

Sensitive Data Protection Policy

Western Kentucky University

04/8/2008

1.0 Policy Constituents.

This policy applies to all University employees, academic and administrative units, foundations, vendors, contractors, third-party systems vendors and integrators, and agencies which handle or process WKU data for any reason. Individuals/organizations covered above are responsible for reading, understanding and abiding by this policy and are collectively referred to henceforth as “**policy constituents**”.

2.0 Purpose:

The purpose of this policy is as follows: 1. To make policy constituents aware of their responsibility regarding the “handling” (collection, storage, transmission, processing, transport, and/or disposal) of all university data but in particular “sensitive data”. 2. To provide guidelines and acceptable practices for handling sensitive data. 3. To identify unacceptable practices and emphasize that they be discontinued immediately.

3.0 What are Sensitive Data?

Sensitive data are any data that can be used for unintended purposes depending on the situation and circumstances. Data related to identity theft such as SSN, credit card number, bank account information, driver’s license, WKUID, other unique IDs, name, address, passwords, PINS, and ID pictures are of particular concern as all or most of this information is collected in the course of university business. Other types of data such as donor information, mailing lists, scholarship information, financial information, and bidding information are examples of data that could require confidential handling or restricted access. These examples are not exhaustive or all inclusive. Policy constituents handling any university data must understand what data are sensitive and confidential.

4.0 Data Handling Guidelines:

1. Do not collect and/or store SSN unless it is required by a federal or state agency and there is no other option in terms of unique identifier. If collection and storage of SSN are required for operations in a given unit, register this by sending an email to DataSecurity@wku.edu explaining why SSN must be utilized and how and where it is being collected/stored.
2. Use the WKUID assigned to all individuals as the unique identifier for all WKU entities. If WKUID is not available or does not exist for certain populations, use a non-SSN type of ID.
3. Data should be stored in as few places as possible and duplicated only when necessary. Unless absolutely necessary, data should be stored on central administrative systems only.
4. Avoid storing data on departmental servers or creating “Silo” databases that duplicate data on central administrative systems.
5. Inventory and identify the data under your control that is external to central administrative systems. Know where you have data and in what form (electronic, paper, etc.). Purge or delete data files in a timely manner. That is, keep data you control “cleaned up”. Data on old machines, network drives floppy disk, backup tapes, etc. should be inventoried and purged/archived or moved to more secure locations.

6. Do not store on or copy sensitive data to mobile, external storage devices such as CD, DVD, floppy disks, laptops, USB memory keys, PDAs, cell phones, or any other device that can easily be stolen or compromised.
7. Do not store on or copy sensitive data to local workstations or network drives unless such data is not available on centralized systems. If you must store data on workstations or network drives, it is your responsibility to secure your workstation and/or ensure that only authorized individuals have access.
8. Do not use shared network drives to share or exchange data internally or externally unless you are certain that access to those shared drive resources is restricted to individuals authorized to handle such data. Example: Do not put anything sensitive or confidential on what is currently the Novell F:/Shared drive. Potentially, everyone with a Novell account can access it.
9. Know and understand your environment technically. Understand who has access to areas you send, receive, store, or transmit data. Attend any WKU Sensitive Data Protection course offerings.
10. Transmission of any sensitive data should be encrypted. Websites should use HTTPS or SSL encryption if they collect data. FTP/Telnet or any other means of transferring files and data should use encrypted versions of these protocols: Example SSH and SFTP. When in doubt, contact the IT Help Desk.
11. Release of WKU Data to 3rd Parties: Do not release WKU data of any kind to 3rd party, non-WKU entities, for any reason, unless such entities have agreed in writing to restrict the use of such data to the specific and intended purposes authorized by the WKU department or unit enlisting the services of the 3rd party entity. Any WKU department or unit releasing data to a non-WKU 3rd party entity is responsible for how the data are used (misused). Release of highly sensitive and confidential data (beyond FERPA allowed “directory information”) is prohibited.
12. Do not send, receive, or store any sensitive data using email under any circumstances. Email is not secure.
13. Under no circumstances should credit card numbers be collected and stored on standalone devices, digital media, or paper media. Processing credit card numbers should be done via secure methods which authorize or deny the transaction in real time but DO NOT retain or store the credit card number. Collecting credit card numbers via phone calls, websites or email and retaining such numbers on paper or in electronic files for some sort of periodic processing is bad practice, insecure and should be discontinued immediately. If you need help processing credit cards securely, contact the IT Help Desk.
14. Report any breaches, compromises, or unauthorized/unexplained access of sensitive data immediately to the IT security officer by emailing DataSecurity@wku.edu or calling the IT Help Desk @745-7000.

5.0 Policy Adherence:

Abuses or violations of this policy will be referred to the appropriate authority for consideration under the University’s various disciplinary processes. The University reserves the right to take any action,

up to and including suspension/dismissal for a WKU (student) and discipline/termination for a WKU employee.

All employees of the University will be responsible for reading and understanding this policy and must certify that they have read it and understand it.

Approved by Administrative Council: 8/13/2007
Modified 4/9/2008 to add 4.0, 11.