU Data Center or managed cloud hosted secure data center; appropriate contract and security for cloud hosted application; activity logs; right to audit clauses; right to third-party audit results. • Access must be re-certified and security controls must be audited periodically for RED and ORANGE data. • Encryption NOT required for data at rest.	Banner (ERP), Medicat (Medical Records), CataMart (eProcurement), SecureShare folders, Bounty2 folders

Storage Encryption Table: This table summarizes the encryption requirements for data storage.

	Storage Zone		
Data Sensitivity	Low	Med	High
Green	Y	Y	Y
Blue	Y	Y	Y
Yellow	N	Y	Y
Orange	N	E	Y
Red	N	E	Y

Y=Allowed without encryption
E=Allowed with encryption
N=Not Allowed

Data Handling by Sensitivity - Transport

Sensitivity Level	Requirements	General Constraints	Email Constraints
Green	May be transmitted via unsecured channels	No constraints.	No constraints.
Blue **Yellow**	May be transmitted via unsecured channels	User must take precautions to protect the data while in transit; including physically securing removable storage and mobile devices, not viewing sensitive data over public wireless networks and locking your screen when it is unattended.	Be careful about recipients.
Orange	Only transmitted through secure (encrypted) channels	• Cannot be sent off campus to non-secure email addresses such as Gmail or transmitted to unsecure file sharing sites. • Should only be accessed off campus through a VPN account, a WCU virtual desktop, via a secure FTP server (SFTP) or secure web site (HTTPS). • The Data Steward should approve the transfer of data and method of transport to a third-party.	Should only be sent via WCU Email and the body and attachments are encrypted.
Red	Only transmitted through secure (encrypted) channels	• Cannot be sent off campus to non-secure Email addresses such as Gmail or transmitted to unsecure file sharing sites. • Should only be accessed by a user off campus through a secure channel via a WCU managed device[3]. • The Data Steward should approve the transfer of data and method of transport to a third-party.	Should never be sent via Email (even using internal WCU Email system unless so approved by University Counsel and encrypted).

Notes:

1) Any release of education records as defined by FERPA without the consent of the appropriate University official may result in adverse employment action up to and including termination of employment. Directory Information as defined by FERPA may be published by the University.
2) If the data must "possibly be encrypted" refer to the storage encryption table. For help with encryption methods and tools please contact the IT Help Desk.
3) RED data cannot be transported to end-user devices or systems that are not owned or managed by WCU. WCU virtual desktops that are specifically secured to have access to RED and ORANGE data are considered a WCU managed device.

Guiding Principles for Handling Sensitive Data:

1) For all categories except *GREEN* the user must take precautions to keep the data from unauthorized access. Best practice for sensitive data is to always choose a more secure storage zone and use encryption if possible.
2) A combination of data elements could elevate the sensitivity of all the elements. For example, a social security number alone is not sensitive until it is combined with a name or other personally identifiable information (PII). See Appendix B for more detail about PII combination data records.
3) Sensitive elements of a data record may be removed or redacted allowing that record to be transmitted or stored in a less secure way.
4) The cost of a data breach is often based on the number of records exposed. Large numbers of records containing sensitive data should not be stored in the *Low Security Zone* or transmitted through an unsecured channel.
5) Extracting data from a system in the High Security Zone for reporting purposes means it is now being used in a lower security zone. The procedures and requirements for handling in that lower security zone must be followed.
6) Any *YELLOW, ORANGE or RED* electronic or print data must be shipped by a tracked carrier with a recipient signature required. For encrypted data, the encryption key should only be released after the package has arrived and been signed for.

Glossary of Terms:

- **Cloud Hosted** - An application or data storage service that is not located on campus and is not operated by WCU IT. Some of these are adopted by an end-user (consumer-level) and others are have been adopted by WCU which has a service contract with the provider (enterprise-level).
- **Compromise or Disclosure of Sensitive Data** –The release of information, accidental or otherwise, to individuals or organizations that should not have access to the information whether they intend to use it maliciously or not.
- **DMZ or Demilitarized Zone** - A networking configuration that separates the internal systems from the more publicly accessible ones with an internal firewall, thus the internal systems have an extra layer of defense.
- **Data Center** – A computer facility that generally includes the necessary physical security and environmental controls to properly protect sensitive data. It also includes other technical layers of defense such as additional firewalls.
- **Data Steward** - The Chancellor, Provost, Vice Chancellors, General Counsel, and the Director of Athletics are responsible for ensuring the appropriate handling of the enterprise-level data produced and managed by their division/unit. These positions are the institutional Data Stewards.
- **Data Encryption** - Encryption refers to mathematical calculations and algorithmic schemes that transform plaintext into cyphertext, a form that is non-readable to unauthorized parties. Data can be encrypted where it is stored (at rest) or encrypted on the network (in transit)
- **FERPA/Directory Information** - Family Educational Rights and Privacy Act, a Federal law that protects the privacy of student education records. Directory information is generally not considered harmful or an invasion of privacy if disclosed. WCU has identified what it considers directory information here: WCU Directory Information
- **HIPAA** – Health Insurance Portability and Accountability Act, a Federal law which among other things regulates the use and disclosure of Protected Health Information (PHI). Refer to University Policy 123 for more information.
- **Managed vs Unmanaged Storage** – Managed storage can either be on-campus or off-campus. What makes it managed is the extra security mechanisms that are in place to protect the data. These mechanisms range from better user access controls to protecting systems to contractual agreements about data protection.
- **PII** – Personally Identifiable Information
- **Shared vs Published Data** – Data distributed to a limited audience for a limited use is considered sharing. An example is sending a schedule in an Email message. On the other hand, making data widely available, such as on a public web page, so that it may appear to be another official version of the data is considered publishing.
- **VPN** – Virtual private network, a way to extend the campus network to off-campus devices through an encrypted network connection.

Appendix A – Data Access Requirements and Device Definitions

This table defines the controls required for an application based on the sensitivity (color) of the data being accessed.

Blue/Green Data Requirements

- Web application doesn't need to be behind the Web Application Firewall (WAF)
- Two-Factor Authentication (2FA) not required
- Does not require an encrypted network connection
- May be accessed from any device
- Data at rest does not have to be encrypted
- May use a non-WCU account to access

Yellow Data Requirements – same as Blue/Green except:

- Web application must be behind the WAF
- Must be accessed from at least a **Registered** device
- Data at rest not allowed in the Low Security Zone
- Application must authenticate using a WCU-issued account and utilize WCU authentication services

Orange Data Requirements – same as Yellow except:

- Must use 2FA except for Domain device + on-campus
- Must be an encrypted network connection (HTTPS, VMview, VPN)
- Data at rest must be encrypted if not stored in the High Security Zone

Red Data Requirements – same as Orange except:

- Must be accessed from at least a **Managed** device

***Note:** Access to records that are your own personal information do not raise the data sensitivity level of an application. For example, only being able to access your own Red data in myWCU does not make the requirements for that application Red.

Device Definitions:

The controls listed here define the requirements for each level of device trust to be used in conjunction with the data access requirements listed above.

- **Trusted device – highest level**
  - Has enforced policies that the user cannot change; management agent/Registered Device
  - Operating System(OS) & application patching automated
  - Remote wipe
  - Endpoint Protection
  - Encryption Policies
  - No Admin Privilege on OS
  - OS & Application Authentication using WCU account
  - Data Loss Prevention: Implement DLP software and limit use of removable storage via policy
- **Managed device** – Any WCU or personally-owned device that is either using ActiveSync (or equivalent) or is a Domain device (managed-BYOD) – Volunteered or Agreed to Terms of Service for personal devices; required for WCU owned.
  - Adheres to Mobile Device Sync Policy
  - Remote wipe
  - Passcode usage required and managed
  - Enable built in encryption or use of encrypted folders
  - Enrolled in ActiveSync (or equivalent) or is a Domain device with security policies set
- **Registered device** – Devices that are known/registered
  - Device has a specific person and contact information recorded in WCU's registration system
  - Maximum registration period of one year for personally owned devices
- **Non-trusted device** – Any device that is not managed or registered

Appendix B – PII Combination Data Records

A combination of data elements could elevate the sensitivity of all the elements. For example, a social security number alone is not sensitive until it is combined with a name or other personally identifiable information (PII). Table 1 below is based on information published by The Department of Homeland Security about PII sensitivity. Utilizing tables 1 and 2 you can see that some combinations of PII data elements can increase the sensitivity of data.

Table1:

Types and Examples of PII				
Data Element	Non-sensitive PII	Sensitive PII	Paired PII	FERPA Directory
92#	x			
Name	x			x
Email	x			x
Phone #	x			x
Address	x			x
SSN		x		
Last 4 SSN			x	
DOB			x	
Citizenship or immigration status			x	
Driver's license		x		
Passport #		x		
Financial Acct #s		x		
Account passwords			x	
Medical information			x	
Criminal history			x	
Mother's maiden name			x	
Sexual Orientation			x	
Student Activities	x			

Table 2:

Data Element Combinations (examples)				
Name PII	1 or more Non-sensitive PII element	1 Sensitive PII element	1 Paired PII element	Data Sensitivity Color
• Name	• Email, • phone# • home address			Yellow
• Name			• DOB	Yellow
• Name	• Email		• DOB	Orange
• Name		• SSN		Red
	• Email	• SSN		Red

Interpretation of Table 2

- A record containing {any Non-sensitive PII} + {any Sensitive PII} = Red
- A record containing {Name PII} + {any Paired PII} + {any other element of Non-Sensitive or Paired PII} = Orange
- For example, it takes more than name and DOB to raise the data sensitivity color.

Effect on Data Handling

If the combination of data elevates the sensitivity of a file or record to Orange:

1) Data may still be stored unencrypted on WCU enterprise storage (Mercury, SharePoint and OneDrive);
2) Data transmitted to another application or system must be done via a secure (encrypted) channel;
3) Access to the application or system must be re-certified annually.

If the combination of data elevates the sensitivity of a file or record to Red:

1) Data must be stored as an encrypted file anywhere in the Medium Security Zone (see the *Data Handling by Security Zone – Storage* table in this procedure document for detail);
2) Data transmitted to another application or system must be done via a secure (encrypted) channel;
3) Access to the application or system must be re-certified annually.

FERPA Data

All student data collected and stored by WCU is protected by FERPA and designated as Yellow. This includes directory information. Directory information is also considered PII data. Directory Information may be released but its release is controlled. Employees should not release directory information unless they are explicitly authorized to do so. Any release beyond the look-up tool on WCU's website should go through WCU Legal Counsel.

FERPA-Specific Examples:

Name	+	DOB	=	Yellow				
Name	+	Email	+	Student Activities	=	Yellow		
Name	+	Student Activities	+	DOB	=	Orange		
Name	+	Home Address	+	Last 4 SSN	=	Orange		
Name	+	Citizenship	+	DOB	=	Orange		
Name	+	Email	+	DOB	+	Last 4 SSN	=	Orange
Name	+	SSN	=	Red				
Email	+	Driver's License	=	Red				