WESTERN ILLINOIS UNIVERSITY

Data and Computer Security Policies, Procedures and Guidelines

Office of the CTSO
and the Technology Security Committee

Created: 7/30/2008
Last Updated: 7/20/2011

The policies, procedures, and guidelines in this document provide guidance to the university community related to the proper protection and usage of university computing resources as well as data under university care.

Contents

Data and Computer Security Policies, Procedures & Guidelines

It is the policy of Western Illinois University to maintain network, systems, applications and processes in compliance with federal, state and industry regulations and guidance including FERPA, HIPAA and PCI. Furthermore, it is the policy of WIU to protect the privacy of data under our care and in accordance with the FCC's Red Flag Rules and the state of Illinois's Identity Protection Act. The office of the CTSO will maintain these policies, guidelines and procedures including coordinating an annual review.

Scope

This policy applies to:

1. All faculty, students, employees, student employees, contractors, consultants, vendors, agents, and those affiliated with third parties that access WIU computer resources or data; and
2. All computers, data communication, telecommunication equipment, data centers, wiring closets, labs owned or administered by WIU.

Terminology

- AD- Active Directory (AD) is an implementation of LDAP directory services by Microsoft for use primarily in Windows environments
- Algorithm- Procedure for solving a problem
- Asymmetric Crypto-system – Also known as public key cryptography involving a public and private key pair. You give your public key to anyone you want to share information with securely. You use your private key to encrypt the data and they use your public key can decrypt the data.
- Audit- A formal examination of an organization or individual's accounts or financial situations
- BC- Business Continuity involves keeping core functions of a business running
- Blowfish- a symmetric block cipher that takes a variable length key, from 32 to 448 bits, making it good for both domestic and exportable use
- Block Cipher- symmetric key cipher which operates on fixed-length group of bits, "blocks," with and unvarying transformation
- CIO- Chief Information Officer
- Cut-and-paste or Copy-and-paste - Copying data from one document or computer screen and inserting it in to a different document
- CTSO- Chief Technology Security Officer is a WIU specific title for its Chief Information Security Officer
- Customer – Anyone that the university provides services to online
- Data Owner – The department having primary responsibility for the creation and maintenance of data. The data owner is responsible for determining how the data may be used within existing policies, and authorizing who may access data.
- Degaussing- To erase information from
- DES- Data Encryption Standard developed by IBM
- DMZ-Demilitarized Zone; Firewall configuration for securing local area networks
- DNS- Domain Name System; serves as a "phonebook" for the internet

- DOD- Department of Defense
- DR- Disaster Recovery
- EAP- Extensible Authentication Protocol is an authentication framework frequently used in wireless networks and Point-to-Point connections
- EAP-MD5- is an EAP security algorithm that uses a 128-bit generated number string, or hash, to verify the authenticity of a data communication.
- EAP-RADIUS- Passing of EAP message of *any* EAP type by authenticator to a RADIUS server for authentication. For example, an EAP message sent between the remote access client and remote access server are condensed and formatted as RADIUS messages between the remote access server and the RADIUS server
- EAP-TLS- Secures wireless LANs through RADIUS server
- Enumerates- to determine the number of
- FERPA- Family Educational Rights and Privacy Act
- FTP- File Transfer Protocol
- IDEA- International Data Encryption Algorithm is a block cipher designed by Xuejia Lai and James Massey of ETH Zurich as a replacement for the Data Encryption Standard
- Intermittently- Stopping or ceasing for a time
- Intranet- A private network that is contained within and enterprise. It may consist with many inter-linked local area networks and also use leased lines in the wide area network.
- IP- Internet Protocol
- IPSec- Internal Protocol security
- ISP- Internet Service Provider
- LAN- Local Area Network
- LDAP-Lightweight directory Access Protocol
- LINUX- UNIX like computer operating system family. Service of free software and open source development

- Lockdown – A method or best practice used to protect systems that restrict the functionality of a system to its core functions thereby reducing the ways a system can be attacked.
- Mainframe - Large and powerful computer capable of supporting hundreds, or even thousands, of users simultaneously
- MS-CHAP version 2- The Microsoft version of Challenge Handshake Authentication Protocol.
- Multi-Factor Authentication – Using two or more dissimilar authentication systems simultaneously. That is something you know (password or passphrase), something you have (token or certificate) or something you are (fingerprint, iris scan). Access to increasingly sensitive systems or data is protected by the use of additional authentication factors and other controls. Multi-factor authentication does not include multiple iterations of the same factor. Using two distinct passwords does not constitute two factors but is instead a single factor (something you know) being used twice.
- NT Admin-A system administrator of Microsoft Windows NT, 2000, 2003, 2007 systems
- Obfuscation- A form of masking data. Making large portions of it unreadable
- Parameters- quantity that defines certain characteristics of a systems of functions
- PCI DSS- Payment Card Industry (PCI) Data Security Standard (DSS) is a set of security standards developed by Visa, MC, etc. to secure credit card transactions
- PDA- Personal Digital Assistant
- Personally Identifiable – Data (such as name, name of parent or other family member social security number, address, phone number, email address, transcripts, birth date) that uniquely identifies an individual.
- Piggy Backing – A way of bypassing security measures by commandeering an authenticated connection to the WIU network.
- POP3-Post Office Protocol; Revives e-mail from a remote server
- Port- An interface on a computer to which you can connect a device
- Proprietary Encryption Algorithms- One person's converting a plaintext message into a cipher ext message which can be decoded back into the original message.
- RACF- Resource Access Control Family; security system that provides access control and auditing functionality for z/OS and z/VM operating systems

- RADIUS- Remote Authentication Dial in User Services
- RC5- Block cipher noticeable for its simplicity; "Rivest Cipher"
- Remote User – A user external to the WIU (Macomb or Quad Cities) network.
- Rootkit- A program that fraudulently gains or maintains administrator level access that may also execute in a manner that prevents detection
- SA- System Administrator
- Session - Period that begins when a user authentication is successful and ends when the user logs off of the system.
- RSA- Name that honors 3 mathematicians, Ron Rivest, Adi Shamir, and Len Adleman who gave a concrete example of how a public key system could be implemented.
- Sensitive Data – Data that when combined with personally identifiable information presents a compliance, state notification law, reputational, financial or consumer fraud risk to the University or is constituents. The following chart (https://www.wiu.edu/users/univtech/techSecure/SensitiveDataChart.pdf) provides guidance on the types of data characterized as sensitive.
- Server - A computer designed to process requests and deliver services and data to other computers over a network.
- SLA-Service Level Agreement
- SMTP-Simple Mail Transfer protocol; de-facto standard for e-mail transmissions
- SNMP- Simple Network Management Protocol
- Split-tunneling – The ability to access local network resources (and local Internet connectivity) while simultaneously being connected to WIU via Virtual Private Network (VPN)
- SSID-Services Set Identifier used in designating wireless networks
- SSL-Secure Sockets Layer
- SSH- Secure shell. A program that allows a user to log into another computer remotely across the Internet, while maintaining security
- Symmetric Cryptosystem- and easy method of scrambling data involving a single key that both parties must know (also known as a shared secret)

- TLS- Transport Layer Security
- UNIX- Computer operating system
- VNC-Virtual Network Computing
- VPN- Virtual Private Network- a secure extension of the WIU network via the internet to such places as home offices, hotel rooms, conference centers, etc.
- WIUP- University mainframe application

1. Appropriate Use Policy

Keep in mind that all users of university computing resources must: Comply with all federal, state and other applicable laws; all generally applicable Board of Higher Education and university rules and policies; and all applicable contracts and licenses. Users are responsible for ascertaining, understanding, and complying with the laws, rules, policies, contracts, and licenses applicable to their particular uses.

The following is a partial list of the state and federal laws governing all users of the WIU's computing resources.

- Obscenity and Pornography
    - Accessing, Viewing, or Downloading Child Pornography 18 USC § 2252
    - Forfeiture of computer for committing above 18 USC § 2510 et seq.
    - Illinois Compiled Statutes 720 ILCS 5/11-20.1
- Restriction of access by minors to materials commercially distributed by means of World Wide Web that are harmful to minors 47 USC § 231
- Data Management and Protection
    - Identity Protection Act 5 ILCS 179
    - Children's Online Privacy Protection Act (COPPA)
    - FTC Identity Theft Red Flag Rules
    - Payment Card Industry Data Security Standards (PCI DSS)
    - Gramm-Leach-Bliley Act (GLBA) Title V
    - Family Educational Rights and Privacy Act (FERPA)
    - Health Insurance Portability and Accountability Act (HIPAA)
    - Fair Credit Reporting Act (FCRA)
- Transporting of Obscene Materials for Sale or Distribution 18 USC § 1465
- Intercepting Electronic Communications 18 USC § 2703 et seq
- Computer Fraud 18 USC § 1030
    - Illinois Compiled Statutes Computer Fraud 720 ILCS 5/16D-6
    - Illinois Compiled Statutes Computer Tampering (hacking, maliciously spreading viruses, etc.) 720 ILCS 5/16D-3
    - Illinois Compiled Statutes Illicit or Unauthorized Use of a Password 720 ILCS 5/16D-7
- Slander and Libel 47 USC § 230c1
    - Illinois Compiled Statutes Slander and Libel 740 ILCS 145/1
- Copyright 17 USC
    - Rights of Copyright Holders 17 USC § 106 to 121
    - Infringement of Copyright 17 USC § 501 to 513
    - Circumvention of Copyright Protection Systems 17 USC § 1201

Users of university computing systems or data are required to take appropriate measures, as defined in the Administrative Procedures under Appropriate Use Procedures, to protect university computing systems and data.

Appropriate Use Procedures

- Use only those computing resources that they are authorized to use and use them only in the manner and to the extent authorized.

  Individual positions must be analyzed to determine the potential vulnerabilities associated with work in those positions. The WIU Internal Auditing office, working in cooperation with the various electronic services administrators, has designated specific computer positions (both Civil Service and Administrative/Professional) as requiring background checks prior to employment, due to the sensitive and/or extensive access personnel in these positions have to our computerized information systems. It may also be appropriate for certain divisions to designate locations as sensitive and to require appropriate procedures and safeguards for all employees whose duties include access to those areas (e.g. the Morgan Data Center).

  Upon termination of a person who occupies a position of special trust or responsibility, or is working in a sensitive area, management shall immediately revoke all access authorizations to computing resources.
- Users must not make unauthorized attempts to circumvent the security mechanisms of any university system.
- Users must not attempt to degrade system performance or capability, or attempt to damage systems, software or intellectual property of others.
- Users must avoid unauthorized viewing or use of another person's computer files, programs, accounts, and data.
- All new employees and student workers must have computer security awareness training. The University shall also provide an ongoing awareness and training program in information security and in the protection of computer resources for all personnel whose duties bring them into contact with critical or sensitive university computer resources or data. Including but not limited to training related to ethics, FERPA, HIPAA, GLBA, PCI, Red Flag and the Identity Protection Act.
- Users and areas must comply with all administrative the University Technology section of the Administrative Procedures Handbook.
- With the intent of returning you a functional and safe computer as quickly as possible, the university reserves the right to wipe and reinstall university owned or operated computers back to a standard university image. By default data will not be retained. Retaining data will require a signed data transfer form.
- Honor copyright restrictions on electronic material

2. Data Security Policy

The university and all members of the university community are obligated to respect and to protect university data. There are, however, technical and legal limitations on our ability to protect confidentiality. For legal purposes, electronic communications are no different than paper documents. Electronic communications are, however, more likely to leave a trail of inadvertent copies and more likely to be seen in the course of routine maintenance of computer systems. The

university does not regularly monitor the content of personal web pages, e-mail or other on-line communications. However, the university must reserve the right to examine computer records or monitor activities of individual computer users (a) to protect the integrity or security of the computing resources or protect the university from liability, (b) to investigate unusual or excessive activity, (c) to investigate apparent violations of law or university policy, and (d) as otherwise required by law. In limited circumstances, the university may be legally compelled to disclose information relating to business or personal use of the computer network to governmental authorities or, in the context of litigation or a served subpoena.

All university areas accepting, working with, or transmitting sensitive data (defined in the Sensitive Data Chart, Adobe PDF, login required) are required to take appropriate measures, as defined in the Administrative Procedures under Sensitive Data Handling Procedures, to protect sensitive data under their care.

Sensitive Data Handling Procedures

University policy requires that controls be in place to manage risk to the confidentiality, integrity and availability of sensitive data in any form and represent a minimum standard for protection of this data. Additional controls required under applicable laws, regulations, or standards governing specific forms of data (e.g., health information, credit cardholder data, student), may also apply.

Each individual who creates, uses, processes, stores, transfers, administers, and/or destroys sensitive university information is responsible and accountable for complying with these standards.

Areas are expected to follow guidelines as defined in the Administrative Procedures under University Data Management procedures when computers are transferred between individuals, when data is transferred between computers, when computers are disposed and when computers are located off campus for extended periods of time.

Security Classifications

Categories of university information based upon intended use and expected impact if disclosed. Data classifications are defined by data owners with two exceptions SSNs and credit card data that are explicitly defined and protected by policy.

- **Public**
  Information intended for public use that, when used as intended, would have little to no adverse effect on the operations, assets, or reputation of the university, or the university's obligations concerning information privacy. Information typically found on the Internet.
- **Internal**
  Information not intended for parties outside the university that, if disclosed, could have

adverse effect on the operations, assets, or reputation of the university, or the university's obligations concerning information privacy. Information typically found on an Intranet.

- **Sensitive**
  Information intended for limited use within the university that, if disclosed, could be expected to have a serious adverse effect on the operations, assets, or reputation of the university, or the university's obligations concerning information privacy.

Creation

University employees create records as part of the normal course of conducting the business of the university. These records document the decisions and activities of our complex educational and business enterprise. It is essential that they be created and maintained appropriately throughout their entire life cycle.

Sensitive information contained in university records constitutes an area of critical concern because of the severe risk to the university should records be mishandled or information inappropriately accessed or disclosed. As a consequence, records containing sensitive information should exist only in areas where there is a legitimate and justifiable business need.

Campus Units should work to identify and track all university records through their life cycle by way of records retention schedules (prepared in collaboration with administrative offices such as the Business Office and university Archives) as defined by state law. A first priority in this effort should be the identification of sensitive information. Records schedules will document the existence of these materials, the rationale behind keeping them, and help ensure their availability during the period in which they are vital as either active administrative or historical records. Record retention schedules also will work to ensure the timely disposal of non-permanent, inactive records, thereby mitigating the risk of exposure of information when it no longer serves an active administrative or historical function.

Access

Sensitive information requires strict control, very limited access and disclosure, and may be subject to legal restrictions. In some cases, information is sensitive because it has been aggregated into a single document.

Only university employees who have authorization from the data owner(s), and have a signed confidentiality agreement on file, may have access to sensitive information. Any other disclosure of sensitive information requires the written approval of the appropriate Officer of the university, in consultation with general counsel as necessary. Things to remember when working with sensitive data:

- As a general rule, employees are not allowed to take sensitive data off campus (or to make unofficial copies)
- Where access to sensitive data has been authorized, use of such data shall be limited to the purpose required to perform university business.
- Users will respect the confidentiality and privacy of individuals whose records they access, observe ethical restrictions that apply to the information they access, and abide by applicable laws and policies with respect to accessing, using, or disclosing information.
- Notification of a user's termination or removal of authorized access to sensitive information must be conveyed immediately to University Technology.

Use, Transmission and Disposal

The following controls are **required** when using, transmitting or disposing of sensitive information.

- Do not discuss or display it in an environment where it may be viewed or overheard by unauthorized individuals.
- Do not leave keys or access badges for rooms or file cabinets containing such information in areas accessible to unauthorized personnel.
- When printing, photocopying or faxing it, ensure that only authorized personnel will be able to see the output.
- Store paper documents in a locked drawer **and** in a locked room, or in another secure location approved by the Data Owner.
- Properly identify such information as sensitive to all recipients, by labeling it "Sensitive," providing training to personnel, explicitly mentioning the classification, or similar means.
- Encrypt electronic information using a generally available encryption algorithm such as that built-in to common office automation applications (such as newer versions of word, excel, PowerPoint, acrobat, winzip, etc.):
    - Placing it on removable media;
    - Placing it on a mobile computer (e.g., laptops, PDAs, smart phones); or
    - Sending it via e-mail to **non-wiu.edu addresses**.
- Do not send this information via email, instant message, chat or unsecured file transfer (such as FTP) unless it is encrypted.
- Follow an established and documented software development lifecycle when building applications that process sensitive information.

Transport

The following controls are **required** when transporting sensitive information:

- When sending such information by mail (including U.S. Postal Service, DHL, UPS, FedEx, etc.), the sender must obtain secure, certified, tracking and signature confirmation services and use a tamper-evident sealed package. It is highly recommended that obfuscation or encryption of the sensitive data items be done before hand.
- Do not send unencrypted sensitive information by campus mail or email.
- When carrying unencrypted sensitive information, or devices containing such information, ensure that it is physically secure at all times.

- Do not remove sensitive information from an approved secure location without prior approval of the data owner, appropriate VP area or legal counsel.
- As a general rule, employees are not allowed to remove sensitive data from the university.
- In the event that an individual employee or job responsibility requires sensitive information to be removed from the university, the information (whether electronic or paper) must be protected at all times from inappropriate disclosure. Each department that has individual employees or positions requiring sensitive data to be removed from the university must have appropriate procedures in place for protecting the data while outside the university and destroying the data when it is no longer required to perform the job.
- Tape media containing sensitive data should be encrypted using an approved encryption method before being sent offsite. Where feasible, alternatives to mail delivery must be utilized such as a secured, encrypted online transmission. These transmissions that utilize passwords to encrypt or decrypt data must have their own unique identifier or password.

Disposal of Records, Computers and Media

- Department managers are responsible for educating and training employees as to the purpose of this policy and how to dispose of information properly.
- University records should be destroyed in accordance with the **Credit Card Data Retention Policy** or departmental retention schedules.
- Destroy electronic instances of university information by physical destruction or by using a DOD approved wiping method. **Reformatting a hard drive is not sufficient to securely remove all data.**
- Shred (crosscut shredding recommended) or pulp all highly sensitive information in paper form. This includes all transitory work products (e.g., unused copies, drafts, notes).
- Ensure that obsolete computers and electronic media (anything that can store data such as CDs, DVD, thumb drives, diskettes, iPods, etc.) are disposed of properly to ensure that no data remains. This may entail physical destruction of the computer's hard drive (or electronic media) or may instead entail electronic measures such as erasing the hard drive via a DOD approved method. University Technology (uTech) has procedures and technologies in place to dispose properly of old university computers. Check with your college technology representative or university Technology (uTech) for details.

Social Security Number (SSN) Usage and Protection Policy

Western Illinois University collects and maintains social security numbers of employees, students, vendors, and others in the ordinary course of its business and as required by law. Recognizing the sensitive nature of this information the University will handle social security numbers with a high degree of security and confidentiality in accordance with legal standards defined in the Administrative Procedures under Social Security Number Usage and Protection Procedure.

Social Security Number Usage and Protection Procedure

In order to protect individual privacy and identity, Western Illinois University adheres to section 10 of the Identity Protection Act. Therefore, social security numbers must not be:

- Publicly posted or publicly displayed;
- Used as the primary account number or identifier for an individual, except where legally mandated or required;
- Visibly printed on identification cards or badges;
- Printed on materials that are mailed to individuals through the U.S. Postal Service, private mail services, electronic mail, or any similar method of delivery, unless State or federal law requires it;
- Required to access online University services;
- Encoded, embedded or printed using bar codes, chips, magnetic strip, RFID or other technologies;
- Used, transmitted, or stored on records or record systems that are not encrypted and secure. For example, certain communication channels such as email, wireless, IM, chat, P2P, FTP, telnet, bulletin boards, SMS messaging, Microsoft Word/Excel/Access and web 2.0 technologies (blogs, tweeter, Facebook, etc.) are not acceptable choices for the sending, receiving or storage of SSNs; and
- Used for any purpose other than the purpose for which it was authorized and collected.

Furthermore, the University will:

- Ensure, to the extent practicable, the confidentiality of social security numbers. Social security numbers are considered sensitive data elements and will be managed and protected accordingly;
- Not unlawfully disclose an individual's social security number;
- Strictly limit access to records and record systems containing social security numbers to those who have a business related reason to know this information. Requiring areas to assess, document and report to their VP area, annually or upon significant change, their business need for social security numbers. Annual assessment must include a statement of purpose or purposes for the collection and usage of social security numbers;
- Direct areas which request a SSN (verbally or on a form) to inform individuals of the following:

    - Whether the disclosure is mandatory or voluntary;
    - By what statutory or other authority the SSN is solicited;
    - What uses will be made of the SSN and by whom;
    - How long a SSN will be retained; and
    - How a SSN will be destroyed or protected

- Train users and areas to protect the confidentiality of social security numbers;
- Redact social security numbers from the information or documents before allowing the public inspection or copying of the information or document;
- Dispose of records containing social security numbers in a responsible manner that minimizes risk that the social security numbers can be accessed inappropriately; and
- Ensure that obsolete computers and electronic media (anything that can store SSNs such as tapes, CDs, DVD, thumb drives, diskettes, iPods, cell phones, smart phones, PDAs, printers, etc.) are disposed of properly.

Credit Card Handling Policy

The major credit card issuers created PCI (Payment Card Industry) compliance standards to protect personal information and ensure security when transactions are processed using a credit card. All members of the payment card industry (financial institutions, credit card companies and merchants) must comply with these standards if they want to accept credit cards.

All university areas accepting credit cards as payment (defined as merchants) for items or services are required to take appropriate measures, as defined in the Administrative Procedures under Credit Card Handling & Compliance Procedures, to comply with PCI DSS and to protect cardholder information.

Credit Card Handling & Compliance Procedures

The following procedures are intended to support the universities Payment Card Industry (PCI) Data Security Standard (DSS) compliance efforts and should be reviewed annually and updated as appropriate:

- An annual risk assessment of all areas (and corresponding vendors) taking credit cards as payment or supporting the credit card payment environment will be coordinated through the office of the Chief Technology Security Officer and the Business Office. Policies, procedures and training will be updated as appropriate.
- Vendors processing, transmitting or storing cardholder data on behalf of the university must provide annual evidence of their compliance with PCI DSS.
- Information security contract language must be added to all contracts that provide access to university systems, data, sensitive areas (such as data centers, wiring closets, etc.) or provide custom development on behalf of the university. The agreement should include an acknowledgement that the service provider is responsible for the security of cardholder data the provider possesses.
- Non-encrypted cardholder data may not be taken outside the university and may not be provided to non-approved outside entities (such as 3rd party vendors providing processing, analysis, etc.). University merchants can work with the business office to get a vendor approved. University approved vendors are: Paypal, Authorize.net, Global Payments and Illinois Funds E-PAY
- Areas wishing to purchase applications that process, transmit or store cardholder data must insist that the vendor provide evidence that the application has been assessed against PCI Payment Application Data Security Standards (PA-DSS) and that the vendor has provided a PA-DSS implementation guide (where configuration options are provided) that shows how the application needs to be configured to maintain or achieve compliance.
- Quarterly network scans conducted by a PCI Approved Scanning Vendor (ASV) are required.
- Performing an external penetration testing at least once a year and after any significant infrastructure or application upgrade or modification. Including both a Network-layer penetration test and an Application-layer penetration test.

- Ensure that web-facing applications are protected against known attacks by having custom application code reviewed for common vulnerabilities by an organization that specializes in application security or installing an application layer firewall in front of web-facing applications.
- The business office and office of the CTSO will provide annual training on the proper use of credit cards. All employees that work in areas that take credit cards as payment must signoff annually that they've received this training.

Credit Card Data Retention and Disposal Procedures

Payment Card Industry (PCI) Data Security Standard (DSS) requirement 3.1 requires that the university maintain and adhere to a data retention and disposal procedures. The purpose of this procedure is to ensure that records that are no longer needed are discarded appropriately and in a timely fashion. Each area that takes credit cards as payment must periodically (minimally annually) review these procedures to determine any circumstances that necessitate changes in the way they retain or dispose of cardholder data.

Lack of compliance may result in fines of $25,000 per merchant per month and may eventually result in the loss of merchant privileges.

Retention Periods:

The state of Illinois defines credit card records as receipts and defines the following retention guidelines.

Cardholder Data Transmission, Retention and Disposal	**State of Illinois Guidance**
Credit/Debit card data (Name, Authorization Code, Authorization Date)	3 years
Credit/Debit card data (Last 4 digits of account number)	3 years
Full credit card account number	3 years (encryption required prior to storage)
Credit/Debit card data (magnetic stripe track data, card validation code, PIN)	Never stored
Cardholder data over electronic mail, instant messaging, text messaging, chat, blogging and voice-mail	Encryption required prior to transmission
Cardholder data over a wireless network	May only be transmitted over secure wireless
Cardholder data over unsecure protocols (telnet, ftp, etc.)	Encryption required prior to transmission

Credit Card Data Disposal:

Cardholder data maintained on paper should be shredded as soon as business conditions allow but not more than the guidance provided by the state of Illinois. If cardholder data must be maintained on paper for any period of time caution must be taken to ensure control and protection of the document. Including:

- Minimizing who has access to the document;
- Ensuring that disallowed data (card validation code, PIN) is not present;
- Concealing all but the last four (4) digits of the cardholder account number; and
- Maintaining the paper document in a locked secure area with limited controlled access.

Cardholder data maintained electronically should be eliminated as soon as business conditions allow but not more than the guidance provided by the state of Illinois. If cardholder data must be maintained electronically for any period of time caution must be taken to ensure control and protection of the document. Electronic cardholder data presents additional challenges to data maintained on paper. So in addition to the items mentioned for cardholder data maintained on paper the following require consideration for cardholder data maintained electronically:

- If business conditions allow eliminate the electronic retention of cardholder data.
- If business conditions allow concealing or removing as much of the cardholder data as possible (for example, removing all but the last 4 digits of the cardholder account number).
- Encrypt or one-way hash cardholder data prior to storage.
- Do not make backup copies of unencrypted cardholder data*
- Cardholder data must not be transmitted via or stored on electronic mail, instant messaging, text messaging, blogging and voice-mail
- Cardholder data must not be transmitted via unsecure protocols (such as telnet, FTP, etc.)
- Cardholder data must not be transmitted over an unsecure wireless network
- Regardless if you think your old computer holds or does not hold cardholder data, ensure proper disposal of end of life computer equipment by adhering to WIU's computer disposal policy.

Policy on Foundation Records Confidentiality

The Western Illinois University Foundation recognizes its responsibility in maintaining the confidentiality of the records it manages, and will adhere to the following policy:

All data existing in or originating from the Western Illinois University Foundation shall be considered confidential and shall be used only for official University, Foundation and Alumni Association related activities. Under no circumstances should such data be used for commercial or political purposes.

Web Privacy Policy

Western Illinois University (WIU) is committed to ensuring the privacy and accuracy of confidential information; therefore, WIU does not share personal information gathered from its websites. WIU also complies with the Family Educational Rights and Privacy Act (FERPA), which prohibits the release of education records without student permission. Although FERPA regulations apply to students, the University is equally committed to protecting the privacy of all visitors to our websites. WIU will not sell, rent, or market personal data to third parties.

The University's web privacy notice shall not be construed as a contractual agreement. The University reserves the right to amend the information at any time without notice. Privacy and public records obligations of the University are governed by applicable Illinois statutes and U.S. federal laws. Because WIU is a public institution, some information collected, including the summary server log information, e-mails, and information collected from web-based forms, may be subject to the Freedom of Information Act (FOIA). While WIU does not actively share information, in some instances, the University may be required by law to release information gathered.

Scope

This privacy notice applies to all Western Illinois University websites containing "wiu.edu." This includes websites of academic and administrative units, as well as official and unofficial pages. Official pages are sanctioned by WIU while unofficial pages are those not sanctioned by WIU; including but not limited to staff, faculty, student organizations, and student personal pages. In addition, the websites of students, faculty, and staff should not request confidential information from visitors. Examples of confidential information include Social Security numbers, WIU identification numbers, credit card numbers, passwords, and birthdates.

Do not enter confidential information on a Western website unless the site uses encryption. One way to know whether a site uses encryption is if the web address begins with https (i.e. https://webapps.wiu.edu). In addition, the browser may display a locked padlock icon in the lower right corner.

Data Gathered

There are four primary types of information that may be collected during a visit to a WIU website: network traffic information, web server statistic logs, cookies, and information voluntarily provided.

Network Traffic

In the course of ensuring network security and consistent service for all users, the University may use software programs to:

- analyze network traffic,
- identify unauthorized access,
- detect computer viruses and other software that might damage University computers or networks, and
- monitor and maintain the performance of the University network.

In the course of such monitoring, these programs may detect such information as e-mail headers, addresses from network packets and other information. Information from these activities is used solely for the purpose of maintaining the security and performance of the University's networks and computer systems. Personally identifiable information from these activities is not released to external parties unless required by law.

Web Server Logs

University web servers collect and store information from website visitors to monitor performance and to improve service. This information includes:

- page visited,
- date and time of the visit,
- domain name or IP address of the referring site,
- domain name and IP address from which the access occurred,
- version of browser used and the capabilities of the browser,
- search terms entered into the WIU search engine, and
- ECOM (unique person identifier for ECOM-based services only)

The University makes no attempt to identify individual visitors from this information. Any personally identifiable information is not released to external parties unless required by law. The data is used in aggregate by University Technology (uTech) to further refine websites for efficiency and is not associated with specific individuals. Raw data from the web server logs is only shared with the owner of a website. Summary reports produced from the logs help content publishers determine what web browsers and pages are most popular. For example, if the aggregate reports show a particular web page is popular or used more by freshmen than by seniors, publishers might use this information to customize the content of the page.

Cookies

Cookies are data stored by a web browser, and are often used to remember information about preferences and pages visited. For example, when visiting a site, a user may see a "Welcome Back" message. The first time the site was visited, a cookie was most likely set on the computer. Web browsers can be reconfigured to refuse to accept cookies, to disable cookies, and to remove cookies from the hard drive as needed.

Some web servers within WIU may also use cookies to retain user preference information. It is against University policy to share this information with external third parties.

State Agency Website Act (Public Act 093-117)

University websites will not use permanent (persistent cookies) or any other invasive tracking programs that monitor and track University website viewing habits unless users opt-in to such tracking.

Information Voluntarily Provided (Optional Information)

In the course of using WIU websites, individuals may choose to provide information to help the University better serve the needs of the campus community. For example, users may send an e-mail (through a web form or mailto: link) to request information, register for events, or send an address for an application or other materials. Any personally identifiable information will be used only for the purpose indicated. The University does not retain the information longer than necessary or required by law.

E-Commerce

Several sites within WIU allow individuals to pay for products or services online with a credit card. These transactions are encrypted. It is University policy that confidential information entered in a transaction is used only for the purposes described in that transaction. Credit card information such as credit card numbers is not stored on WIU servers or personal computers.

Social Security Numbers (SSNs)

Any web page that requests Social Security Numbers will inform users of the following:

- whether the disclosure is mandatory or voluntary,
- by what statutory or other authority the SSN is requested,
- how it will be used,
- a list of third parties with whom the institution shares this data, and
- if appropriate, an explanation of your right to opt out of collection/sharing.

Family Educational Rights and Privacy Act (FERPA)

Consistent with FERPA, the University does not release personal student information, other than public directory information, to other parties unless the University receives explicit written authorization. Directory information includes: student's name; school and home addresses; WIU e-mail address; telephone numbers; major field of study; dates of attendance; full- or part-time status; classification; degrees, honors and awards received (including Dean's List) and date granted; anticipated graduation date; most recent previous educational agency or institution attended;

participation in recognized university activities and sports; and for members of athletic teams, weight and height.

Students can restrict the release of directory information by contacting the Office of the Registrar.

Children's Online Privacy Protection Act (COPPA)

Western Illinois University complies fully with the Children's Online Privacy Protection Act. Accordingly, if a user of the University web is under the age of 13, the user is not authorized to provide Western Illinois University with personally identifying information, and the University will not use any such information in its database or other data collection activities without obtaining explicit parental consent before collecting personal information from children.

Public Forums

WIU makes some public chat rooms, forums, message boards, and news groups available to its users. The University does not ordinarily log public chat sessions, however, any information that is disclosed in these areas becomes public information. Individuals should exercise caution when disclosing confidential information.

Online Surveys

At any time there may be numerous online surveys being conducted on the University's website. University policy states that confidential information gathered is used only for the purpose indicated in the survey. Unless otherwise noted on the specified survey, answers are confidential and individual responses will not be shared with other parties. Aggregate data from surveys may be shared with external third parties.

Providing Information

There is no legal requirement for an individual to provide any information at the WIU website. However, the University website will not work without routing information and essential technical information. Failure of a browser to provide nonessential technical information will not prevent the use of the WIU website, but may prevent certain features from working. For any optional information that is requested at the website, failure to provide the requested information will mean that the particular feature or service associated with that part of the web page may not be available.

Third-Party Content

While visiting a Western website, individuals may encounter links to web pages and sites which are not owned or controlled by WIU. Such websites do not contain a "wiu.edu" address. Be aware that these remote sites are not under the control of Western Illinois University and no warranty or claim

concerning these services is implied or should be assumed. Remote sites may have different policies regarding privacy (or no policies at all); therefore, users should avoid entering personal information into such remote sites. If there are doubts about entering personal information, contact Western Illinois University using the information provided below.

Security and Accuracy of Confidential Information

WIU does its best to ensure that the personal information it collects is accurate. Users with an ECOM ID can check and update personal information such as their mailing address and e-mail address at Student/Alumni Records System (STARS) and WIUP (for employees).

While no computer system is 100 percent secure, WIU has security measures in place to protect against the loss, misuse, or alteration of the information under its control. These security measures and the systems are audited by the State of Illinois. To report a security incident, e-mail abuse@wiu.edu.

Sharing of Information

WIU does, upon explicit request of users, share information with other parties and gather information from other private data providers. This is done only at the request of users (persons to whom the information applies). Unless specifically required under public information requests filed under FOIA, it is against University policy to release confidential information gathered through the web. However, when circumstances arise for the need to share information gathered from its University web servers, the University may share as:

- authorized or required by law,
- to assist law enforcement investigations, legal proceedings, or internal investigations of University rule and regulation violations.
- permitted under University and campus policies,
- required by an approved University contract,
- consent is explicitly given (opt-in),
- certain student and employee demographic information with Western Illinois University Alumni Association, the Western Illinois University Foundation, applicant students' high schools and other educational institutions with questions about students who have been admitted or earned a degree from the University.

Exceptions to Rule

The University web is comprised of numerous servers, and some servers may adopt different privacy notices as their specific needs require. If another University server has a privacy notice that differs from this notice, then that notice must be approved by the President's Cabinet, and it must be posted on the site. However, those sites cannot adopt a privacy notice that supersedes federal or state laws or regulations or University or campus policies.

Right to Correct Inaccuracies

Personal information that contains inaccuracies or that needs to be updated should be changed by contacting the appropriate office.

Questions

For questions about this privacy notice or if personal data has been compromised or improperly handled, contact the University Auditor at (309) 298-1664 or I-Auditing@wiu.edu or the Office of the Chief Technology Security Officer at (309) 298- 4500 or MA-Rodriguez@wiu.edu. For requests made under the Freedom of Information Act (FOIA) contact the University FOIA officer at (309) 298-1993 or DR-Shinberger@wiu.edu.

Encryption Policy

Proven, standard algorithms should be used as the basis for encryption technologies. The use of proprietary encryption algorithms is not allowed for any purpose. Symmetric cryptosystem key lengths must be at least 128 bits (256-bit is recommended). Asymmetric crypto-system keys must be of a length that yields equivalent strength. WIU's key length requirements will be reviewed annually and upgraded as technology allows.

Note: Be aware that the export of encryption technologies may be restricted by the U.S. government. Residents of countries other than the United States should make themselves aware of the encryption laws of the country in which they reside.

Note: Be aware that while travelling outside the U.S. you may be required to provide your encryption keys or password. Best practice states that you should never travel with sensitive data but if you must access sensitive data while travelling download it via VPN at your destination and delete the local copy before continuing your trip.

Additional encryption requirements for devices or media hosting sensitive data

Servers/Workstations/Laptops

Proper use of sensitive data begins by evaluating business processes for the need to take in or store sensitive data and if indeed it is needed ensure that appropriate protection (obfuscation, masking, one-way hash, encryption, etc.) is applied throughout the data lifecycle. Sensitive data must never exist on University computers unprotected.

It is recommended that University owned or managed computers storing sensitive data employ full disk encryption with an approved software or hardware encryption solution. Additionally, WIU

recommends the deployment of software to assist in the recovery or remote wiping of University computers.

PDAs, Cell phones and removable media

Any device or media with memory or that can be used to transport data (such as but not limited to tapes, CDs, DVDs, diskettes, thumb drives, memory sticks, PDAs, cell phones, printers, fax machines, MP3 devices, digital cameras, etc.) must never hold sensitive data or must be protected (obfuscation, masking, one-way hash, encryption, etc.) and must be properly disposed.

3. Computing System Protection Policies & Procedures

Access

No one may access records containing sensitive data unless specifically authorized to do so. Even authorized individuals may use sensitive data only for authorized purposes. The members of the university community are required to respect the privacy of others and their accounts. No one may access or intercept files or data of others without permission, nor may they use another's password or access files under false identity.

Technology assets are to be hosted in an appropriately secure physical location. Technology assets include servers, workstation computers, ports (active ports in public areas), modems and network components (cabling, electronics, etc.).

Passwords help protect against misuse by seeking to restrict use of university systems and networks to authorized users. Each authorized user is assigned a unique password that is to be protected by that individual and not shared with others, is difficult to crack, is changed on a regular basis, and is deleted when no longer authorized. See the university password policy for more details.

University Technology management will ensure that controls are in place to avoid unauthorized intrusion of systems and networks and to detect efforts at such intrusion.

Each university information system should have a system access policy that controls access rights and privileges and protects assets and data from loss or inappropriate disclosure by specifying acceptable use guidelines for users, operations staff and management. A systems access policy will provide guidelines for external connections, for data communications, for connecting devices to a network, and for adding new software to systems. As part of the policy, the responsibility and accountability for its implementation must be established.

The management for each area will also ensure that administrative access procedures include provisions for alternative administrative access in the event that the primary access holder is incapacitated or otherwise unable to perform required administrative activities.

Users of university network resources will be required to accept a notice such as the following prior to being granted access to WIU information assets.

> This system is to be used only by authorized personnel, and all others will be prosecuted. Activities on this system are automatically logged and subject to review. All data on this system is the property of Western Illinois University, which reserves the right to intercept, record, read or disclose it at the sole discretion of authorized personnel. Specifically, system administrators may disclose any information on or about this system to law enforcement or other appropriate individuals. Users should not expect privacy from system review for any data, whether business or personal, even if encrypted or password-protected. WIU abides by the Family Educational Rights Act of 1974, and takes precautions to prevent the disclosure of confidential information. Use of this system constitutes consent to these terms.

Accountability

Individual users are responsible for ensuring that others do not use their system privileges. In particular, users must take great care in protecting their usernames and passwords from eavesdropping or careless misplacement. Passwords are never to be 'loaned.' Individual users may be held responsible for any security violations associated with their usernames.

All controlled systems must maintain audit logs to track usage information to a level appropriate for that system. All user sessions and all failed connection attempts must be logged. Audit logging may also apply to networks. If inappropriate use of the network is suspected specific traffic logging of the network may occur. WIU respects your privacy but due to legal, regulatory or compliance reasons what you do on the university network may be logged and may be audited.

Downloading software, particularly software that is not job-related or endorsed by the university, may introduce security risks and should only be done after authorization by a Dean/Director in consultation with University Technology Directors.

Authentication

Authentication and data encryption must be implemented for all systems that send or receive sensitive data or when it is critical that both parties know with whom they are communicating.

Availability

Mission critical systems are expected to be available at all times during applicable business hours. Each critical system must have a published availability statement which details redundancy and recovery procedures, and specifies hours of operations and maintenance downtime periods. It must also include contact information for reporting system outages. This statement must be submitted to and approved by the Vice President of Quad Cities, Planning and Technology.

Backup of data must be well-documented and tested. Backups of mission critical data must be maintained in secure off-site storage to guard against the impact of disasters.

Perimeter Security Procedures

The University will have technologies in place that control access from outside the university appropriately including but not limited to the following:

- One or more perimeter routers that provide the first level of defense against inappropriate external access. It is recommended that these routers be redundant within the same location as well provide support for the graceful failover to another location such as a Disaster Recovery (DR) facility.
- One or more firewalls must provide stateful packet inspection that by default denies all requests on all ports. Additional recommended functionality includes but is not limited to support for NATing, RFC 1918 addressing, IPv6, deep packet inspection and layer seven intelligent (application aware) inspection.
- Provide firewalled and monitored (IPS/IDS) segments that minimally separate external, presentation, application, internal – business, internal – students (ResNet), mainframe and university data segments
    - These networks will be protected by a firewall that by default deny all requests on all ports.
    - Only required ports and services must be turned on.
    - Operating system software on these Internet computing assets must be hardened so that only required software, services, protocols, default accounts, and security features are enabled. By default, all software, services, protocols, and default accounts must be disabled.
    - All Internet generated requests must first be directed through a DMZ segment. No Internet generated traffic will ever be allowed to route directly into WIU trusted networks.
        - All requests routed into WIU trusted networks must be generated from the DMZ segment
        - No Web server will house User ids and/or passwords
        - No server accessible from the outside will store sensitive data
- Provide firewalled segments that separate production applications, pre-production applications and test/development applications. Thus allowing for segmentation of duties, proper testing and proper change control.
- Provide for proper monitoring and filtering (see Internet Security and Usage Policy)

Remote Access Guidelines

A remote user shall use either dial-in or virtual private networking (VPN). VPN uses a secure tunnel through the local ISP connection to the University network. VPN is recommended over modems for remote access.

General requirements:

- Vice President or higher approval is required to download sensitive data to remote computers. Furthermore, it is prohibited to download sensitive data such a credit card data to a remote computer or media. This also includes but is not limited to printing, faxing, cut-and-paste, etc.

- Users with administrative rights to servers, network/telecom infrastructure equipment or applications must use a University approved multi-factor authentication solutions (such as tokens, certificates) when connecting remotely.
- Connecting computers should be properly patched and running current antivirus and anti-malware.
- Remote access for vendors must only be allowed during a maintenance window and with proper and approved change control. It is highly recommended that there be WIU oversight of the session.

VPN Requirements

- All data transmitted must be encrypted.
- Split-tunneling or accessing the Internet through your local Internet Service Provider while connected to WIU is prohibited.

Wireless Policy

Wireless access points or devices with wireless capability are allowed in one of three fashions.

- Restricted non-secure wireless access to Internet (no university network access)
- Secure wireless access to the university network and the Internet
- A secure non SSID broadcasting wireless network will be supported for areas that take credit cards as payment and must have access to wireless.

The OPS isolated wireless LAN is a noted exemption to this policy.

Additional guidelines on wireless:

- Use the strongest supportable authentication available.
- Use the strongest supportable encryption available. WEP is not acceptable encryption.
- Must be installed, supported, and maintained by University Technology (uTech). Rogue Access Points (APs) and other wireless devices violate university policy.
- Maintain a hardware address (MAC address) that can be registered and tracked.
- Wireless clients that cannot support these security requirements will only be allowed limited access to the internet.
- Any area that takes credit cards as payment for products or services must ensure that wireless is not used within their area or must use a University Technology (uTech) supported secure wireless network that does not broadcast its SSID. Areas will be required to demonstrate a need for wireless networking.
- ResNet wireless will conform to university wireless options #1 and #2. Rogue Access Points (APs) are not allowed.

Intrusion Prevention Guidelines

- All university owned or operated systems accessible from the internet or by the public must operate university approved active intrusion detection software during anytime the public may be able to access the system.
- All systems in the DMZ must operate university approved active intrusion detection software.
- All host based and network based intrusion detection systems must be checked on a daily basis and their logs reviewed.
- All intrusion detection logs must be kept for a minimum or 30 days.

Physical Security Guidelines

This Policy establishes rules for the granting, control, monitoring, and removal of physical access to Information resource facilities (such as data centers, wiring closets, offsite tape storage, etc.). This includes but is not limited to the following:

- Physical security systems must comply with all applicable regulations including but not limited to building codes and fire prevention codes.
- Physical access restricted facilities must be documented and managed.
- All Information resource facilities must be physically protected in proportion to the criticality or importance of their function.
- Access to Information resources facilities must be granted only to support personnel and contractors whose job responsibilities require access to that facility. Each entry into the datacenter must be logged by a card access system or paper log.
- The process for granting card and/or key access to Information resource facilities must include the approval of Assistant Director Computer Center.
- Each individual that is granted access rights to an Information resource facility must sign an appropriate access and non-disclosure agreements.
- Access cards and/or keys must not be shared or loaned to others.
- Access cards and/or keys that are no longer required must be returned to the uTech Access Control Administrators. Cards or keys must not be reallocated to another individual, bypassing the return process. Cards must be deactivated at once.
- Lost or stolen access cards and/or keys must be reported to the uTech Access Control Administrators as soon as practicable. Lost or stolen access cards must be deactivated at once.
- Cards and/or keys must not contain sensitive information such as SSN or credit card numbers.
- All Information resources facilities that allow access to visitors will track visitor access with a sign in/out log.
- Card access records and visitor logs for Information resource facilities must be kept for routine review minimally for one year.
- The uTech Access Control Administrators must remove the card and/or key access rights of individuals that change roles or are separated from their relationship with the University.

- Visitors in controlled areas of Information resource facilities must be accompanied by authorized personnel at all times. Regular visitors may be provided a vendors access badge. This access requires a business sponsor and must be reviewed annually for continued appropriateness.
- The uTech Access Control Administrators must review access records and visitor logs for the facility on a periodic basis and investigate any unusual access. Recommended monthly but minimally quarterly.
- The University Technology Cabinet or other technology steering committee must review card and/or key access rights for the facility on a periodic basis, minimally annually, and remove access for individuals that no longer require access.
- The datacenter must be equipped with raised floors, heat, air-conditioning, humidity & water control, door cameras, fire suppression and smoke alarms to assure a proper operating environment for System components.
- Power distribution to the datacenter must be secured from unauthorized access. Additionally, all devices in the datacenter or other Information resource facilities should use an uninterruptible power supply (UPS) or other source of continuous reserve power.
- Signage for restricted access rooms and locations must be practical, yet minimal discernible evidence of the importance of the location should be displayed.

Database, Data Mart, Data Warehouse Policy

- There should be only one authoritative source for electronic university records. Because of the strength of RACF security and the technology available on the mainframe to support encryption at rest, it is recommended that the one authoritative source be the Mainframe.
- Proper use of sensitive data begins by evaluating your business processes for the need to take in or store sensitive data and if indeed it is needed ensure that appropriate protection (obfuscation, masking, one-way hash, encryption, etc.) is applied throughout the data lifecycle. Sensitive data must never exist on University systems unprotected.
- The requirement to protect sensitive data extends to backup copies of sensitive data especially when this data is outside University control such as with a vendor, in transit or stored off University property.
- Direct access to data from the Internet must be disallowed. Instead requests for data should be proxied between a requesting segment and a segment hosting the data.
- Don't use default database administrative accounts, such as SA in Microsoft SQL, to access data.
- It is recommended that the default communication port be changed to limit communication between application and data source to approved parties or IP addresses.
- It is recommended that communication between requesting server or application and data source be encrypted.
- It is recommended whenever possible to separate duties between database administrators, application developers, web administrators, etc.
- Database management should be done over secure channels such as SSL or SSH.
- When developing and configuring applications, do not connect to a database as a user with superuser-like authority or as the database owner. Instead, make use of customized users with appropriate limited privileges.

- Some Database Management Systems grant, by default, a number of "public" privileges to each user. It is better to revoke these privileges when possible and grant them as needed.
- Do not grant unnecessary privileges to users and review regularly for continued appropriateness.
- Data accuracy and consistency is important; a unified approach to data governance is highly recommended.
- Every program or every collection of programs implementing a single business function must have unique database credentials.
- Any passwords stored within the database must be encrypted or hashed with an appropriate algorithm.
- It is recommended that developer groups have a process in place to ensure that database passwords are created, controlled and changed in accordance with the university password policy or sooner (in the case of a key resource departure).

Patching Policy

All university owned or operated computer systems and devices are to be protected through the deployment and installation of software patches, service packs, hot fixes, etc. This applies to all services installed, even though some services may be temporarily or permanently disabled (if you don't want to patch it uninstall it). Compliance with this policy must be actively tracked and documented by the support entity responsible for the administration or support of corresponding systems.

Critical security patches must be installed universally across applicable university computers, when they first become available. Non critical patches should be deployed as soon as possible but no later than six months (fall and summer breaks). WIU supports a centralized patching model and advocates that clients receive updates from official university sources managed by University Technology. Windows computers must be configured with auto-update enabled. This setting must be enforced via Active Directory Group Polices.

All security patches must be installed unless testing against critical systems results in system instability or reduction in needed functionality. Exceptions must be documented including a plan of action to eliminate the exception.

University areas responsible for the management of university owned or operated computers must have operational plans in place that includes regular (recommended quarterly but minimally semi-annually) checks to ensure the completeness and effectiveness of their patching processes. Additionally, semi-annual patching metrics and any exceptions must be presented to the CTSO.

Note: As a general rule, it is recommended that when possible you move to the latest version of an application as that will tend to be the most secure. This is especially true for software that is end-of-life as any future vulnerability will not be remediated by the vendor.

Anti-Malware Guidelines

The university supports an approved anti-malware product. Using a non-approved solution will not be University supported and is not recommended.

The following minimum requirements shall remain in force:

- The anti-malware product shall be operated in real time on all client computers and Windows server computers. The product shall be configured for real time protection.
- The anti-malware library definitions shall be checked at least once per day and updated as available.
- Anti-malware scans shall be done a minimum of once per week on all university controlled workstations and servers.
- Removing or permanently disabling anti-malware protection violates this policy.
- WIU supports a centralized anti-malware model and advocates that clients receive anti-malware updates from official University sources managed by University Technology.

Password Policy

This policy provides password guidance intended to maintain control over access to WIU systems and data as well as enumerates authentication requirements necessary for compliance with Payment Card Industry (PCI) Data Security Standards (DSS) that governs university use of credit cards as payment. This policy must be reviewed annually and updated as appropriate.

Password Use

1. All WIU owned or operated computers, which are permanently or intermittently connected to the network, must have an approved password-based access control system.
2. All in-bound non-ecommerce connections to WIU computers from external networks (Internet, dial-up lines, etc.) must, at a minimum, be protected with a password.
3. All vendor-supplied and or default passwords must be changed before any computer or communications system is used in production or hosts any WIU data.
4. Users are prohibited from logging into any system or network anonymously (guest). All Users must be positively identified by a unique ID and password. When non – administrative users need to elevate to administrative level privileges, they must have initially logged-in using their personal User-ID that clearly indicated their identity. Public systems such as those found in the Library and the Student Union are exempt from this requirement.
5. Systems should require re-authentication after 30 minutes of inactivity.

6. Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public", "private" and "system" and must be different from the passwords used to log in interactively.
7. Passwords used on WIU Systems **should NOT** be:
    - The same password as for other non-WIU access (e.g., personal ISP account, option trading, benefits, etc.);
    - Shared with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential information;
    - Revealed over the phone;
    - Revealed in an email, IM, chat rooms, blogs or text message;
    - Discussed in front of others or online;
    - Revealed on questionnaires or web forms;
    - Shared with family members, friends or acquaintances; or
    - Revealed to co-workers.
8. It is strongly recommended, unless there are mitigating circumstances, that passwords are not shared. They represent sensitive, confidential information.
9. Group or shared accounts are allowed strictly to support the universities external outreach mission. These accounts can only be used by non-university entities. University areas sponsoring these arrangements are responsible for documenting and annual review of these arrangements to ensure continued appropriateness. General password controls apply to these arrangements.
10. Vendor accounts must only be enabled during a maintenance window and with proper & approved change control.
11. If someone requests a user id and password, refer the individual to this policy and have him or her call the Support Center (309.298.2704).
12. Do not use personal information (e.g. name, birthday, phone, address, etc.) or your username as part of your password.
13. Do not use the "Remember Password" feature of any application (e.g., Internet Explorer, Outlook, Netscape, Mozilla's Firefox, etc.).

General Password Controls

The following password controls must be implemented on WIU controlled network and systems:

1. Passwords must be changed every one hundred & twenty (120) days or less to coincide with the university business model based on semesters.
    - Up to two (2) grace logins are allowed to support users that do not use a system as often as every one hundred & twenty (120) days
    - All accounts are disabled after fifteen (15) months of inactivity except accounts having access to credit card which must be disabled after ninety (90) days or less of inactivity.
    - STARS & TeleSTARS are targeted to support a password change policy during the fall semester 2009.
2. Passwords must be a minimum of eight (8) characters in length.
    - STARS & TeleSTARS currently only support four (4) characters but planned support for eight (8) characters is targeted for fall semester 2009.
3. Long passwords of up to fifteen (15) characters should be supported.
    - WIUP can only support up to eight (8) characters; STARS & TeleSTARS can currently only support four (4) characters but planned support for eight (8) characters is targeted for fall semester 2009.
4. All passwords must contain one or more numbers and one or more alphabetic characters.
    - STARS & TeleSTARS currently only support numeric characters but planned support for alphabetic characters is targeted for fall semester 2009.
    - Planned support on all systems for upper case letters is targeted for fall semester 2009.
5. Users must not be able to reuse the ten (10) previous passwords.
6. User accounts are locked after six (6) invalid logon attempts or less.
    - Lock out accounts for 30 minutes or until administrator enables the user ID;
7. Unsuccessful logon attempts should be logged.

Additional Password Controls Specific to Roles Having Administrative Rights (complete and unrestricted access) on Systems or Networks

1. All administrative-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed every 60 days. Areas may choose to change passwords more often but never less.
2. No more than six (6) logon sessions should be supported.

Additional Password Controls for Areas Taking Credit Cards as Payment

When PCI DSS requirements and university policy do not match the most restrictive policy applies:

1. Have account additions, deletions and modifications managed centrally;
2. Have a user's identity verified before performing password resets;
3. Have first time passwords set to a unique value for each user and must require the password to be changed immediately after the first use;
4. Have access immediately revoked upon termination of employment;
5. Be disabled after ninety (90) days of inactivity (overrides university policy of fifteen months of inactivity);
6. Not be shared, generic or group accounts;
7. Have their corresponding passwords changed every ninety (90) days or less. (overrides user level access policy of one hundred & twenty days but is overridden for administrative-level access by university policy which states that administrative passwords must be changed every 60 days or less);
8. Have passwords with a minimum password length of seven characters (is overridden by university policy which states eight character minimum);
9. Have passwords that contain both numeric and alphabetic characters;
10. Have passwords that are different from any of the last four (4) previous passwords (is overridden by university policy which states the previous ten passwords);
11. Require all access to any database containing cardholder data to be authenticated (includes access by applications, administrators and all other users).

Administrative Rights Guidelines

This Policy establishes guidelines for the proper use of administrative rights on University computer systems. This includes but is not limited to the following:

- WIU computers are University property and are intended for University business.
- Individuals should refrain from installing non University approved or unlicensed applications (software)
- The University strongly recommends and encourages individuals to utilize University Technology support staff to install any software that is necessary on their workstation.
- Individuals should refrain from altering or removing any standard software as originally installed.
- Non-standard software may be removed as part of a normal repair process if necessary to restore system functionality.
- WIU recommends that individuals save all documents on their university provided personal network space and not to the local computer or removal media.
- Multi-factor (two or more factors) authentication is required for remote access to the network by administrators, vendors and third parties.
- All University workstations are configured with remote support software. This software allows technology staff to remotely assist users if necessary. Below are recommended technical controls for the use of Remote Desktop Protocol (RDP) at WIU:

    - Block all unencrypted traffic such as telnet and the UNIX R commands (rsh, rlogin, etc.) at the perimeter and residential networks.
    - Block remote administration applications (such as RDP, Apple NetAssistant, PCAnywhere, VNC, etc.) at the perimeter and residential networks. Requiring that remote administration be done strictly over an encrypted VPN session.
    - Block remote control services (such as GoToMyPC, LogMeIn, etc.) at the perimeter and residential networks.
    - Allow Secure Shell v2 (SSH-2) both internally and remotely for remote administration. Only when a device cannot support SSH-2 should Secure Shell v1 (SSH) be used.

Server Lockdown and Hardening Procedures

All University owned or operated servers must be consistently and systematically locked-down (a method used to protect computers by restricting functionality of a system to its core functions thereby reducing the ways a system can be attacked). However, servers with access to sensitive data or exposed to public networks (such as the Internet) may require additional precautions based on associated risk. The office of the CTSO maintains lockdown standards, for Windows and UNIX/Linux/Mac servers.

Change Management Guidelines

The purpose of the Change Management Policy is to manage changes in a rational and predictable manner so that constituents can plan accordingly. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce negative impact to the user community and to increase the value of Information resources.

- Changes to WIU Information resources such as: operating systems, computing hardware, networks, and applications are subject to the Change Management Policy and must follow appropriate Change Management procedures.
- A Change Management Committee that represents uTech, AIMS, ESS, Library, etc. must meet regularly (recommend weekly) to review change requests and to ensure that changes and communication is being satisfactorily performed.
- All scheduled change requests must be submitted in accordance with change management procedures so that the Change Management Committee has time to review the request, determine and review potential failures, and make the decision to allow or delay the request.
- A formal written change request must be submitted for all changes, both scheduled and unscheduled.
- Customer notification must be completed for each scheduled or unscheduled change.
- All changes affecting computing environmental facilities (e.g., air-conditioning, water, heat, plumbing, electricity, and alarms) need to be reported to or coordinated with Physical Plant.
- Each scheduled change request must receive formal Change Management Committee approval before proceeding with the change.
- Emergency changes (made outside standard change management) will require Director/Dean or above approval as well as follow up Change Management procedures to properly document the emergency change.
- Changes may be delayed or denied for such things as inadequate planning, inadequate backout plans, the timing of the change will negatively impact a key business process, or if adequate resources cannot be readily available.
- A Change Management Log must be maintained for all changes. The log must contain, but is not limited to:
    - Date of submission and date of change
    - Owner and contact information
    - Nature of the change
    - Back out plan
    - Indication of success or failure
- Continues unplanned changes or blatant disregard for the Change Management process constitutes a security event and may entail disciplinary action.

Business Continuity and Disaster Recovery Guidelines

The university responds in a manner that prioritizes the immediate safety of our constituents, preservation of property, and a quick recovery in order to meet business needs. Minimally the following must be addressed:

- Key systems, applications and data must be enumerated, key individuals identified, and documented procedures put in place to switch to alternative systems should our primary systems be incapacitated.
- All computer resources used for mission critical applications shall have cost effective, written contingency plan that will provide for prompt and effective continuation of critical missions in the event of a disaster.
- In the event that the main datacenter becomes inoperable, the university will shift its operations to its designated back-up facility which is reasonably distant from the main campus so as to reduce the chance that it will be affected by the same event, yet close enough to relocate to quickly if necessary.
- WIU maintains back-ups of its files at off-site facilities. Should an event cause our primary records to be inaccessible or destroyed, the university must have procedures in place to access the back-up files in order to assure the least possible impact. Minimally quarterly testing of backup and restore procedures must be conducted, documented and reported.
- Testing of recovery plans must be completed annually (it is recommended that key system be tested twice a year) and documentation and training adjusted as needed.
- WIU has business relationships with several entities upon which we rely for varying services. Arrangement must be made for the continued availability of products and services during a business interruption. This can take a number of forms including contractual, insurance, and documented and tested plans.
- BC/DR plans must address regulatory and compliance requirements such as PCI as well as state of Illinois audit general findings and recommendations.

Integration of Contingency Planning / Disaster Recovery into Projects

All new technology projects will address contingency planning / disaster recovery as part of their development. Minimal items that need to be determined are:

- How critical is this project to the recovery of the business unit?
- How will the business unit function without the services of the project?
- How will the business unit recover the services provided by the project?
- What additional equipment or services are needed for this project to be fully recoverable?
- Provisions for contracting disaster recovery services from the vendor should be reviewed as part of the contract.

Incident Response Guidelines

The uTech Security Specialist is responsible for up keep of the University Security Incident Response procedures and for the initial evaluation, escalation of security incidents to include the following:

- Assess the seriousness of an incident,
- Assess the extent of damage,
- Identify the vulnerability created and the risk to the University
- Estimate what additional resources are required to mitigate the incident.
- Proper escalation (Vice President for QC Campus, Planning & Technology, CTSO, uTech, Support Center, ESS, AIMS, law enforcement, other external entities, etc.)
- Ensure that proper follow-up reporting occurs and that procedures are adjusted so that responses to future incidents are improved.

Vendor Management Policy

University units using 3rd party vendors for information system services or custom software development must ensure that proper controls are in place to satisfy the Universities "due diligence" requirements including but not limited to the following:

- Information security contract language must be added to all contracts that provide access to University systems, data, sensitive areas (such as data centers, wiring closets, etc.) or provide custom development on behalf of the University. This is coordinated through the Office of the Vice President for Administrative Services. Sample contract language is available here.
- It is recommended that a Non-Disclosure Agreements (NDA) be on file at the business office for each vendor that handles University proprietary or sensitive data on behalf of the University.
- Custom software development by third parties of critical systems or systems collecting, transmitting or storing sensitive data must comply with Secure Application Development guidelines as defined in the Administrative Procedure.

Secure Application Development Guidelines

This Policy establishes guidelines to ensure that risk associated with university applications are properly managed. This includes but is not limited to the following:

- Units are encouraged to consult with University Technology (uTech) and Administrative Information Management Systems (AIMS) prior to engaging any custom application development to assure that centralized, freely available full-time programming resources can be used in some capacity, including defining requirements, scope, architecture, security, data modeling, project management, etc.

- It is highly recommended that any major application development effort or any application development effort involving sensitive data follow the university Secure Web Application Development Standards (ECOM login required).
- Applications must work on existing infrastructure.
- The office of the CTSO reserves the right to have an application assessed prior to being made available for use. Depending on the risk to the university this may include having the application assessed by a third party at department expense.
- On request, source code and documentation will be provided to the office of the CTSO or internal audit (may apply to custom code developed by a 3rd party for the university)
- Prior to installation on WIU's production environment, major applications or applications that touch sensitive data must be tested on an uTech-managed test environment.
- Units should make provision for ongoing technical support of the application, whether through local programming resources, a SLA with University Technology, or a maintenance contract.
- No programs will run at a level that bypasses security
- Units must complete an application authorization form (ECOM login required) which provides for the authorization, inventory and tracking of future application development efforts.
- Custom software development requires but is not limited to the following:
    - An application firewall should be in place to provide an umbrella of security for yet to be remediated applications and yet unknown (zero day) vulnerabilities.
    - It is recommended that peer code reviews and walkthroughs be done.

Applications must be scanned for security vulnerabilities and remediated prior to going into production. This requirement can be met by vendors providing a detailed independent 3rd party security audit reports (security vendor must be reputable such as VeriSign, Foundstone, etc.) showing that all high level or higher security vulnerabilities have been remediated or a reasonable remediation timeline has been documented and agreed upon. Minimally annually University Technology must conduct penetration testing of network components and applications.