Table of Contents

1. Acceptable Use Regulation

1.1 Network Mission. The Network, and through the Network the Internet, offers an abundance of educational material as well as opportunities for collaboration and the exchange of ideas and information. Washburn University recognizes the educational value of the Internet, and strongly encourages the responsible use of the Network by all students and employees. Successful operation requires that all users view the Network as a shared resource, and work together to maintain its integrity by behaving in a responsible, conscientious manner.

This regulation describes the types of network applications that are contrary to our Network Mission and which are therefore prohibited. These are guidelines only and are not meant to be an exhaustive list of prohibited activities.

1.2 Definition of Network. The Network is defined as all Washburn University computer and communication devices and technology infrastructure which store, access or transmits data.

1.3 Definition of User. A user is defined as any person that is not Information Technology Services Personnel who has been assigned a valid WUAD logon by Information Technology Services (ITS). Such logons (or accounts) should be used only by the owner of the account in a legal and ethical manner.

1.4 Privacy Rights and Security. Student and employee data files, email, and electronic storage areas are considered the property of Washburn University, subject to Washburn University' control and inspection. The appropriate Information Technology Services administrator may access all such files and communications to ensure system integrity and that users are complying with the requirements of this regulation and any associated regulations. Students and employees should not expect that information stored on the Network will be private.

Users are responsible for the use of their individual account and should take all reasonable precautions to prevent others from being able to use their account. Under no conditions should a user provide his or her password to another person. Users will immediately notify the Information Technology Services if they have identified a possible security problem relating to misappropriated passwords.

1.5 Prohibited Use

1.5.1 Illegal or Destructive Activities. Users may not use the Network for any purpose that violates the law or threatens the integrity of the Network or individual workstations. Prohibited activities include, but are not limited to:

- Attempting to gain unauthorized access to the Network or go beyond their authorized access. This includes attempting to log on through another person's account, generic account or access another person's files, attempting to obtain passwords, or attempting to remove any existing network security functions. Users will not actively search for security problems, because this will be construed as an illegal attempt to gain access.
- Intentionally developing or using programs to harass other users or to attempt to violate the security or alter software components of any other network, service or system. Examples of such activities include hacking, cracking into, monitoring or using systems without authorization, scanning ports, conducting denial-of-service attacks and distributing viruses or other harmful software.
- Attempting to damage hardware, software or data belonging to the university or other users. This includes adding, altering or deleting files or programs on local or network hard drives and removing or damaging equipment such as mice, projectors, motherboards, speakers or printers.
- Fraudulent use of credit card numbers to purchase online merchandise.
- Connecting or disconnecting any hardware to the network that has not been pre-approved by ITS
- Distributing or downloading licensed software or installing software such as games or music in violation of software license agreements (piracy). This includes any peer-to-peer file sharing.

1.5.2 Inappropriate Material. Users should use the Network in an ethical and lawful manner and will not use the Network to access or distribute material that that advocates illegal acts including but not limited to violence or discrimination toward others if not for scholarly purpose. This includes but is not restricted to distribution through email, discussion groups or web pages. Use of the Network that is discriminatory or harassing may violate the other policies, procedures, and regulations.

1.5.3 Respect for Other Users. Users should be respectful to all individuals. The University encourages civil discourse and tolerance in communication, including all use of electronic information resources.

Users will not harass other persons through the network. Such harassment includes, but is not limited to, distribution of unsolicited advertising, chain letters, or email spamming (sending an annoying or unnecessary message to a large

number of people). Users will not post personal contact information about other people, including address, telephone, home address, work address, etc. Users will not send mail that does not accurately identify the sender, the sender's return email address, and the email address of origin.

1.5.4 Resource Limits. No software shall be downloaded from the Internet or email on a workstation without prior permission from Information Technology Services personnel. Software installed by any user other than Information Technology Services personnel is considered a violation of this regulation without prior consent. Users have a right to temporary use of disk storage space and are responsible for keeping their disk usage below the maximum size allocated. Long term storage of large video files should be stored on the streaming server. Extremely large files, if left on the network for an extended period, may be removed at the discretion of the CIO.

Users will check their email frequently. Where applicable, users will comply with Washburn University policies, regulations and procedures as well as state and federal statutes and regulations governing public record retention.

Users are to utilize the university email for the purposes related to the university and performance of their jobs, but incidental personal use is allowed. Use of university technology, including email accounts, is limited to purposes related to the university and employees' job performance. Use of university technology for private financial gain, advertising, solicitation or fund-raising for any non-university purpose will be considered a violation of this regulation unless approved by the Area Head.

1.5.5 Theft of Intellectual Property. Users will respect the legal protection provided by copyright law and license agreements related to content, text, music, computer software and any other protected materials. Users will not plagiarize works that they find on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were original to the user. Users will respect the rights of copyright owners. Copyright infringement occurs when an individual inappropriately reproduces a work that is protected by a copyright. If a work contains language that specifies acceptable use of that work, the user shall follow the expressed requirements. If the user is unsure whether or not they can use a work, they should request permission from the copyright owner. It is the regulation of Washburn University that any illegal peer-to-peer file sharing over the University's network is prohibited. Unauthorized distribution of copyrighted material, such as through peer-to-peer networks, may subject users to civil and criminal penalties. Federal law authorizes a copyright owner to recover civil damages. You can also be prosecuted criminally for copyright infringement.

1.6 Virus Protection. To maintain a secure and reliable computing environment within our campus, Washburn University requires all computers connected to the Network to, or that could be connected to the Network, have a reliable and updated anti-virus scan program on each computer. This program will be updated and scans performed on a regular basis. Information Technology Services shall maintain network-level anti-virus protection on university owned devices. Any person who knowingly introduces malware such as a virus, worm, or Trojan horse programs onto any computer or server is subject to disciplinary action, including restitution.

1.7 Security Awareness. All students and employees who have access to computers, email, or other forms of electronic data will acknowledge that they have read and agree to comply with all Washburn University policies and regulations adopted by Information Technology Services.

1.8 Username and Password. Washburn University requires all employees and students be properly identified and authenticated before being allowed to access the university Network. Users are responsible for safeguarding their passwords and are responsible for all transactions using their passwords. No individual may assign his or her account or password to any other person. Any person who deliberately makes their account available to an unauthorized user will incur termination of their account. Similarly, any person who fraudulently gains access to another person's password or account may incur disciplinary action.

1.9 Network Security. Any and all actions that jeopardize the integrity and stability of the network by violating the network security standards outlined in the Acceptable Use Regulation or other university regulation or policy is subject to disciplinary action commensurate to the level of risk or damage incurred.

1.10 Access. Employees and students who are given authorization may connect to the university Network, for university activities through a wired or wireless connection after demonstrating compliance with security procedures established by the Information Technology Services.

1.11 Remote Access. This regulation refers to connection to the university computing Network from outside of the Washburn University network, such as from an employee's home.

The computer systems, networks and data repositories of the university's Network are critical resources and will be protected against unauthorized access, malicious access, and disruption of service. Authorized users of the university's computer systems, networks and data repositories may be permitted to remotely connect to those systems, networks

and data repositories for the conduct of university related business only through secure, authenticated and carefully managed access methods.

1.12 Technology Hardware and Software Procurement. To maintain high levels of reliability, cost effectiveness, and interoperability of the communications and data technology within the university, Washburn University requires all technology purchases, with the exception of toner/ink cartridges, be approved by Information Technology Services.

1.13 Ellucian Banner. Washburn University maintains a database system for a wide variety of information management purposes. Much of the information is personal information on students, faculty, employees, alumnae and friends of the university. Washburn University considers the security of this information to be one of the university's most serious responsibilities, and accordingly, access to these databases is limited to persons who have a legitimate need to use the information to advance the academic and administrative goals of the university.

Persons who are given passwords and have legitimate access to the information on Ellucian Banner have a strict responsibility to ensure that this information is used appropriately, and that the privacy of persons identified through this information is strictly protected. This responsibility extends both to information available on computer screens as well as information available in print media, including all printouts, manual dossiers, correspondence files, directories, and similar forms of information banks.

1.14 Telephone System and Voice-Mail. Washburn University provides telephone and voice mail access to many employees. The same policies and expectations that govern e-mail also govern voice mail and telephone usage.

1.15 Violation of these Regulations and Procedures. The CIO has authority to disable any account where there is a violation of these regulations and procedures. Violations of will be addressed through the Student Conduct Code for students or Washburn University Policies, Regulations, and Procedures Manual (WUPRPM) for employees and may result in disciplinary action up to and including termination. The university may involve, and will cooperate with, law enforcement officials if criminal activity is suspected. Violators may also be subject to civil or criminal liability under applicable law.

2. Information Security Plan

2.1 Purpose. This compliance plan ("Plan") describes Washburn University's safeguards to protect non-public, financial-related personal information ("covered information") in accordance with the requirements of the Gramm-Leach-Bliley Act of 1999 (GLBA) and any amendments thereafter. The Safeguards Rule of the GLBA, as defined by the Federal

Trade Commission (FTC), requires financial institutions, which the FTC explicitly indicated includes higher education institutions, to have an information security program to protect the confidentiality and integrity of personal information.

2.1.1 These safeguards are provided to:

- Ensure the security and confidentiality of covered information.
- Protect against anticipated threats or hazards to the security or integrity of such information.
- Protect against unauthorized access to or use of covered information that could result in substantial harm or inconvenience to any customer.

2.1.2 This Information Security Plan also provides for mechanisms to:

- Designate an employee or employees to coordinate the information security program.
- Identify and assess the internal and external risks that may threaten covered information maintained by Washburn University.
- Design and implement safeguards to control the identified risks.
- Oversee service providers, including third party contractors, to ensure appropriate safeguards for covered information are maintained.
- Periodically evaluate and adjust the information security program as circumstances change.

2.2 Scope. This regulation applies to all Washburn University colleges, departments, administrative units, affiliated organizations and third party contractors that create, access, store or manage covered information.

2.3 Responsibility. The Chief Information Officer (CIO) or designee is responsible for this plan. The CIO or designee will approve any exception to this plan.

2.4 Authority. This plan responds to the Gramm-Leach-Bliley Act of 1999 that mandates protection of customer information, which for universities is primarily student financial information. See section 1.6 Definitions for a definition of information covered by this regulation.

2.5 Regulation. The University will develop, implement and maintain a comprehensive information security program that contains administrative, technical, and physical safeguards to protect covered information.

2.6 Definitions

2.6.1 "Covered Information" Information that Washburn University has obtained from an employee or student in the process of offering employment or a financial service, or such information provided to the University by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student's parent when offering a financial aid package, and other miscellaneous financial services. Examples of student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers, in both paper and electronic format.

2.6.2 "Information Security Program" The administrative, technical, or physical safeguards used to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle covered information.

2.6.3 "Service Providers" Any person or entity that receives, maintains, processes, or otherwise is permitted access to covered information through its direct provision of services to the University.

2.7 Roles and Responsibilities

2.7.1 IT Security Analyst (ITSA). The ITSA is responsible for coordinating and overseeing all elements of Washburn University's information security program. The ITSA will work with appropriate personnel from other offices as needed (such as the Registrar's Office, Internal Audit, and the Division of Financial Services) to ensure protection of covered information.

2.8 Information Security Program Elements

2.8.1 Risk Assessment. Under the oversight of the ITSA, risk and privacy assessments are performed for all information systems that house or access covered information. These risk and privacy assessments shall address unauthorized access, use, disclosure, disruption, modification and/or destruction of information or the information system itself. Further, the assessments shall identify known potential threats, the likelihood of their occurrence and the magnitude of the impact of those threats should they occur.

2.8.2 Internal and external risks at Washburn University include, but are not limited to:

- Unauthorized access of covered information by persons within or outside the University
- Compromised system security as a result of human error, vulnerabilities, infection by malicious software, or unauthorized system access

- Interception of data during transmission
- Loss of data integrity
- Physical loss of data in a disaster
- Errors introduced into the system
- Corruption of data or systems
- Unauthorized access through hardcopy files or reports

2.9 Unauthorized Disclosure

2.9.1 Risk and privacy assessments are used to determine the likelihood and magnitude of harm that could come to an information system, the affected individual(s), and ultimately the University itself in the event of a security breach. By determining the amount of risk that exists, the University shall determine how much of the risk should be mitigated and what controls should be used to achieve that mitigation.

2.9.2 Both risk and privacy assessments shall be performed prior to, or if not practical, immediately after acquisition of an information system (in the event that the information system is owned/operated by the University) or prior to initial establishment of service agreements (in the event that the information system is owned/operated by a third party on behalf of the University). Further, the risk and privacy assessments shall be reviewed and, where required, updated after three years or whenever a significant change is made to the information system, whichever comes first.

2.9.3 Risk assessment should include consideration of risks in each of the following operational areas, in accordance with the requirements of the GLBA.

2.10 Employee Training and Management

2.10.1 Prior to being granted access to covered information, new employees in positions that require access to covered information will receive training on the importance of confidentiality of employee and student records, student financial information, and other types of covered information, and the risks of not providing appropriate protection. Furthermore, all employees receive annual training in general information technology security. Training also covers controls and procedures to prevent employees from providing confidential information to an unauthorized individual through social engineering or improper disposal of documents that contain covered information. All training will be reviewed and, where needed, updated at least annually.

2.10.2 Each department that is responsible for maintaining covered information is instructed to take steps to protect the information from accidental deletion, destruction, or loss due to environmental hazards, such as fire and water damage.

2.11 Information Systems. Including network and software design, as well as information processing, storage, transmission, and disposal.

2.12 Incident Management. Including detecting, preventing and responding to attacks, intrusions, or other systems failures. Washburn University's strategy for managing IT security incidents, including assessing risks, is described in the Security Incident Reporting and Response Regulation and associated IT Security Incident Management.

2.13 Designing and Implementing Safeguards. Safeguards are necessary to mitigate and control the risks identified through risk assessment. Furthermore, the effectiveness of safeguards' key controls, systems, and procedures should be regular tested to ensure continued protection of covered information. Protection of covered information is explicitly encompassed by Washburn University's comprehensive information security program that protects all Washburn University information and technology assets, commensurate with size and complexity of the institution, the nature and scope of activities, and the sensitivity of information assets.

2.14 Overseeing Service Provider. In the process of choosing a service provider that will maintain or regularly access covered information, the selection and retention processes shall ensure the ability of the service provider to implement and maintain appropriate safeguards for covered information. The CIO will review all technology related contracts. Contracts with service providers may include the following provisions:

- An explicit acknowledgment that the contract allows the contract partner access to covered information.
- A specific definition or description of the covered information being provided.
- A stipulation that the covered information will be held in strict confidence and accessed only for the explicit business purpose of the contract.
- An assurance that the contract partner will protect the covered information it receives according to commercially acceptable standards and no less rigorously than it protects its own covered information.
- A provision providing for the return or destruction of all covered information received by the contract provider upon completion or termination of the contract.

- An agreement that any violation of the contract's confidentiality conditions may constitute a material breach of the contract and entitles Washburn University to terminate the contract without penalty.
- A provision ensuring that the contract's confidentiality requirements shall survive any termination of the agreement.

2.15 Program Evaluation and Adjustment. The ITSA will periodically review and adjust the information security program as it relates to the GLBA requirements, with input from the Technology Steering Committee and relevant stakeholders. Program evaluation should be based on results of testing and monitoring of security safeguard effectiveness and reflect changes in technology and/or operations, evolving internal and external threats, and any other circumstances that have a material impact on the information security program. The CIO will review any recommended adjustments.

Approved by the Technology Steering Committee on September 28, 2017

3. Backup Regulation

3.1 Overview. Electronic backups are a business requirement to enable the recovery of data and applications in the case of natural disasters, system disk drive failures, data entry errors, viruses, or system operations errors.
3.2 Purpose. The purpose of this regulation is to establish the rules for the backing up and storage of backups containing Washburn University's electronic information.

3.3 Scope. This regulation applies to all Staff that are responsible for the installation and support of IT, individuals charged with IT Security, and data owners. A list of data owners is on file with the ITS department.

The Assistant Director of Systems & Network Services is responsible for implementation of this plan.

3.4 Regulation. Backups are used to provide corrective action against various types of threats including:

- Human error - accidental deletion of files
- Malicious software – viruses delete or corrupt systems and data
- Intentional actions – a hacker deletes files
- Hardware failure – a hard drive fails, and files will be deleted
- Application processing errors – database will be restored

• Facility issues – a fire, water damage, or electrical surge damages equipment

Backups are an important part of providing information systems availability and are critical to Washburn University's business continuity. The ITSA will determine the risks related to Information Systems and will evaluate the following tiers to determine the appropriate Tier for Washburn University given our recovery time objectives (how much downtime is acceptable), recovery point objectives (how much data loss is acceptable), and costs:

- Tier 1: Data backup with no hot site - systems are backed up and the media is sent to an off-site storage facility. Without a hot site, recovery may require weeks or months. Manual or additional processes are needed to continue business operations.
- Tier 2: Data backup with a hot site – contains the elements of Tier 1 plus a hot site provides the required hardware and operating systems to allow recovery from the backup media. Recovery can typically be achieved in one to two days depending upon the extent of damage, activation of hot site, and restore time.
- Tier 3: Electronic vaulting - contains the elements of Tier 2 plus mission critical data is electronically vaulted where data is transmitted to another secure location (typically off-site) via a network or communication link rather than via portable media. Recovery can typically be achieved in less than one day.
- Tier 4: Point-in-time copies - selected systems are copied to disk according to a pre-determined schedule. In this Tier either an off-site facility receives encrypted disks or the point in time copies are used to supplement traditional encrypted backup media sent off-site. Depending upon the type of disruption, recovery may require several hours up to one day.
- Tier 5: Transaction integrity - software applications are coded to ensure transactions are fully complete with integrity. This ensures consistency of data between production and recovery systems. Recovery may be able to be achieved in less than one hour.
- Tier 6: Near zero data loss - robust business continuity solutions maintain the highest levels of data currency and allow quick access to data. Solutions have no dependence on the applications and may require some form of disk mirroring or synchronizing solutions. Recovery may be achieved in less than an hour with almost no loss of data.
- Tier 7: Highly automated, business integrated solution - contains the elements of Tier 6 plus automation. Restoring of systems, applications, and data is automated. This Tier may involve data replication to a redundant data center. Recovery may be achieved in a few minutes with almost no loss of data.

Once the appropriate Tier has been identified, the ITSA shall ensure:

- Washburn University's Backup Plan identifies procedures to implement the requirements of this regulation and the appropriate Tier.
- Documentation identifies the location of sensitive information to ensure that it can be backed up.
- Documentation includes all important sources of data such as accounting systems, electronic records, diagnostic images, and other documents created or used.
- Procedures create and maintain retrievable exact copies of information.
- The frequency and implementation of backups is appropriate according to the requirements of the selected Tier.
- Backups are stored in a safe and secure place and comply with the requirements of the selected Tier. Backups shall be encrypted to ensure information confidentiality.
- Procedures specify when a retrievable, exact copy of sensitive information will be created before movement of equipment.
- Procedures identify who is responsible for creating a retrievable exact copy of sensitive information before movement of equipment.

The frequency and extent of backups will be in accordance with the importance of the information and the acceptable risk as determined by the data owner. The IT backup and recovery process for each system will be documented and periodically reviewed.

Vendor(s) providing off-site backup storage and recovery solutions will be cleared to handle the highest level of information stored.

Physical access controls implemented at off-site backup storage and recovery locations will meet or exceed the physical access controls of the source systems. Backups will be protected in accordance with the highest sensitivity level of information stored.

A process will be implemented to verify the success of the electronic information backup. Backups will be periodically tested to ensure that they are recoverable.

Signature cards held by the off-site backup storage and disaster recovery vendor(s) for access to backups will be reviewed annually or when an authorized individual leaves Washburn University.

Procedures between Washburn University and the off-site backup storage and disaster recovery vendor(s) will be reviewed at least annually.

Backups will have at a minimum the following identifying criteria that can be readily identified:

- System name
- Creation date
- Classification
- Washburn University contact information

4. Access Controls

4.1 Purpose. Access controls are the rules that an organization applies in order to control access to its information assets. The risks of using inadequate access controls range from inconvenience to critical loss or corruption of data. This regulation defines access control standards for system use notices, remote access, and definition and documentation of trust relationships for Washburn University information systems.

4.2 Scope. This regulation applies to all Washburn University colleges, departments, administrative units, and affiliated organizations that use university information technology resources to create, access, store or manage Washburn University Data to perform their business functions.

4.3 Regulation. Access control standards for Washburn University information systems are to be established in a manner that carefully balances restrictions that prevent unauthorized access to information and services against the need for unhindered access for authorized users.

4.3.1 System Use Notice. Before a user gains access to a Washburn University computer, a general system use notice will be displayed that welcomes users and identifies it as a Washburn University system, warns against unauthorized use of the computer, and indicates that use of the system implies consent to all relevant Washburn University policies. The general system use notice should also be displayed before a user gains access to a Washburn University information system, where practical. The system use notice will state the following:

Washburn University Acceptable Use

- Use only those computing resources for which you have authorization

- Protect your account information from access by others

- Use computing resources for university-related work

- Comply with all applicable local, state and federal laws, including copyright and licensing laws
- Respect the privacy of others
- Respect the use of computing resources by others
- Comply with security measure employed by the university
- Report violations of all policies, procedures and regulations
- Comply with all Washburn University policies and regulations at: http://www.washburn.edu/faculty-staff/human-resources/wuprpm

PLEASE NOTE: Store documents in My Documents or other networked drives. Documents stored in C: are not backed up.

4.3.2 Remote Access. Remote access control procedures will provide appropriate safeguards through appropriate identification, authentication, and encryption techniques. Direct log-on to campus computers from off-campus locations is not allowed. A remote user will first authenticate to an authorized campus remote access service with strong encryption, such as Washburn University's VPN service, before logging into a campus computer. This restriction does not apply to authenticated user access to web applications like Webmail or to systems designed for public access.

4.3.3 Trust Relationships. Trust relationships for centrally-managed University information systems or any system with confidential data will be defined and documented, approved by an appropriate authority, and periodically reviewed and revised as needed. Security controls, such as firewall rulesets, will be configured to enforce the trust relationships.

4.4 Definitions

4.4.1 Authentication. Process of verifying one's digital identity. For example, when someone logs into a workstation or server with their WUAD, the password verifies that the person logging in is the owner of the WUAD. The verification process is called authentication.

4.4.2 Confidential Data. Highly sensitive University Data intended for limited, specific use by a workgroup, department, or group of individuals with a legitimate need-to-know.

4.4.3 Washburn University Computer. Any computer considered to be the property of Washburn University.

4.4.4 Local Network. Any segment of Washburn University's data network physically located on any Washburn University campus. This includes devices on the network assigned any routable and non-routable IP addresses and applies to the wireless network and the network serving Washburn University's student residence halls.

4.4.5 Remote Access. Accessing a Washburn University local network from any physical location outside the Washburn University campus. This includes access from off campus using Washburn University's Virtual Private Network (VPN) service.

4.4.6 Trust Relationships. A specification of the level of access granted to computer systems and/or applications that are trusted to access resources on a server and its associated data and applications. This applies to access controls between systems, not access rights for individual users or roles.

4.4.7 University Data. Any data related to Washburn University ("University") functions that are:

- Stored on University information technology systems.
- Maintained by Washburn University faculty staff, or students.
- Related to institutional processes on or off campus.

This applies to any format or media (in other words, it is not limited to electronic data).

4.4.8 Virtual Private Network (VPN). Provides a secure communication channel over the Internet that requires authentication to set up the channel and encrypts all traffic flowing through the channel.

4.5 Roles and Responsibilities. ITSA - Responsible for developing guidance on documentation and approval of trust relationships.

4.6 Implementation Procedures. The System Use Notice should be passively displayed such that no user action is required to view it before logging into the Washburn University computer or information system.

4.7 Questions/Waivers. The CIO is responsible for this regulation. The CIO or designee will approve any exception to this Regulation or related procedures. Questions should be directed to the ITSA.

5. Security for Information Technology Resources

5.1 Purpose. To establish and maintain security requirements necessary to protect University information, computing and network resources, and minimize susceptibility to attacks on Washburn University resources or from Washburn University locations against other sites.

5.2 Scope. This procedure and accompanying requirements apply to all Washburn University locations and all system users at any location, including those faculty, students and staff using privately owned computers or systems to access University information, computing and network resources.

Security requirements shall be in place for the protection of the privacy of information, protection against unauthorized modification of information, protection of systems against the denial of service, and protection of systems against unauthorized access. Users are reminded that all usage of Washburn University's information technology resources is subject to all University policies / regulations and regulations.

5.3 General Regulation. Washburn University information, computing and network resources may be accessed or used only by individuals authorized by the University. The University encourages the use of computing and network resources and respects the privacy of users. Nonetheless, the University may access information stored on the University's network of computers for any reason deemed necessary by Information Technology Services (ITS).

The system administrator will need approval from the CIO to access specific mail and data for any purpose. There is no expectation of privacy or confidentiality for documents and messages stored on University-owned equipment.

5.4 Requirements for Information, Computing and Network Security. The following system requirements represent the minimum standard that will be in place in order to establish and maintain security for University information, computing and network resources.

5.4.1 Initial Network Hook-up. Each system will be capable of passing a test for vulnerabilities to hacker attacks and relaying of unsolicited email prior to being attached to Washburn University's information, computing and network resources. System testing will be the responsibility of the ITSA.

5.4.2 Password Specification

5.4.2.1 Password Regulation. All passwords on any system, whether owned by Washburn University or by an individual, directly connected to Washburn University's network will adhere to the following standards when technically possible. This includes devices connected to the campus network with a direct wired connection, wireless, remote access software (e.g., Windows Remote Desktop), use of a Virtual Private Network (VPN), and the like. This regulation applies to all passwords - WUAD, system, user, database, application, etc. Any system that does not comply may have its network access blocked without prior notification. The password standards are maintained by the CIO or designee. Exceptions will be approved by the CIO.

5.4.3 Password Standards

5.4.3.1 Passwords will have a minimum of 10 characters.

5.4.3.2 Passwords will contain characters from 3 of the 4 following categories:

- Uppercase letters
- Lowercase letters
- Numbers
- Special characters (e.g.: !,@,#,$,%,^,&,*, etc. But be aware if traveling outside the U.S. that some symbols, like the U.S. dollar sign, may not be available on international keyboards)

5.4.3.3 Passwords cannot be easily guessed (e.g.: no variants of dictionary words, family names, pet names, birthdates, etc.).

5.4.3.4 Most passwords will be changed every 180 days. Others may need to change more often, depending on access to secure information.

5.4.3.5 Passwords will be changed significantly and cannot repeat more frequently than every two years.

5.4.3.6 Passwords that are written down or stored electronically will not be accessible to anyone other than the owner and/or issuing authority.

5.4.3.7 Passwords will not be shared unless explicitly permitted by the issuing authority. WUAD passwords will not be shared under any circumstances.

5.4.3.8 Anyone who believes their password has been compromised will immediately notify ITS User Services to evaluate possible risks.

5.4.3.9 Default passwords in vendor-supplied hardware or software will be changed during initial installation or setup.

5.4.3.10 The WUAD password will never be transmitted over the network in clear text (e.g., it will always be encrypted in transit). It is also strongly recommended that other types of passwords be encrypted in transit.

5.4.4 Unattended Computers. To protect against unauthorized access to data on computers left unattended, the following precautions are required:

5.4.4.1 Enable password protection on the screen saver for all university computers with the exception of special-purpose computers designed for public access, such as information or registration kiosks, public computers in the library, or computer labs where locking is undesirable due to the risk of a user monopolizing a shared computer. The length of time before the password-protected screen saver comes on should be set to 20 minutes or less. For lab situations, it is recommended that computers be set to automatically logout after at the most 30 minutes of idle time.

5.4.4.2 Never leave your computer unattended and unprotected. Before leaving your computer, lock the display or log out in a manner that requires a password to gain access.

5.4.5 Protection from Malicious Software and Intrusions. Malicious software, or malware, comes in many forms - viruses, worms, Trojan horses, denial of service attacks, botnets, spyware, adware, spam relays, etc. All pose a security risk, some of which are a very serious threat to the confidentiality, integrity, or availability of Washburn University's information and technology resources. Appropriate precautions will be taken to protect Washburn University systems and information from compromise by malware. To that end, Washburn University may require the installation of essential security software on computers connected to the Washburn University campus network or accessing Washburn University information and technology resources. The following sections define specific requirements for antivirus, spyware/adware, personal firewalls, and email. Assuring the validity of malware protection software is the responsibility of each user and the ITSA.

5.4.6 Virus Protection

5.4.6.1 Computers listed below will use the university-supplied antivirus software configured in a managed mode (managed mode allows a server to monitor and configure the antivirus protection on the client computer and push updates to the client on demand). If there is a documented performance issue associated with the use of the university-supplied antivirus software, users will need to have an antivirus on the computer that provides the same security as Washburn

University's standard virus protection. If a University owned or managed computer is compromised and is not running an antivirus program, the computer will remain blocked until the system is rebuilt and an antivirus program is installed.

- Any university-owned computer.
- Users of Washburn University's Virtual Private Network (VPN).

5.4.6.2 Antivirus software will be activated when the computer boots up and remain active at all times during its operation.

5.4.6.3 Real-time file scanning will be enabled where files are scanned for malicious anomalies before they are written to the hard drive.

5.4.6.4 The version of the antivirus software (e.g., the antivirus program or engine) will be no more than one version behind the current version offered by the vendor or the version endorsed by Washburn University, and will be supported by the vendor.

5.4.6.5 Virus definition files (e.g., the database in the antivirus software that identifies known malware) will be up-to-date with the most current version available from the vendor.

5.4.6.6 Checking for and installing updates to virus definition files and antivirus software will be automated and performed at least daily.

5.4.6.7 Comprehensive virus scans of all local hard drives will be performed at least weekly.

5.4.7 Spyware/Adware Protection

5.4.7.1 All Washburn University computers connected to the campus network will run active spyware/adware protection software.

5.4.7.2 Spyware/adware definition/detection rules will be up-to-date with the most current version available from the vendor.

5.4.7.3 Scans of all local hard drives for spyware/adware will be performed at least weekly.

5.4.8 Personal Firewall Protection

5.4.8.1 All computers using the university-supplied security software (which includes virus, spyware, intrusion, and firewall protection) will have the firewall enabled.

5.4.8.2 Any other computer connected to the campus network will run a personal firewall. Microsoft Windows Firewall is an acceptable personal firewall.

5.4.9 Email Protection

5.4.9.1 All campus email servers (Office 365) will provide antivirus protection that detects and mitigates infected email messages.

5.4.9.2 Infected messages will be discarded or quarantined, not returned to the sender.

5.4.10 Security Patches. All systems connected to the campus network and the applications and databases running on those systems will have the latest security patches available from the respective vendors applied. Any system or application with known vulnerabilities for which a patch is not available will take appropriate measures to mitigate the risk, such as placing the system behind a firewall. Washburn University may block access to the network for systems that have not been patched.

The ITSA will determine whether the repair will require the computer to be reformatted and the operating system and all software and data re-installed, depending on the nature of the compromise.

5.4.11 Data Storage. Storage of all types of sensitive information, whether on computer systems, on physical media, or in hard-copy documents should have controls (physical, logical, environmental) in place to protect the data integrity. More sensitive information should have more extensive controls to guard against alteration. Appropriate logging and monitoring controls will be in place over stored information to ensure authorized access and appropriate use. Periodically, the ITSA and data owners should review access rights to ensure the access rights remain appropriate and current.

- Portable Devices: Data storage in portable devices, such as laptops, smart phones, and tablets, poses unique problems. These devices may be lost, stolen, or subject to unauthorized and undetected use. All portable device storage will be encrypted prior to placing any sensitive data on the device.

- Cloud Storage: No sensitive data may be stored in any personal third-party cloud storage. The storing of sensitive data on any organizationally approved third-party cloud storage will be pre-approved by the CIO.
- Removable Media: Portable electronic storage media, such as magnetic, optical, and solid-state devices that can be inserted into and removed from a computing device and that are used to store text, video, audio, and image information. Such devices have no independent processing capabilities. Examples include hard disks, floppy disks, zip drives, compact disks, thumb drives, pen drives, and similar storage devices. All data stored on removable media will be encrypted using AES256 encryption.

5.4.12 Data Transmission. Electronic transmission of information can include encrypted e-mail, secure FTP (sFTP), secure shell, dedicated line, and transmission via the Internet. When transmitting sensitive information over a public network, information should be encrypted to protect it from interception or eavesdropping. An advanced encryption standard (AES) with 256 bits is the recommended standard for sending files over a public network, other techniques include secure e-mail protocols, sFTP, and secure sockets layer (SSL) certificates. Transmission of sensitive data is not allowed utilizing the wireless network.

5.4.13 Security Personnel Responsibilities

5.4.13.1 Information Technology Security Analyst (ITSA)

The University employee who leads the IT security program to protect Washburn University's information, computing, and network resources. Responsibilities include assisting with university-wide IT security policies/regulations, controls and procedures; developing and maintaining security architecture, standards, and guidelines; monitoring compliance with IT security policies/regulations and standards; risk assessment; coordinating responses to security incidents; communication with organizations outside the University; co-chairing the Security Incident Response Team (SIRT); and promoting training and awareness of the secure use of information, computing and network resources.

5.4.13.2 Security Incident Response Team (SIRT)

A team that provides advisory, proactive, and reactive support for Washburn University's IT security program. Responsibilities include coordinating the campus-wide response to major security incidents; coordinating implementation of preventative measures in their colleges/units; communicating threats and best practices to their colleges/units; approving requests for restoring network access

to vulnerable or compromised computers; participating in the development of IT security policies/regulations, standards, guidelines, and procedures; and assisting with IT security training and awareness efforts.

5.4.13.3 Deans and Department Heads

Responsibilities include authorizing access to computer systems in their units, ensuring that System Users understand and agree to comply with University and unit security policies / regulations, and ensuring that the technical and procedural means and resources are in place to assist in maintaining the security policies / regulations and procedures outlined above.

5.4.13.4 System Users

Responsibilities include agreeing to and complying with all applicable University and unit security policies / regulations and procedures; taking appropriate precautions to prevent unauthorized use of their accounts, software programs, and computers; protecting university data from unauthorized access, alteration, or destruction; representing themselves truthfully in all forms of electronic communication; and respecting the privacy of electronic communication.

5.5 Questions

Questions regarding this regulation should be sent to the CIO.

6. IT Security Incident Reporting and Response

6.1 Purpose. This regulation governs the actions required for reporting or responding to security incidents involving Washburn University information and/or information technology resources to ensure effective and consistent reporting and handling of such events.

6.2 Scope. This regulation applies to all members of the Washburn University community, including students, personnel, units, and affiliates using University information technology resources or data.

6.3 Regulation. All members of the Washburn University community are responsible for reporting known or suspected information or information technology security incidents. All security incidents at Washburn University will be promptly reported to the ITSA and other appropriate authorities as outlined below in Section 6.6: Implementing Procedures.

All individuals involved in investigating a security incident should maintain confidentiality, unless the CIO authorizes information disclosure in advance.

6.4 Definitions

6.4.1 Security incident. Any real or suspected event that may adversely affect the security of Washburn University information or the systems that process, store, or transmit that information. Examples include:

- Unauthorized access to data, especially confidential data like a person's name and social security number
- Computer infected with malware such as a worm, virus, Trojan Horse, or botnet
- Reconnaissance activities such as scanning the network for security vulnerabilities
- Denial of Service attack
- Web site defacement
- Violation of a Washburn University security procedures and regulations
- Security weakness such as an un-patched vulnerability

6.4.2 Personal identity information (PII)

K.S.A. § 21-6107: Crimes involving violations of personal rights defines PII as including, but not limited to: an individual's name; date of birth; address; telephone number; driver's license number or card or nondriver's identification number or card; social security number or card; place of employment; employee identification numbers or other personal identification numbers or cards; mother's maiden name; birth, death or marriage certificates; electronic identification numbers; electronic signatures; and any financial number, or password that can be used to access a person's financial resources, including, but not limited to, checking or savings accounts, credit or debit card information, demand deposit or medical information.

6.5 Roles and Responsibilities. The incident manager is responsible for managing the response to a security incident as defined in the incident response summary table in Section 6.6.2.2 below.

The **Security Incident Response Team** oversees the handling of security incidents involving confidential data (e.g., personal identity information). This team has authority to make decisions related to the incident and to notify appropriate parties. The team consists of:

1. Senior administrator for the affected unit
2. Chief Information Officer
3. IT Security Analyst

4. General Counsel
5. University Relations Director
6. Others as needed (for example, FBI / WU Police for criminal incidents)

6.6 Implementing Procedures

6.6.1 Reporting Security incidents

Any member of the Washburn University community who suspects the occurrence of a security incident will report incidents through the following channels:

All suspected high severity events as defined in Section 6.6.2.1 below, including those involving possible breaches of personal identity information, will be reported directly to the ITSA as quickly as possible by phone (preferred), e-mail, or in person. If the ITSA cannot be reached, contact the CIO.

All other suspected incidents will also be reported to the ITSA. Reports should be made by sending email to abuse@washburn.edu (preferred) or by notifying the ITSA by phone, email, or in person.

6.6.2 Responding to Security Incidents

6.6.2.1 Incident Severity. Incident response will be managed based on the level of severity of the incident. The level of severity is a measure of its impact on or threat to the operation or integrity of the institution and its information. It determines the priority for handling the incident, who manages the incident, and the timing and extent of the response. Four levels of incident severity will be used to guide incident response: high, medium, low, and NA (Not Applicable).

High

The severity of a security incident will be considered "high" if any of the following conditions exist:

Threatens to have a significant adverse impact on a large number of systems and/or people (for example, the entire institution is affected)

Poses a potential large financial risk or legal liability to the University

Threatens confidential data (for example, the compromise of a server that contains or names with social security numbers or credit card information)

Adversely impacts an enterprise system or service critical to the operation of a major portion of the university (for example, e-mail, student information system, financial information system, human resources information system, learning management system, Internet service, or a major portion of the campus network)

Poses a significant and immediate threat to human safety, such as a death-threat to an individual or group.

Has a high probability of propagating to many other systems on campus and/or off campus and causing significant damage or disruption

Medium

The severity of a security incident will be considered "medium" if any of the following conditions exist:

Adversely impacts a moderate number of systems and/or people, such as an individual department, unit, or building

Adversely impacts a non-critical enterprise system or service

Adversely impacts a departmental system or service, such as a departmental file server

Disrupts a building or departmental network

Has a moderate probability of propagating to other systems on campus and/or off campus and causing moderate damage or disruption

Low

Low severity incidents have the following characteristics:

Adversely impacts a very small number of systems or individuals

Disrupts a very small number of network devices or segments

Has little or no risk of propagation or causes only minimal disruption or damage in their attempt to propagate

NA (Not Applicable)

This is used for events reported as a suspected IT security incident but upon investigation of the suspicious activity, no evidence of a security incident is found.

6.6.2.2 Incident Response Summary Table. The following table summarizes the handling of IT security incidents based on incident severity, including response time, the responsible incident managers, and notification and reporting requirements. Detailed

procedures for incident response and management are further defined in the Washburn University Security Incident Response Plan.

Incident Severity	Characteristics (one or more condition present determines the severity)	Response Time	Incident Manager	Who to Notify	Post-Incident Report Required
High	Significant adverse impact on a large number of systems and/or people Potential large financial risk or legal liability to the University Threatens confidential data Adversely impacts a critical enterprise system or service Significant and immediate threat to human safety High probability of propagating to a large number of other systems on or off campus and causing significant disruption	Immediate	IT Security Analyst or the Chief Information Officer	IT Security Analyst Chief Information Officer SIRT representative	Yes
Medium	Adversely impacts a moderate number of systems and/or people Adversely impacts a non-critical enterprise system or service Adversely impacts a departmental scale system or service Disrupts a building or departmental network Moderate risk of propagating and causing further disruption	4 hours	IT Security Analyst	IT Security Analyst Unit head SIRT representative Technical support for affected device	No, unless requested by the Chief Information Officer

Incident Severity *(Continued)*	Characteristics (one or more condition present determines the severity)	Response Time	Incident Manager	Who to Notify	Post-Incident Report Required
Low	Adversely impacts a very small number of non-critical individual systems, services, or people	Next Business Day	Technical support for affected device	IT Security Analyst	No
	Disrupts a very small number of network devices or segments			Technical support for affected device	
	Little risk of propagation and further disruption				
N/A	"Not Applicable" - used for suspicious activities which upon investigation are determined not to be an IT security incident.				

6.7 Questions/Waivers. The CIO is responsible for this regulation. The CIO will approve any exception to this regulation or related procedures. Questions should be directed to the ITSA.

7. Security Incident Response Plan

7.1 Purpose. All security incidents will be managed in an efficient and time effective manner to make sure that the impact of an incident is contained and the consequences for the organization and its students are limited. This document sets out the Washburn University plan for reporting and dealing with security incidents.

7.2 Scope. This plan applies to all Washburn University colleges, departments, administrative units, affiliated organizations and third party contractors that create, access, store or manage covered information.

7.3 Authority. This plan responds to the Gramm-Leach-Bliley Act of 1999 that mandates protection of customer information, which for universities is primarily student financial information. See section 4 Definitions for a definition of information covered by this regulation.

7.4 Definitions

7.4.1 "Covered Information" Information that Washburn University has obtained from an employee or student in the process of offering employment or a financial service, or such information provided to the University by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student's parent when offering a financial aid package, and other miscellaneous financial services. Examples of student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers, in both paper and electronic format.

7.4.2 "Security Incident" A Security Incident means any incident that occurs by accident or deliberately that impacts your communications or information processing systems. An incident may be any event or set of circumstances that threatens the confidentiality, integrity or availability of information, data or services in Washburn University. This includes unauthorized access to, use, disclosure, modification, or destruction of data or services used or provided by Washburn University.

7.5 Roles and Responsibilities. The Security Incident Response Plan will be followed by all personnel in the organization. This includes all employees, temporary staff, consultants, contractors, suppliers and third parties operating on behalf of Washburn University, working with Washburn University's or student's data or on Washburn University premises. For simplicity, all of these personnel are referred to as 'staff' within this plan.

7.5.1 Roles. The Washburn University Security Incident Response Team (SIRT) is comprised of various members of the Washburn Community. For a full listing of the current SIRT team members please contact the ITSA.

7.5.2 Responsibilities

7.5.2.1 The Incident Response Lead is responsible for:

- Making sure that the Security Incident Response Plan and associated response and escalation procedures are defined and documented. This is to make sure that the handling of security incidents is timely and effective.
- Making sure that the Security Incident Response Plan is up-to-date, reviewed and tested, at least once each year.
- Making sure that staff with Security Incident Response Plan responsibilities are properly trained, at least once each year.

- Leading the investigation of a suspected breach or reported security incident and initiating the Security Incident Response Plan, as and when needed.
- Reporting to and liaising with external parties, including the acquirer and card brands, legal representation, law enforcement, etc. as is required.
- Authorizing on-site investigations by appropriate law enforcement or payment card industry security/forensic personnel, as required during any security incident investigation. This includes authorizing access to/removal of evidence from site.

7.5.2.2 Security Incident Response Team (SIRT) members are responsible for:

- Making sure that all staff understand how to identify and report a suspected or actual security incident.
- Advising the Incident Response Lead of an incident when they receive a security incident report from staff.
- Investigating each reported incident.
- Taking action to limit the exposure of sensitive or payment card data and to reduce the risks that may be associated with any incident.
- Gathering, reviewing and analyzing logs and related information from various central and local safeguards, security measures and controls.
- Documenting and maintaining accurate and detailed records of the incident and all activities that were undertaken in response to an incident.
- Reporting each security incident and findings to the appropriate parties. This may include the Department of Education, card brands, vendors, business partners, students, etc., as required.
- Assisting law enforcement and card industry security personnel during the investigation processes. This includes any forensic investigations and prosecutions.
- Resolving each incident to the satisfaction of all parties involved, including external parties.
- Initiating follow-up actions to reduce likelihood of recurrence, as appropriate.
- Determining if policies, processes, technologies, security measures or controls need to be updated to avoid a similar incident in the future. They also need to consider whether additional safeguards are required in the environment where the incident occurred.

7.5.2.3 All staff members are responsible for:

- Making sure they understand how to identify and report a suspected or actual security incident.
- Reporting a suspected or actual security incident to the ITSA (preferable) or to another member of the Security Incident Response Team (SIRT);
- Reporting any security related issues or concerns to the ITSA, or to a member of the SIRT;
- Complying with the security regulations and procedures of Washburn University. This includes any updated or temporary measures introduced in response to a security incident (e.g. for business continuity, incident recovery or to prevent recurrence of an incident).

7.6 Incident Response Plan Steps

7.6.1 Report. Information security incidents will be reported, without delay, to the Incident Response Lead (preferable) or to another member of the Security Incident Response Team (SIRT). The member of the SIRT receiving the report will advise the Incident Response Lead of the incident.

In the event that a security incident or data breach is suspected to have occurred, staff members should discuss their concerns with the ITSA.

7.6.2 Investigate. After being notified of a security incident, the SIRT will perform an initial investigation and determine the appropriate response.

If the Security Incident Response Plan is initiated, the SIRT will investigate the incident and initiate actions to limit the exposure of data and in mitigating the risks associated with the incident.

7.6.3 Initial incident containment and response actions. Ensure that no-one can access or alter compromised systems.

- Isolate compromised systems from the network and unplug any network cables – without turning the systems off.
- If using a wireless network, change the SSID (Service Set Identifier) on the wireless access point and other systems that may be using this wireless network (but not on any of the systems believed to be compromised).
- Preserve all logs and similar electronic evidence, e.g. firewall logs, anti-virus tool, access control system, web server, application server, database, etc.

- Perform a back-up of applicable systems to preserve their current state – this will also facilitate any subsequent investigations.
- Keep a record of all actions performed by the SIRT.
- Monitor for further indications of compromise or suspicious activity in Washburn University environment, or that of third parties.
- Seek advice before processing any further payment transactions.
- Gather details of all compromised or potentially compromised payment card numbers, PII, etc. (the 'covered information').

7.6.4 Inform. Once the SIRT has carried out their initial investigation of the security incident:

- The Incident Response Lead will alert the SIRT's general counsel primary contact.
- The Student Aid Internet Gateway (SAIG) Agreement requires that as a condition of continued participation in the federal student aid programs, PSIs report actual data breaches, as well as suspected data breaches. Title IV PSIs will report on the day that a data breach is detected or even suspected.
- The Incident Response Lead and / or the SIRT personnel responsible for communications / PR will inform all relevant parties. This could include local law enforcement, State and Federals agencies, and other parties that may be affected by the compromise such as Washburn University students, partners or vendors.

7.6.5 Maintain Business Continuity. The SIRT will engage with operational teams in the organization to make sure that the University can continue to operate while the security incident is being investigated.

7.6.6 Resolve. The SIRT will work with external parties, including vendors, law enforcement, etc., to ensure appropriate incident investigation (which may include on-site forensic investigation) and gathering of evidence, as is required.

The members of the SIRT will take action to investigate and resolve the problem to the satisfaction of all parties and stakeholders involved. This will include confirmation that the required controls and security measures are operational.

The Incident Response Lead will report the investigation findings and resolution of the security incident to the appropriate parties and stakeholders as is needed.

7.6.7 Recovery. The Incident Response Lead will authorize a return to normal operations once satisfactory resolution is confirmed.

The SIRT will notify the rest of the business that normal business operations can resume. Normal operations will adopt any updated processes, technologies or security measures identified and implemented during incident resolution.

7.6.8 Review. The SIRT will complete a post-incident review after every security incident. The review will consider how the incident occurred, what the root causes were and how well the incident was handled. This will help to identify recommendations for better future responses and to avoid a similar incident in the future.

Changes and updates that may be required include:

- Updates to the Washburn University Security Incident Response Plan and associated procedures.
- Updates to Washburn University's security or operational policies and procedures.
- Updates to technologies, security measures or controls
- The introduction of additional safeguards in the environment where the incident occurred.

The ITSA will ensure that the required updates and changes are adopted or implemented as necessary.

7.7 Testing and Updates. Annual testing of the Incident Response Plan using walkthroughs and practical simulations of potential incident scenarios is necessary to ensure the SIRT are aware of their obligations, unless real incidents occur which test the full functionality of the process.

7.7.1 The Incident Response Plan will be tested at least once annually.

7.7.2 The Incident Response Plan Testing will test the organization's response to potential incident scenarios to identify process gaps and improvement areas.

7.7.3 The SIRT will record observations made during the testing, such as steps that were poorly executed or misunderstood by participants and those aspects that need improvement.

7.7.4 The Incident Response Lead will ensure the Security Incident Response Plan is updated and distributed to SIRT members.

8. Physical and Environmental Security Regulation

8.1 Purpose. This regulation defines the requirements for protecting Washburn University information technology resources from physical and environmental threats in order to reduce the risk of loss, theft, damage, or unauthorized access to those resources, or interference with Washburn University operations**.**

8.2 Scope. This regulation applies to all Washburn University colleges, departments, administrative units, and affiliated organizations that use university information technology resources to create, access, store or manage University Data to perform their business functions.

8.3 Regulation. All Washburn University information technology resources should have appropriate physical and environmental security controls applied commensurate with identified risks.

8.4 Definitions

8.4.1 Core network facilities. The cabling, equipment, and network/telecommunications rooms associated with the high-speed backbone of the Washburn University campus network that carries aggregated network traffic for all the buildings and external network connections.

8.4.2 Mobile storage devices. Any easily movable device that stores Washburn University data, including but not limited to laptop computers, smartphones, external hard drives, and USB flash drives.

8.4.3 Uninterruptable Power Supply (UPS). A device designed to provide power, without delay, during any period when the normal power supply is incapable of performing acceptably.

8.4.4 University Data. Any data related to Washburn University ("University") functions that are **a)** stored on University information technology systems, **b)** maintained by Washburn faculty staff, or students, or **c)** related to institutional processes on or off campus. This applies to any format or media (in other words, it is not limited to electronic data).

8.5 Roles and Responsibilities. Responsibility for physical and environmental security of Washburn University information technology resources is shared by the individuals using these systems, units that own them, and system administrators responsible for managing the systems.

8.6 Implementing Procedures

8.6.1 Physical Security

8.6.1.1 Network wiring and equipment – Network wiring and equipment rooms and cabinets will be locked when unattended with access limited to authorized personnel (typically network support staff) and visitors escorted by said authorized personnel. Other network cabling and devices should likewise be physically secured where feasible. Core network facilities should have the date and time of entry and departure recorded.

8.6.1.2 Office doors – All office doors should remain locked after hours or when offices are unattended for a prolonged period of time.

8.6.1.3 Mobile storage devices – Mobile storage devices should be stored securely when unattended. Appropriate secure storage methods include a locking security cable attached directly to the device, storage in a locked cabinet or closet, storage in a locked private office, or the like. Encrypting data stored on mobile devices, such as whole disk encryption on laptop computers, likewise reduces the risk of a breach of University Data resulting from theft, loss, or unauthorized access. When traveling with mobile storage devices or using them in public places, appropriate security precautions should be taken to prevent loss, theft, damage, or unauthorized access. Use of tracking and recovery software on laptop computers is encouraged.

8.6.2 Environmental Security.

8.6.2.1 Electrical power – Electrical power for servers hosting enterprise and departmental services will be protected by uninterruptable power supplies (UPS) to ensure continuity of services during power outages and to protect equipment from damage due to power irregularities. Each UPS should have sufficient capacity to provide at least 30 minutes of uptime to the systems connected to it. Systems hosting confidential data should also be protected with a standby power generator where feasible.

8.7 Questions/Waivers. The CIO is responsible for this regulation. The CIO or designee will approve any exception to this regulation or related procedures. Questions should be directed to the ITSA.

9. Collection, Use and Protection of Social Security Numbers

9.1 Purpose. Washburn University ("the University") is committed to protecting the privacy and confidentiality of personal information related to students, faculty, staff, and other individuals associated with the University. This regulation governs the collection, storage, use, and disclosure of Social Security Numbers (SSNs) at the University, consistent with federal and state laws and regulations and the increasing need to protect personal identity data. This regulation also authorizes the creation of alternative methods of identification that will reduce reliance on the SSN, allow for easy identification of a person for University transactions, and provide for linking an individual's personal information and records in various university information systems.

9.2 Scope. This regulation applies to all Washburn University colleges, departments, administrative units, and affiliated organizations. For the purposes of this regulation, affiliated organization refers to any organization associated with the University that uses university computer network resources to create, maintain, or store data to perform their business functions.

9.3 Objectives. In issuing this regulation, the University is guided by the following objectives:

9.3.1 Broader awareness of the confidential nature of the SSN and the risk of identity theft related to unauthorized disclosure.

9.3.2 Reduced collection of SSNs except where authorized by law.

9.3.3 Reduced use of the SSN in records and information systems, including display screens and printed reports.

9.3.4 Reduced electronic storage of SSNs to a minimum number of locations.

9.3.5 Consistent policies regarding the collection, storage, use, and disclosure of SSNs throughout the University.

9.3.6 Increased confidence by students, employees, and affiliates/guests that their SSNs are handled in a confidential manner.

9.4 Regulation. Use of the SSN as an identifier will be discontinued, except where authorized for employment, IRS reporting, federal student financial aid processing, state and federal reporting requirements, and a limited number of other business transactions. (See Appendix A below for a list of currently approved uses of the SSN.) While the SSN will continue to be collected and retained as authorized by law, it will not be used for routine identification or authentication purposes. A unique nine-digit Washburn Identification Number (WIN) will be permanently assigned to each individual associated with the University as a personal identifier alternative to the SSN. The WIN will begin with a "W" to prevent confusion with an SSN.

9.5 Implementing Requirements

9.5.1. Washburn University prohibits the use of a person's SSN as a publicly visible identification number for University-related transactions, unless specifically required by law or business necessity.

9.5.2 Each member of the University community will be assigned a unique identification number that will not be the same as nor derived from the individual's SSN. This number is called the WIN. The WIN will be printed on University photo ID cards.

9.5.3 For computer access or sign-in purposes, University students, faculty, staff, and others will use their WIN in combination with a password. The WIN will be used as the standard identifier for all computer resource authentication purposes.

9.5.4 SSNs will not be used for identification purposes unless required by law or internal university business necessity. For business processes that require an SSN, the last four digits of the SSN may be used to confirm the identity of an individual.

9.5.5 Academic records, such as grades, and other pieces of personal information will not be publicly posted or displayed with the SSN or any portion of the SSN.

9.5.6 Any University office that requests an SSN from an individual will indicate if it is voluntary or required. The request should include or be accompanied by a disclosure statement approved by the University Data Administrator. Disclosure statements should state under what authority and why the SSN is being requested, how the number will be used, and to whom it can be disclosed.

9.5.6.1 An SSN can only be used for the purpose it was collected.

9.5.7 Systems developed or purchased the University after the effective date of this regulation shall comply with the provisions of this regulation. Such systems will not collect SSNs, or display SSNs visually, whether on monitors, printed

forms, hardcopy reports, or other system output, unless required by law or business necessity. See Appendix A for further information.

9.5.8 In the transition to one location for the SSN, university systems may use the SSN as a data element, but not as a key for access to databases. In exceptional circumstances, it may be necessary to use the SSN as an alternative search field. All such cases shall be approved by the ITSA, who shall seek recommendations from the data owner.

9.5.9 When a business process requires the SSN, it will be stored in a secure manner. The SSN shall not be stored on devices that are not secured (e.g., laptops, thumb drives, CDs). Any transmission of data containing SSNs will be encrypted over any communication network.

9.5.10 Any University department or office that collects and/or maintains an individual's SSN in either paper or electronic media will: 1) ensure that the number is stored in a secure and confidential environment; 2) eliminate using the number for any purpose except those specifically addressed in this regulation; 3) begin a steady and purposeful movement away from dependency on the SSN in performing its functions and processes; 4) properly control and restrict access to SSNs to prevent unauthorized disclosure; and 5) properly erase or destroy the storage devices or printed documents that contain SSNs to ensure the information cannot be recovered or reconstructed.

9.6 Legacy Data. The University recognizes that the SSN will be retained and used as a person identifier in information systems containing older "legacy" data pertaining to ex-students, ex-faculty or staff, or others formerly associated with the university. It is impractical to assign WIN numbers to these individuals.

9.7 Related Laws, Regulations and Policies. A variety of federal and state laws and regulations address the use of the SSN. These include the Privacy Act of 1974, the Family Education Rights and Privacy Act (FERPA), Gramm-Leach-Bliley Act, Health Insurance Portability and Accountability Act (HIPAA), and Kansas Statues Annotated, 76-768.

9.8 Questions. The CIO is responsible for this regulation.

9.9 Appendix: Approved Uses for Social Security Numbers (SSN). This Appendix is considered to be part of this regulation (Collection, Use, and Protection of Social Security Numbers).

The SSN is required for certain legal and business activities and to ensure the accuracy of inter-institutional data exchanges and communications between institutions involved in those activities. Approved uses of the SSN by the University are listed below.

9.9.1 Employment: The SSN is required for a variety of employment matters; such as proof of citizenship, tax withholding, FICA, or Medicare.

9.9.2 Application and Receipt of Financial Aid: Students applying for student aid using the federal Free Application For Student Assistance (FAFSA) are required to provide SSNs. Students are also required to provide SSNs when applying for student education loans.

9.9.3 Tuition Remission: The SSN is required for state reporting of taxable tuition remission benefits received by employees, their spouses and dependents, and by graduate assistants.

9.9.4 Benefits Administration: The SSN is often required for verifying enrollment, processing, and reporting on various benefit programs, such as medical benefits, health insurance claims and veterans' programs.

9.9.5 Insurance: SSN will be needed to file insurance claims through Washburn benefits center.

9.9.6 IRS Reporting: The SSN is used for federally required reporting to the IRS. For example, the University reports the value of all taxable and non-taxable scholarships and grants awarded to non-resident aliens to the IRS.

9.9.7 Student Information Exchange: Many institutions, including postsecondary educational institutions, use the SSN as a student identifier. The SSN may be used for the exchange of information from student academic records between appropriate institutions, including other colleges and universities or certification and licensure programs.

10. Media Sanitization and Disposal Regulation

10.1 Purpose. The purpose of this regulation is to protect Washburn University Data from unauthorized disclosure. This regulation defines the requirements for ensuring University Data are permanently removed from media before disposal or reuse, a process called "media sanitization," and properly disposing of media. The reuse, recycling, or disposal of computers and other technologies that can store data pose a significant risk since data can easily be recovered with readily available tools - even data from files that

were deleted long ago or a hard drive that was reformatted. Failure to properly purge data in these circumstances may result in unauthorized access to University Data, breach of software license agreements, and/or violation of state and federal data security and privacy laws.

10.2 Scope. This regulation applies to all Washburn University colleges, departments, administrative units, and affiliated organizations.

10.3 Regulation. To prevent unauthorized disclosure of Washburn University Data, media leaving control of the responsible department and destined for reuse or disposal will have all University Data purged by ITS in a manner that renders the data unrecoverable.

Media that will be reused within the department should likewise have all University Data purged to prevent unauthorized disclosure.

Media containing University Data authorized by the appropriate administrative head for transfer to individuals or organizations outside the University are exempt.

10.4 Definitions

10.4.1 Affiliated Organization. Any organization associated with the University that uses university information technology resources to create, access, store or manage University Data to perform their business functions.

10.4.2 Confidential Data. Highly sensitive University Data intended for limited, specific use by a workgroup, department, or group of individuals with a legitimate need-to-know.

10.4.3 DeGaussing. Demagnetizing magnetic storage media like tape or a hard disk drive to render it permanently unusable. Since the media typically can no longer be used after degaussing, it should only be used to purge data from media that will be discarded.

10.4.4 Disintegration. A physically destructive method of sanitizing data; the act of separating into component parts.

10.4.5 HIPAA. Health Insurance Portability and Accountability Act of 1996 that among other things established standards for the security and privacy of human health-related information.

10.4.6 Incineration. A physically destructive method of sanitizing media; the act of burning completely to ashes.

10.4.7 Internal Data. Washburn University Data intended for internal University business use only with access restricted to a specific workgroup, department, group of individuals, or affiliates with a legitimate need.

10.4.8 Media. Material on which data are or may be recorded, such as magnetic disks or tapes, solid state devices like USB flash drives, optical discs like CDs and DVDs, or paper-based products.

10.4.9 Media sanitization. The process of removing data from storage media such that there is reasonable assurance that the data may not be retrieved and reconstructed.

10.4.10 Public Data. University Data explicitly or implicitly approved for distribution to the public without restriction.

10.4.11 Pulverization. A physically destructive method of sanitizing media; the act of grinding to a powder or dust.

10.4.12 Purging. A media sanitization process that removes all data and any remnant of the data so thoroughly that the effort required to recover the data, even with sophisticated tools in a laboratory setting (i.e., a "laboratory attack"), exceeds the value to the attacker. A common method of purging data is to overwrite it with random data in three or more passes.

10.4.13 University Data. Any data related to Washburn University ("University") functions that are a) stored on University information technology systems, b) maintained by Washburn faculty staff, or students, or c) related to institutional processes on or off campus. This applies to any format or media (in other words, it is not limited to electronic data).

10.5 Roles and Responsibilities. ITS is responsible for ensuring that University Data are properly removed or destroyed from media before it leaves the control of the department for reuse or disposal.

10.6 Implementation Procedures. While the primary purpose of this regulation is to protect non-public University Data (e.g., data classified either internal or confidential), it is often very difficult to separate these classifications from public or personal data on the media, or determine conclusively that remnants of non-public data are not recoverable.

Therefore, it is often most expedient and cost effective to purge all University Data from the media before reuse or disposal rather than try to selectively sanitize the sensitive data.

Likewise, it is often most cost effective to physically destroy the media rather than expend the effort to properly purge data. However, if physical destruction is contracted to a third party outside the University, all University Data will be purged from the media by ITS before giving it to the third party.

Specific instructions for different types of media and regulations follow:

10.6.1 Electronic Storage Media (hard disk drives in computers, external hard drives, USB flash drives, magnetic tapes, etc.)

10.6.1.1 If purging is done by overwriting the data, the entire media/device will be overwritten with a minimum of three passes.

10.6.1.2 Equipment that can store University Data, such as desktop and laptop computers or external hard drives, and is permanently leaving the control of the University should have all data storage devices removed before disposition. If the equipment leaving University control will retain the data storage devices, all University Data will be properly purged by ITS.

10.6.1.3 The only acceptable methods for physically destroying a hard drive are shredding, pulverizing, disintegration, or incineration.

10.6.1.4 Degaussing is an acceptable method of purging data from magnetic media. Be aware that this normally renders the media unusable.

10.6.2 Paper-Based Media

10.6.2.1 Any paper-based or other hard copy media containing confidential University Data will be shredded with a cross-cut shredder before disposal or transferred to an authorized third party contracted by the University for secure disposition of documents. The maximum particle size for paper-based media containing confidential data should be 1x5 mm (1/32"x1/5"). Media containing internal data should likewise be shredded with a cross-cut shredder if disclosure of the information contained therein might adversely impact the institution, an affiliated organization, or an individual. The maximum particle size for media containing internal data is 2x15 mm (1/16"x3/5").

10.6.2.2 Incineration by methods compliant with all relevant health, safety, and environmental laws and regulations is an acceptable method for disposal of paper-based media.

10.6.3 Optical Media (e.g., CDs and DVDs). Optical media containing internal or confidential University Data will be physically destroyed before disposal. An appropriate method of physical destruction is shredding with a cross-cut shredder.

10.6.4 Smartphones and other handheld devices. Mobile devices like Smartphones (e.g., iPhones, Androids), MP3 players, and even cell phones, store information and often contain personal or other sensitive information. Any University Data will be purged from these devices by ITS before reuse or disposal, like any other storage media. It is also advisable to purge all other data from the device before reuse or disposal to protect your personal information.

10.6.5 Other Media Types. For other media and additional guidelines, refer to NIST Special Publication 800-88, Revision1: Guidelines for Media Sanitization

10.6.6 Export controls. Media containing University Data in equipment that will be reused outside the United States will comply with export laws and regulations.

10.6.7 Electronic Protected Health Information. Washburn University units responsible for electronic protected health information covered by HIPAA will also have media sanitization and disposal policies and procedures in accordance with HIPAA Security Final Rules, Section 164.310, Physical Safeguards, part (d), (1) & (2).

10.6.8 Federal Tax Information. Washburn University units handling Federal Tax Information will also have media sanitization and disposal policies and procedures in accordance with IRS Publication 1075: Tax Information Security Guidelines for Federal, State, and Local Agencies.

10.7 Questions/Waivers. The CIO is responsible for this regulation. The CIO or designee will approve any exception to this regulation or related procedures. Questions should be directed to the ITSA.