BOWIE STATE UNIVERSITY 1865	https://www.bowiestate.edu/about/administration-and-governance/division-of-information-technology/security-and-compliance/

Information Security Program

Program Overview #	1.0	Effective Date	04-2014	Email	infosec@bowiestate.edu
Version	1.5	Contact		Phone	TBD
BSU Policies	Section X :15.09; 15.10; 15.11; 15.12; 15.13; 15.14; 15.21; 15.22; 15.23; 15.24				
Standards/Regulations Addressed	Standards/ Regulations	Controls			
	USM Security Standards v4	NIST 800-53 specific controls cited in specific rules and procedures.			

Table of Contents

SUMMARY

Information systems provide a foundation of technology for Bowie State University (BSU) business activity that utilizes university-owned data. This program defines methods, rules, procedures, and other requirements necessary for the secure and reliable operation of the BSU information systems and network infrastructure. The standards for information security contained in this document are best practice and are rooted in the University System of Maryland (USM) Security Standards and the National Institute of Standards and Technology (NIST) Cybersecurity Framework. Legislative controls contained in FERPA, PIPA, and Gramm-Leach Bliley laws are included as well.

Care was taken to communicate technical concepts in plain English, avoiding technical terms and acronyms where possible. The document audience is all BSU employees and business partners. Examples and details designed to illustrate why information security is important are presented. We hope to encourage understanding and improve awareness of information security across the many groups of Users with varying degrees of education that comprise the BSU family.

This document provides a definitive statement of information security policies and practices to which all employees are expected to comply. It is intended to:

- Acquaint employees with information security risks and the expected ways to address these risks.
- Clarify employee responsibilities and duties with respect to the protection of information resources.
- Enable management and other employees to make appropriate decisions about information security.
- Coordinate the efforts of different groups within the University so that information resources are properly and consistently protected, regardless of their location, form, or supporting technologies.

Everyone recognizes that a highway system and motor vehicles are essential to commerce. People now appreciate how information systems made up of computers and networks are another infrastructure essential to commerce. Just as every driver has a role to play in the orderly and safe operation of the transportation infrastructure, there are information security roles and duties for every employee at BSU. For example, it is a driver's duty to report accidents, and it is an employee's duty to report information security problems. Just as car manufacturers are required to provide safety belts with vehicles, system designers at BSU are required to include necessary security measures such as user access restrictions based on job function and the need to know.

This document defines baseline control measures in a program of information security everyone who connects to the BSU network is expected to be familiar with and to follow consistently. Sometimes called the "standard of due care controls", these security measures are the

minimum required to prevent a variety of problems including, but not limited to:

- theft,
- fraud and embezzlement,
- research raiding and espionage,
- sabotage,
- errors and omissions,
- system unavailability, and
- loss of confidence and damage to reputation.

The BSU Policies citations listed in the table above define general University goals, expectations, and responsibilities concerning technology use. The BSU Policies and the DIT rules define the minimum controls necessary to prevent legal problems such as an allegation of negligence, breach of fiduciary duty, or a privacy violation. This document contains DIT rules that detail both reasonable and practical ways for all of us at BSU to avoid risk and prevent unnecessary losses.

BSU critically depends on continued citizen confidence. This confidence has gradually increased over many years of dedicated effort by BSU students, faculty, staff, and leadership. While confidence takes many years to earn, it can be rapidly lost due to problems such as denial of service attacks that disrupt the educational process, system outages that stop intra-university communication, or the theft of unsecured personally identifiable information (PII) resulting in potential identity theft. The trust that the community we serve has in the University is a competitive advantage that must be continuously nurtured and grown. This information security initiative is designed to protect these efforts.

MANAGEMENT SUPPORT FOR INFORMATION SECURITY

Critical Education Business Function – Information is a foundation of higher education and research. The information carried in the BSU network and information systems: the data, hardware, software and people that use them are necessary for the performance of almost every essential activity at the University. If there were a serious security problem with this information or information systems, BSU could suffer serious consequences including loss of current and prospective student enrollment, reduced revenues, and degraded reputation. As a result, information security now must be a critical part of the BSU business environment.

Supporting Educational Mission and Business Objectives - This document outlines information security requirements prepared to ensure that BSU can support further growth of the University and support a consistently high level of service to our constituents. In addition, the document is intended to support BSU's reputation for providing high quality and affordable educational opportunities for a diverse student population of Maryland citizens and the global community through the effective and efficient management of its resources. Because the prevention of security issues is considerably less expensive than correction and recovery, this document will help reduce the overall cost of University operations.

Consistent Compliance Essential - A single unauthorized exception to information security measures can jeopardize the entire university community, our business partners and even our educational partners in the University of Maryland System (USM). The interconnected nature of information systems requires that all employees observe a minimum level of security. This

document defines that minimum level of due care. In some cases, these requirements will conflict with other objectives such as improved efficiency and minimized costs. Management has examined these trade-offs and has decided that the minimum requirements defined in this document are appropriate for all employees at BSU. As a condition of continued employment, all employees, contractors, consultants, and temporaries, must consistently observe the requirements outlined in this document.

BSU Team Effort Required - The tools available in the information security field are relatively unsophisticated. Many of the needed tasks cannot be achieved with products now on the market. This means that users at BSU must step in and play an important role in the information security. Information and information systems are distributed to the office desktop and are used in remote locations; the employee's role has become an essential part of information security. Information security is no longer the exclusive domain of the Division of Information Technology. Information security is now a team effort requiring the participation of everyone who encounters BSU information or information systems.

INFORMATION SECURITY ROLES AND RESPONSIBILITIES

Information Security Committee – The committee provides oversight and advice regarding information systems security and privacy assurance for BSU. Committee members include subject matter experts in information security and assurance. Members are designated by the Division of Information Technology (DIT) Vice President/Chief Information Officer (CIO) to provide advice for CIO specific responsibilities that include:

- The development, implementation, and maintenance of a University-wide strategic information systems security plan.
- The development, implementation, and enforcement of University-wide information systems security program and related recommended guidelines, operating procedures, and technical standards.
- The process of handling requested program exceptions, advise the University administration on risk related issues and recommend appropriate actions in support of the University's larger risk management programs.
- To ensure related compliance requirements are addressed, e.g., privacy, security, and administrative regulations associated with University System of Maryland (USM), Federal, and Maryland laws.
- Ensure appropriate risk mitigation and control processes for security incidents.

Information Owners – The Division Vice President is or designates top-level managers in each University area as the Owners of all types of information used for area business activities. Each type of system information must have an Owner. When information Owners are not clearly identified by appointment or organizational design, the Chief Information Officer must make a temporary designation (until the area Vice President can appoint a designee). Information Owners do not legally own information all university information belongs to the institution. They are instead members of the BSU management team who make decisions on behalf of the University. Information Owners or their delegates must make the following decisions and perform the following activities:

- Formulate specific job function profiles that will be granted access to University information.

- Determine the proper access based on job function profiles and determine the proper use of University information.
- Approve information-oriented access and control privileges for specific job function profile.
- Approve information-oriented access control requests that do not fall within the scope of existing job function profiles.
- Select a data retention period for their information.
- Designate original sources for information.
- Employ special controls needed to protect information, such as additional input validation checks at the data point of entry or indicate more frequent backup procedures.
- Define acceptable limits on the quality of their information, such as accuracy, timeliness, and time from capture to usage.
- Approve all new and different uses of their information.
- Approve all new or substantially enhanced application systems that use their information before these systems are moved into production operational status.
- Review reports about system intrusions and other events that are relevant to their information.
- Review and correct current production use of their information.
- Select a sensitivity classification category relevant to their information with the consultation of the BSU General Counsel, and review classifications every five years.
- Select a criticality category relevant to their information with the consultation of the Enterprise IT Security Department so that appropriate safeguards and contingency planning can be performed.

Information Owners must designate an alternative person to act if they are absent or unavailable. Owners may not delegate ownership responsibilities to third-party organizations such as outsourcing organizations, or to any individual who is not a full-time BSU employee. When both the Owner and the alternative back-up Owner are unavailable, the Department Manager, who ordinarily supervises the handling of information may make immediate Owner decisions (and seek the Information Owners subsequent approval).

Data Stewards (aka Application User Coordinators) **are Employee's Immediate Manager** – Information Stewards must make the following decisions and perform the following activities:

- Review and correct security reports that indicate those users who currently have access to university information within their department.
- Authorize new users to access university information and de-authorize users who no longer fit a job function profile.
- Supervise department employee use of university information under their control.
- In conjunction with the DIT, ensure that user access rights are appropriately reviewed and modified for transferred employees

The employee's immediate manager is the Data Steward, who must approve a request for system access based on existing job function profiles. If a job function profile does not exist, it is the manager's responsibility to create the function profile, obtain the approval of relevant Owners, and inform Human Resources and Enterprise IT Security Departments.
When an employee leaves BSU, it is the responsibility of the employee's immediate manager to promptly inform the Human Resources Department and Enterprise IT Security Departments that the privileges associated with the employee's user ID must be revoked. User IDs are specific to individuals, and must not be reassigned to, or used by, others.

Data Custodians - Custodians are DIT information technology specialists: database administrators; system administrators; and functional analysts who physically or logically access information and administer information systems. Like Owners, Custodians are specifically designated for different types of information. In many cases, a manager in DIT will act as the Custodian. If a Custodian is not clear, based on existing information systems operational arrangements, then the Chief Information Officer will designate a temporary DIT Custodian. Custodians follow the instructions of Owners, operate systems on behalf of Owners, but also serve users authorized by Owners. Custodians must define the technical options, such as systems criticality categories, and permit Owners to select the appropriate option for their information. Custodians also define information systems architectures and provide technical consulting to Owners so that information systems are built and run to best meet the University Mission. If requested, Custodians additionally provide reports to Owners about information system operations and information security problems. Custodians are responsible for safeguarding the information in their possession. This includes implementing access control systems to prevent inappropriate disclosure, as well as developing, documenting, and testing information systems contingency plans.

Information Users –
There are two types of Users:
General Users are not specifically designated but are broadly defined as any person who accesses the BSU network.
Departmental Data Users are employees or contractors and consultants with access to internal information or internal information systems.

All Users are required to follow all security requirements defined by Owners, implemented by Data Stewards and Custodians, or established by the Enterprise IT Security Department. All Users must familiarize themselves with, and act in accordance with, BSU information security requirements. Users also must complete information security awareness training. Users must request access from their immediate manager, and report all suspicious activity and security problems.

Enterprise IT Security Department - The Enterprise IT Security Department is the central point of contact for all information security matters at BSU. Acting as internal technical and policy consultants, it is this department's responsibility to create workable information security compromises that take into consideration the needs of Users, Custodians, and Owners, while supporting the University Strategic Plan and Mission. Reflecting these compromises, fulfilling goals set by USM Security Standards and BSU Policy, this department defines specific information security standards, procedures and controls for the University. Enterprise IT Security Department must:

- perform access control administration activities,
- documentation updates and monitor the security program,
- monitor the security of BSU information systems, and
- provide information security training and awareness programs to BSU employees.

The department is responsible for providing management with reports about the current state of information security at BSU. In this regard, Enterprise IT Security Department conducts an annual risk analysis report.

While information systems contingency planning is the responsibility of information Custodians, the Enterprise IT Security Department must provide technical consulting assistance related to emergency response procedures and disaster recovery. The Enterprise IT Security Department is also responsible for organizing a computer incident response team to respond promptly to virus infections, system break-ins, system outages, and similar information security problems.

INFORMATION SENSITIVITY CLASSIFICATION

Reasons For Classification - As a member of the University System of Maryland (USM) and a state university, BSU takes seriously its commitment to respect and protect the privacy of its students, alumni, faculty and staff, as well as to protect the confidentiality of information important to the University's academic mission. BSU classifies its information assets into categories for the purpose of determining who is allowed to access the information and what security precautions must be taken to protect it against unauthorized access.

To assist the appropriate handling of information, a sensitivity classification hierarchy must be used throughout BSU. This hierarchy provides a shorthand way of referring to sensitivity, and can be used to simplify information security decisions and minimize information security costs. One important intention of a sensitivity classification system is to provide consistent handling of the information, no matter what form it takes, where it goes, or who possesses it. For this reason, it is important to maintain the labels reflecting sensitivity classification categories. BSU uses four sensitivity classification categories:

Public – This type of information is specifically approved for public release by the University Relations Department. Unauthorized disclosure of this information will not cause problems for BSU, its customers, or its business partners. Examples are marketing brochures, an academic catalog, material posted on the BSU website, and BSU departmental phone numbers.

Internal - This information is not approved for public release. Unauthorized disclosure of this information to outsiders may affect University interests. Examples are employee office phone numbers, employee email addresses, and office manuals. This type of information is already widely distributed within BSU, or it could be distributed within the organization without advance permission from the information Owner.

Confidential - This information is *sensitive* intended for use within BSU, and in some cases within affiliated organizations, such as BSU partners. Unauthorized disclosure of this information to outsiders may be against laws and regulations, or may cause problems for BSU, its customers, or its business partners. Example: student information (protected by FERPA) and employee performance evaluation records.

Restricted - This information is *sensitive* private or otherwise sensitive in nature and must be restricted to those with a legitimate business need for access. Unauthorized disclosure of this information to outsiders may be against laws and regulations, or may cause problems for BSU, its customers, or its business partners. Decisions about the provision of access to this information must be cleared through the information Owner. Examples are real estate acquisition plans, potential employee negociations and legal information protected by attorney-client privilege.

Default Category - If information is not marked with one of these categories, it should be considered Confidential. Information that falls into the Confidential or Restricted, categories is designated Sensitive.

Labeling - The Owner or Creator of information must designate an appropriate label, and the user or recipient of this information must consistently maintain an assigned label. Labels for sensitive information must be used in the subject field of electronic mail messages or paper memos. Labels for sensitive information must appear on the outside of floppy disks, magnetic tape reels, CD-ROMs, audio cassettes, and other storage media. If a storage volume such as a disk contains information with multiple classifications, the most sensitive category should appear on the outside label. Likewise, when creating a collection of information from sources with various classifications, the collection must be classified at the highest sensitivity level of the source information.

Handling Instructions - All users must observe the requirements for handling information based on its sensitivity. For more information on these definitions, see the BSU Data Classification Quick Reference Table. Owners may designate additional controls to restrict further access to, or to protect further university information under their control.

ACCESS CONTROLS

Network Access Philosophy – The BSU network is a system of hardware components: computing devices, routing devices, switching devices, fiber optic and copper cables, etc. that transmit all types of information in the form of data bits. BSU must protect this equipment and the information it transmits by limiting access to network users who have been trained in and agree to, its proper use. The training required for network access is information security awareness training approved by the IT Enterprise Security Department. BSU Policy recognition is also required before network access is granted.

Network Access Approval Process – The Human Resources Department (HR) must initiate the network access control approval process for all new employees. These steps are required for network access:

1. HR determines that a new employee has been hired by a department and enters the employee information into PeopleSoft application database.
2. The new employee is given a BSU network account and email account based on the employee job function. DIT assigns the standard basic information security awareness training based upon position/role.
3. The new employee completes awareness training each semester in a continuous program of awareness training.

Information Access Philosophy - Access to “Public” information is not restricted by access controls. For example, “Public” information is available on the BSU website, and “Internal” information is available on the BSU intranet. Access to “Confidential” and/or “Restricted” information must be granted only when a legitimate business need has been demonstrated, and job function profile access has been approved in advance by the information Owner.

Information Access Approval Process - An employee's manager must initiate the access control approval process, and the privileges granted remain in effect until the employee's job function profile changes or the employee leaves BSU. If either of these two events occur, the manager must notify the Human Resources Department who confirms the employee status to DIT. Additionally, for the PeopleSoft application (Campus Solutions and Financials) an employee job function profile change or employee separation must be reported to PeopleSoft Enterprise Security Analyst in the Functional Support Team.
The Human Resources Department and IT Enterprise Security Department must approve all non-employees, contractors, consultants, for temporary access to the BSU network.

Departures From BSU - When a user leaves BSU, all system privileges and access to BSU information must cease immediately. For example, departed users must not be permitted to continue to access the BSU network. At this point, all BSU information disclosed to users must be returned. For example, contact lists must remain with BSU. All work done by users for BSU is BSU property, and it too must remain with BSU when users depart. For example, a computer program component written by a member of the PeopleSoft Applications department while employed by BSU is BSU property and must remain with BSU.

Unique User IDs - Each user must be assigned their own unique user ID. This user ID follows an individual as they move through the University. It must be permanently decommissioned when a user leaves BSU. Re-use of user IDs is not permitted. Every user ID and related password are intended for the exclusive use of a specific individual. While user IDs can be shared in electronic mail messages and other places, *passwords must never be shared with anyone*. Information systems technicians have all the privileges they need to do their job, and must never obtain a user's password. User IDs are linked to specific people and are not associated with computer terminals, departments, or job titles. With the exception of Internet pages, intranet pages, and other places where anonymous interaction is both generally understood and expected, anonymous and guest user IDs are not permitted unless approved in advance by the Enterprise IT Security Department.

Privilege Deactivation - After a period of no activity defined in minutes by the Enterprise IT Security Department, online sessions with multi-user machines must be terminated automatically. Users must be sure to log-off from multi-user computers when they leave their desks for more than a few minutes. Dormant user IDs on multi-user computers that have no activity for a period defined in weeks by the Enterprise IT Security Department must have their privileges automatically revoked. Users of multi-user machines should not leave files on these machines as they may be deleted at any time.

User Authentication - All PeopleSoft information system user IDs must have a linked password or a stronger mechanism such as a dynamic password token, to ensure that only the authorized user can utilize the user ID. Users are responsible for all activity that takes place with their user ID and password or another authentication mechanism. A user must change their password immediately if they suspect that it has been discovered or used by another person. Users must notify the Enterprise IT Security Department if other access control mechanisms are broken or if they suspect that these mechanisms have been compromised.

Remote Access – Remote access connections are protected with recommended security controls. These controls include encrypting data while it's in transit.

Remote access shall only be allowed using approved Virtual Private Network (VPN) systems.

Audit Capabilities - Access control systems must be configured to capture significant actions in critical applications. Such significant actions include actions performed by administrative level accounts, additions and changes to critical applications and user's access control profiles, and direct modifications to critical data outside of the application.

NETWORK TOOLS MANAGEMENT

5.4 Network Tools Management – Based on system sensitivity and data classification, BSU networks are protected by firewalls at identified points of interface. Unnecessary services, protocols, and ports shall be disabled on firewalls, switches and routers, (and other network devices as applicable) to reduce BSU's attack surface. Direct access to host on BSU's networks shall be based on Access Control Lists (ACL) and comprehensive audit trails shall be maintained. Access to manage the firewall shall be restricted to approved personne and encypted. The dafault administrator credentials must be changed when possible to reduce the risk of an account compromise of the administrator accounts. Network tools shall also be patched and updated according to BSU's Vulnerability and Change Management policy.

Network tools shall be configured in such a way that it doesn't degrade network performance, and/or cause unauthrized network traffic flows.

VULNERABILITY MANAGEMENT

Vulnerabilities on BSU's networks shall be managed according to the Vulnerability and Change Management policy.

System and Information Integrity - Intrusion detection and prevention systems shall be utilized to monitor network traffic at BSU and BSU devices, especially on critical systems. BSU systems shall have anti-malware tools (where possible) to protect against malicious code, and to maintain the confidentiality, availability, and integrity of the system and the information stored and processed on it. These tools shall be used to scan devices for abnormal files on a regular basis, and the detection signatures shall be updated on a regular basis. Such tools shall be managed by appropriate authroized personnel only and configured in such a way that they cannot be disabled by users without priviledges to do so, and disabled anti-malware tools shall have a business justification.
Systems shall be configured to send alerts to system administrators when an intrusion has been detected enabling authorized personnel to ensure vulnerable systems are quickly and properly remediated when possible.

PASSWORD MANAGEMENT

Choosing Passwords - Users must choose difficult-to-guess passwords. Fixed passwords must not be found in the dictionary and must not be a reflection of the user's personal life. All fixed passwords must be at least 8 characters, and this minimum length must be enforced automatically where systems support it. Users must choose fixed passwords that include both alphabetic and numeric characters.

Changing Passwords - User-chosen fixed passwords must not be reused or recycled. Where systems support it, fixed passwords must be required to change every 90 days and passwords must be changed the first time they are used. If a user suspects that somebody else may know his or her password, the password must be changed immediately. The DIT Help Desk will not reset user passwords unless the user can establish their identity. Presenting a valid government ID and BSU ID is sufficient proof of identity.

Protecting Passwords - Users must not share a fixed password with anyone, including managers, support technicians, and co-employees. Authorized mechanisms to share information such as local BSU network server shared directories, BSU electronic mail, or BSU intranet pages. Passwords must not be stored in any computer files, login scripts or computer programs unless the passwords have been encrypted. Passwords must not be written down unless a transformation process has concealed them, or they are physically secured, such as placed in a locked file cabinet. All default passwords set by the hardware or software vendor must be changed before the involved system can be used for BSU business activities.

A management tool enforces these rules - it is transparent to the end user.

PRIVACY

Expectations Of Privacy - Users must have no expectation of privacy when using the university network. To manage systems and enforce security, BSU may monitor, log, review, and otherwise utilize any information stored on or passing through its systems.

Information Privacy - A wide variety of parties have entrusted their information to BSU for business purposes, and all employees at BSU must do their best to safeguard the privacy and security of this information. Student and patient as well as employee account data are Sensitive (Confidential or Restricted), and access must be strictly limited based on business need for such access. Private information must not be released without advance written authorization of the individual.

An important exception to this rule is that human life must always be preserved.

Laws may provide other exceptions: Teachers, health care providers, emergency responders, and law enforcement are examples of job function profiles exempted in certain circumstances.

One example of a business purpose is a faculty member’s need to access a student academic record to provide informed counseling to the student.

THIRD-PARTY / DISCLOSURES

Preauthorization For Official BSU Public Statements - All employees who will be delivering official information representing BSU must obtain preauthorization from the University Relations Department. Only designated individuals are authorized to be official spokespersons for BSU. Unless an employee is one of these designated spokespersons, all inquiries from the media should be directed to University Relations.

BSU Non-Disclosure Agreements - Whenever communications with third parties necessitate the release of sensitive BSU information, the third party must sign a standard non-disclosure agreement (NDA). Information released to these third parties must be limited to the topics directly related to the involved project or business relationship, and the disclosure must be approved in advance by the involved information Owner.

Third-Party Non-Disclosure Agreements - In some instances, before discussions can be commenced, third parties must require that employees at BSU sign their non-disclosure agreements (NDAs). Recipients of third-party NDAs must forward these agreements to the BSU General Counsel for review and approval.

ACCEPTABLE USE OF THE INTERNET

Not A Fringe Benefit - Internet access and electronic mail are tools provided to students and employees to conduct university business, scholarly activity, and academic research.

Information Reliability - All information acquired from the Internet must be considered suspect until confirmed by separate information from a reliable source. Users must not rely on the alleged identity of a correspondent through outside email or the Internet. The identity of a person or organization is confirmed through authoritative methods such as digital certificates granted by third party verification or digital signatures. More information can be obtained from the Enterprise IT Security Department.

Downloading Software - Users must not install software from the Internet unless specifically authorized to do so by the Information Systems or Enterprise IT Security Department. Users may download data files from the Internet, but must check these files for viruses before using them. Copyright laws must be respected when downloading files.

Sending Security Parameters - Users must not send any sensitive parameters such as credit card numbers, telephone calling card numbers, fixed passwords, or account numbers over the Internet unless the connection is encrypted end-to-end.

International Transfer Of Data - The movement of private or research information such as human resources records or sensitive research across international borders in some countries is illegal. Before transferring any private or sensitive research information across a border, users must check with the BSU General Counsel to ensure that laws are not violated.

Setting Up Extra Services - The establishment of any connection to the BSU network with a third party is forbidden unless the Enterprise IT Security Department has approved the controls associated with this connection. The establishment of electronic data interchange and other electronic business system arrangements is prohibited unless approved by both Enterprise IT Security Department and Information Systems Department.

Information Security Reports - All users in receipt of information about system vulnerabilities must forward this information to the Enterprise IT Security Department, which will determine what action is appropriate. Users must not redistribute system vulnerability information.

ESTABLISHING NETWORK CONNECTIONS

Banner Text – BSU devices shall display banner text upon initial logon to system. Banner texts shall inform the user that access to the system is monitored, and unauthorized access to the system is strongly prohibited. The banner text displayed must be that represented in the State of Maryland's Information Security Policy or language that has been reviewed and approved by the General Counsel.

Connection Approval Required - BSU computers or networks may be connected to third-party computers or networks only after the Enterprise IT Security Department has determined that the combined systems will be in compliance with BSU security requirements. Real-time connections between two or more in-house BSU computer systems must not be established unless Enterprise IT Security has determined that such connections will not jeopardize the information security of sensitive data.

Personal Computer Connections - Employees must not connect their own computers with BSU computers or networks without prior authorization from DIT. Personally-owned systems must not be used to process any BSU information unless the systems have been approved for use by Enterprise IT Security.

New Installations - Employees and vendors working for BSU must not make arrangements for, or actually complete, the installation of voice or data lines with any carrier unless they have obtained written approval from the Director of the Office of Telecommunications.

Firewalls Required - All connections between BSU internal networks and the Internet or any other publicly-accessible computer network must include an approved firewall or related access control system. The privileges permitted through this firewall or related access control system must be based on business needs and must be defined in an access control standard issued by the Enterprise IT Security Department (documentation available from the department). Ingress and egress filtering shall occur on BSU networks.

IT CONTRACTS

IT Contracts - All IT Vendors must have Contracts and must go through Procurement. Furthermore, the BSU Office of Procurement is responsible for the procurement of all equipment, services, materials and supplies utilized by the BSU campus.

IT contracts must address technical requirements and data security. BSU and the IT vendor must reach an agreed level before connection to systems is allowed.

THIRD-PARTY ACCESS

Written Approval Required - Before third-party users are permitted to reach BSU internal systems through real-time direct computer connections, specific written approval of the Enterprise IT Security Department Manager must be obtained. These third parties include information providers such as outsourcing organizations, business partners, contractors, and consultants working on special projects.

Access Restrictions - Third-party information system vendors must be given only inbound connection privileges when the DIT Systems Manager determines that they have a legitimate business need. These privileges must be enabled only for the time period required to accomplish previously-defined and approved tasks. Third-party vendor access that will last longer than one day must be approved by the Enterprise IT Security Department.

Only Public Information Posted - Unless the relevant information Owner has approved in advance, employees must not place anything other than BSU public information in a directory, on a server, or in any other location where unknown parties could readily access it.

Third Party Security Requirements - As a condition of gaining access to the BSU computer network, every third party must secure its own connected systems in a manner consistent with BSU requirements. BSU must reserve the right to audit the security measures in effect on third party-connected systems without a prior warning. BSU also must reserve the right to terminate immediately network connections with all third-party systems not meeting BSU requirements.

THIRD-PARTY CLOUD

For mission-critical systems that require the services of a third party cloud technology vendor to transmit, collect, process, store, or exchange confidential information, the requirements provided in USM IT Security Standards v4.0 shall be reviewed**.**

ENCRYPTION

Default Protection Not Provided - The Internet and other public networks are not protected from wiretapping by default. In all but a few rare instances, if the information is to be protected, then the user must take specific action to enable encryption facilities. Users who employ cellular or mobile phones must not store or discuss Sensitive (Confidential or Restricted) information unless they have taken steps to encrypt the information. Video conferences must not involve discussion of sensitive information unless encryption facilities are known to be enabled.

When To Use Encryption - Whenever confidential information is sent over a public computer network like the Internet, encryption methods authorized by the Enterprise IT Security Department must be used to protect it. Whenever confidential information is stored in a computer, this storage must be with similarly authorized encryption methods. For more information about these circumstances, “Data Classification Quick Reference Table.”

Key Selection - Many encryption routines require that the user provide a seed or a key as input. Users must protect these security parameters from unauthorized disclosure, just as they would protect passwords from unauthorized disclosure. Rules for choosing strong seeds or keys must follow all rules for choosing strong passwords.

ELECTRONIC MAIL

Sharing And Forwarding - Electronic mail accounts, like user IDs, are for specific individuals and must not be shared. If a user goes on vacation or is otherwise unable to check their mail for extended periods, mail can be forwarded to another BSU employee. Out-of-office notices can be established that will automatically inform correspondents that the recipient will not be responding for a certain period of time.

Within the BSU network (e.g. @bowiestate.edu to @bowiestate.edu), if an electronic mail message contains sensitive information, users must not forward it to another BSU recipient unless the other recipient is known to be authorized to view the information.
Never send an electronic mail message containing sensitive information outside the BSU network without end-to-end encryption.

Contents Of Messages: When using State resources to access or use emails system, users must exercise good judgement when opening unsolicited messages. Questions regarding email communications should be directed to ta supervisor or to DoIT personnel.
While using State resources, an end user must not:

- Send any unsolicited messages, including “junk mail" or other advertising materials (email spam), to individuals who did not specifically request such material.
- Engage in any form of harassment via email, telephone, paging, whether in the form of language, frequency or size of messages.
- Engage in any form of unauthorized use, or forging, of email header information.
- Creating or forwarding “chain letters”, “Ponzi”, or other “pyramid” schemes of any type.

Harassing Or Aggressive Messages: - Users must understand that BSU information systems must not be used as an avenue to abuse the exercise of a user’s right to free speech. While cognizant of freedom of speech and academic freedom, the use of BSU’s Information Systems to engage in any communications that are in violation of any BSU Policy and/or applicable Federal and/or State Laws is prohibited. Sexual, ethnic, and racial harassment, including unwanted telephone calls, electronic mail, and internal mail, is strictly prohibited. Users must not respond directly to the originator of offensive electronic mail messages, telephone calls, or other communications. Harassment of any type is strictly prohibited. Employees must report these types of communications to their manager, the Human Resources and/or the Enterprise IT Security Department

PRINTING, COPYING AND FAX TRANSMISSION

Destruction Of Waste Copies - If a printer, copier, or fax machine jams or malfunctions when printing Sensitive or Confidential information, the involved users must protect the information by not leaving the machine until all copies of the sensitive information are removed. All paper copies of readable sensitive information must be disposed of by shredding.

Faxing Precautions - Sensitive materials must not be faxed unless an authorized staff member is on hand at the time of transmission to properly handle the materials at the receiving BSU site. Sensitive information must not be faxed through untrusted intermediaries such as hotel staff or rented mailbox service staff. Confidential information may be faxed by the Internet only if the connection is protected with encryption systems approved by the Enterprise IT Security Department.

Printer Precautions - When printing sensitive information, the user must be present at the printer at the time of printing to prevent the information from being revealed to unauthorized parties, or direct the output to a printer inside an area where only authorized employees are permitted.

Copy Machine Precautions - Unless permission from the copyright Owner is obtained, making multiple copies of material from magazines, journals, newsletters, and other publications is forbidden unless this is both reasonable and customary. Many copy machines contain hard drives capable of storing information. In departments that handle sensitive information copy machine hard drives must be purged of all data before the machine leaves the department.

Leasing and Repair Services - Only third-party vendors who have signed a BSU non-disclosure agreement can perform the repair of fax machines, printers, and copy machines. Third-party vendors of machines that contain storage devices e.g. copy machines or printers with hard drives must agree to purge the storage device of all university information before it is removed from the department.

MOBILE COMPUTING AND WORK AT HOME

Approval For Remote Access - Remote access to BSU computers must be granted only to those users who have a demonstrable business need for such access. Permission to access BSU computers remotely is granted by and annually reviewed by a user's manager.

Location Independence - All security requirements apply at remote locations. Sensitive information stored on computing devices or paper must be kept in a secure manner to protect the information Owner.

Access Control Packages - All portable and remote computers that are under the control of BSU employees and that are used to process BSU business information must be protected with the same access controls that apply to BSU owned computers. These access controls must prevent unauthorized use of the machines and unauthorized access to BSU information. The access controls must prevent virus infections and other types of damage from malicious software.

Handling Of Sensitive Information - Sensitive (Confidential or Restricted) information must not leave BSU offices. If it is necessary to remove computer-readable sensitive information from BSU offices, this information must be protected with encryption facilities provided by DIT and approved by Information Security. If sensitive information is transmitted over public computer networks such as the Internet, this transmission must take place with encryption facilities approved by Enterprise IT Security. All portable and remote systems storing sensitive BSU information must also employ hard disk encryption systems.

Theft Of Equipment - If BSU information systems equipment is not stored in a locked area, users must employ anti-theft equipment such as locking cables to secure BSU equipment. Users must not store passwords, user IDs, or any other access information in portable or remote systems.

Travel Considerations – Travelers are often the target of theft. When traveling users must employ anti-theft techniques. Store equipment in a secure area such as a locked room or auto trunk. If a secure area is not available, employ locking cables to secure BSU equipment. Users must also be careful not to discuss sensitive information when in public places like hotel lobbies, restaurants, and elevators.

VIRUSES, MALICIOUS SOFTWARE, AND CHANGE CONTROL

Virus Checking Required - Virus-checking systems provided by DIT and approved by the Enterprise IT Security Department must be in place on all personal computers with operating systems susceptible to viruses, on all firewalls with external network connections, and on all electronic mail servers. All files coming from external sources must be checked before usage.

If A Virus/Malware Infection Is Detected - If users obtain infection alerts, they must immediately disconnect from all networks and cease further use of the affected computer, and call the Help Desk for technical assistance. Users must not remove viruses or malware on their own. If users believe they may have been the victims of other malicious software, they must immediately call the Help Desk to minimize the damage. User possession or development of viruses or other malicious software is prohibited. Registered academic research in a controlled environment off the BSU business network is an exception to this rule.

Change Control - Users must not install new or upgrade operating systems or application software on BSU business computing devices. These computing devices have been specifically recognized as systems used for regular university business activities. This approach permits DIT to perform automatic software distribution, automatic software license management, automated remote backup, and related functions on a centralized and coordinated basis. While change control will be maintained through the above-mentioned access control packages, users can, however, change the personal preferences of software packages e.g. change fonts for a word processing package, organize email messages folders, etc.

Academic Research - Research that involves the development of viruses or other malicious software must not be conducted on computing machines that are connected to the BSU business network. Research that requires the modification of the operating system or application software must not be conducted on computing machines that are connected to the BSU business network. These types of research are both legitimate and important scholarly work that like all research must be conducted in a controlled environment. It is important that this type of research be:

1. Registered and approved in writing by the BSU Provost, and
2. that the IT Enterprise Security Department is informed in writing, and
3. that the research is conducted in an environment that is separated from the BSU business network.

PERSONAL USE OF INFORMATION SYSTEMS

Personal Use - All user activity is subject to logging and subsequent analysis. Personal use of University/State information technology assets and services is permitted, provided such use is consistent with the University's policies, including but not limited to the Acceptable Use policy, is limited in amount and duration, and does not impede or interfere with the end user's ability to

fulfill his or her assigned duties. End users must not use University/State information technology assets to conduct or manage personal business affairs, e.g., webhosting, real estate business, or supporting a side business. End users must use their best judgment regarding personal use of University/State information technology assets. End users must not use University/State information technology assets for personal use in a manner that would jeopardize the security of the University/State or the University's/State's reputation. Violations of this clause may result in disciplinary action, up to and including termination of employment

Testing Prohibition - Users must not test or attempt to compromise any information security mechanism unless specifically authorized to do so by the Enterprise IT Security Department. Users must not possess software or other tools that are designed to compromise information security. (See registered Academic Research exception above.)

INTELLECTUAL PROPERTY RIGHTS

Legal Ownership – University users understand and acknowledge that (1) the Agency which employs me, and DoIT as the policy setting authority, reserve the right to monitor system activity and usage, including Internet activity. My acceptance of employment or signature of contract communications consent to this monitoring, (2) there should be no expectation of privacy or ownership when using University systems and (3) all emails, files, and documents — including personal messages, files, and documents — created, sent, received, or stored on information systems or devices owned, leased, administered, or otherwise under the custody and control of the Bowie State University/State of Maryland are the property of the State and may be subject to review.

Making Copies Of Software - Users must not make copies of or use software unless they know that the copies are in keeping with the vendor's license to BSU. If DIT has set up a system that is used to process BSU information, users can rely on the fact that all software on this system licensed and authorized. Questions about licensing must be directed to DIT, which maintains documentation reflecting software licenses throughout BSU. Making regular backups of software for contingency planning purposes is permissible. DIT must remove all software that is not authorized on systems that are used to process BSU information.

Information Labeling - In addition to maintaining the labels mentioned in "Information Sensitivity Classification," users must maintain information about the source, date, and usage restrictions for all information provided by third parties. These labels will be important for management decision-making purposes, and will demonstrate that BSU observed appropriate copyright and other intellectual property laws. Users must assume that all materials on the Internet are copyrighted unless specific notice states otherwise.

SYSTEMS DEVELOPMENT

Production System Definition - Information systems that have been designated critical production systems have special security requirements. A critical production system is a system that is regularly used to process information vital to BSU business. Although a production system may be physically situated anywhere, the production system designation is assigned by the Enterprise Systems Manager.

Special Production System Requirements - If the software is developed in-house to run on production systems, it must be developed according to a recognized development methodology (SDM/SDLC). This methodology must ensure that the software will be adequately documented and tested before it is used. The SDM/SDLC also must ensure that production systems include adequate control measures. Production systems also must have designated Owners and Custodians for the critical information they process. All production systems must have an access control system to restrict who can access the system and restrict the privileges available to these users. A designated systems administrator who is not a regular user on the system must be assigned to control access to all production systems.

Separation Between Production, Development, And Test Systems - Where resources permit, there must be a separation between the production, development, and test environments. All security fixes provided by software vendors must go through the systems development methodology testing process, and must be promptly installed. DIT Enterprise Systems, Enterprise Application and Functional Support Departments must follow formal and documented change control processes to restrict and approve changes to production systems. All application program-based access paths other than the approved user access paths must be deleted or disabled before software is moved into production. This documentation must be preserved for audit inspection.

User Programming - Users must not write production computer programs unless specifically authorized by the Chief Information Officer. The construction of spreadsheet formulas, automatic execution scripts that are run when a system is booted, or databases is not considered programming for purposes of this document. Both users and programmers must be careful never to embed user IDs, readable passwords, encryption keys, or other security parameters in any file. (See registered Academic Research exception above.)

DISASTER RECOVERY PLAN (DRP)

In the real event of a disaster, DIT shall utilize the Disaster Recovery Plan (DRP) to remediate and recover from the disaster. BSU DIT is committed to taking the necessary steps to minimize the effects in the event of a disaster, thus continuing to operate mission critical systems quickly. DIT carries out annual DRP tests with the required disaster recovery team to ensure that processes perform as required in the event of a disaster. The DRP is classified as restricted information.

CONTINUITY OF OPERATIONS (COOP)

DIT will utilize the DRP to ensure critical operations are uninterrupted in the event of a disaster. The DRP provides detailed information on how to recover from an IT disaster while maintaining critical IT operations.

PHYSICAL SECURITY

Physical access to areas classed as “secure areas” is based on legitimate business responsibilities. Such areas include the data center, areas with servers and associated media,

networking cabinets and wiring closets. Access to these areas are strictly controlled and based on “need to know” basis.

Proper environmental controls are also in place to prevent accidental or unintentional loss of confidential systems residing on IT Systems.

Physical media containing sensitive information must be destroyed and/or sanitized to prevent unintended data leak/exposure.

VIRTUALIZATION TECHNOLOGIES STANDARDS

Commensurate with risk, virtual servers will have the same security controls applied on non-virtual servers.

REPORTING PROBLEMS AND INCIDENTS

What To Report - All employees must promptly report to the Enterprise IT Security Department any loss of, or severe damage to, their hardware or software. Employees must report all suspected compromises to BSU information and systems. All information security vulnerabilities known to exist must be reported. All instances of suspected disclosure of Sensitive or Confidential information also must be reported to the Enterprise IT Security Department for incident investigation.

How To Report – A hotline has been established to handle information security problem reports. Callers to the hotline can leave messages on this line anonymously: 1-877-FRAUD-11 (1-877-372-8311)**.** Reports must not be sent by electronic mail unless encrypted. Please use the paper form located here: https://www.bowiestate.edu/it/security-and-compliance/itsecurityforms/itsecurityincident/

All reports will be documented, investigated and submitted to the area Vice President for consideration.

EXCEPTIONS

Risk Acceptance - In some rare cases, the business case for non-compliance can be established. In all such cases, the non-compliance situation must be approved in advance through a risk acceptance process. This process requires a risk acceptance memo signed by a Department Manager, reviewed IT Enterprise Security, IT Information Systems and approved by the area Vice President and the DIT VP/CIO. Further details on the risk acceptance process can be obtained through Enterprise IT Security Department.

Further Information - Questions about this DIT rules document should be directed to:

- Enterprise IT Security Department Manager at infosec@bowiestate.edu.
- University Policy information can be found in the BSU General Counsel’s website: https://www.bowiestate.edu/about/administration-and-governance/legal-and-government-affairs/university-policies/index.php

VIOLATIONS

Violations - Engaging in unacceptable use of Bowie State University IT assets is a security violation and is strictly forbidden. Violations may result in disciplinary action, up to and including termination of employment.

The following examples are a general, non-exhaustive, list of unacceptable uses of IT assets and services. Violations may include, but are not limited to, Engaging in any activity that is illegal under local, State, Federal or international law while using the State's information technology assets and electronic communication systems; Unauthorized collecting, transmitting, or sharing of confidential information, e.g., Personally Identifiable Information (PII), HIPAA (personal health) information, and Federal Tax Information (subject to IRS 1075 Compliance); Violating the rights of any person or company protected by copyright, trade secret, patent, intellectual property, or similar laws or regulations, e.g., installing or distributing software products that are either "pirated" or not appropriately licensed for use by the State or authorized for use on the network; Unauthorized reproduction of copyrighted material, e.g., digitizing and distributing photographs from magazines, books or other copyrighted sources, copyrighted music, or installing copyrighted software for which the State does not have an active license; Exporting software, technical information, or technology in violation of international or regional export control laws; Intentionally introducing malicious (or non-approved) programs into the State's electronic communication system infrastructure such as workstations, servers, and networks; Circumventing user authentication or security of any account, host, or network, including disclosing a user's password to others or allowing a user's account to be used by others; Interfering with or denying access to resources to any user or system, e.g., conducting a denial of service attack; Accessing data, servers, or accounts for any purpose other than conducting official State or job related business or duties, even if the user has authorized access; Interfering with or disrupting network users, services, or workstations, including distributing unsolicited advertising or propagating computer viruses; Tampering with the security of State owned workstations, network equipment, services, or files; and Transmitting or storing confidential information to or from a personal email account, on a non-State issued device, or with an unapproved third-party storage service.

BSU is obligated to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. BSU does not consider conduct in violation of an information security rule to be within an employee's or partner's course and scope of employment, or the direct consequence of the discharge of the employee's or business partner's duties. Accordingly, to the extent permitted by law, BSU reserves the right not to defend or pay any damages awarded against employees or business partners that result from violation of this rule or any BSU Policy it enables. Any employee or business partner who is requested to undertake an activity, which he or she believes, is in violation of this rule, must provide a written or verbal complaint to his or her manager, any other manager, the Human Resources Department, or the Enterprise IT Security Department as soon as possible

REFERENCES

University System of Maryland (USM) Security Standards v4
National Institute of Standards and Technology (NIST) SP 800-37; SP 800-30; SP 800-53, NIST SP 800-63.

Related Documents

International Standards Organization (ISO) 27000 Series.

Approval and Ownership

Edited By	Title	Date	Signature
Ebony Pierce	IT Security Manager	05-2017	
Ifueko Fify Omoruyi	IT Security Manager	03-2019	
Victoria Persaud	Information Security	05/2019	
Ifueko Fify Omoruyi	IT Security Manager	06/2019	
Approved By	**Title**	**Date**	**Signature**
IT Security Committee	Information Security	X/2019	
TBD	BSU VP/CIO	X/2019	
Marivic Weiss	Interim VP for IT	06/2019	

Revision History

Version	Revision Date	Review Date	Description
1.1	July 2015		
1.2	May 2017		
1.3	March 2019	**On-going**	
1.4	June 2019		**In response to the USM IT Security audit**
1.5	August 2019		**Edited Physical Security, Disaster Recovery Plan (DRP), Third Party Cloud, Virtualization Technologies Standard, Audit Capabilities, Network Tools Management, Website links, Continuity of Operations (COOP)**