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 include 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 the importance 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 program 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 consistently follow. Sometimes called “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 above define general University goals, expectations, and responsibilities with regard to technology use. The BSU Policies and the DIT rules define the minimum controls necessary to prevent legal problems such as allegations of negligence, breach of fiduciary duty, or privacy violation. This document contains DIT rules that details 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 and is the result of many years of dedicated effort on the part of 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 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 was 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 is able to support further growth of the University, and support a consistently high level of service to our constituents. The document is also 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. Top 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 set forth 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 come into contact with BSU information or information systems.

INFORMATION SECURITY 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 related risk 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 uses of their information.
- Select a sensitivity classification category relevant to their information with consultation of the BSU General Counsel, and review classifications every five years.
- Select a criticality category relevant to their information with 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 back-up alternative 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.

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 the Enterprise IT Security Department.
When an employee leaves BSU, it is the responsibility of the employee’s immediate manager to promptly inform the Enterprise IT Security Department 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 can be 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, including implementing access control systems to prevent inappropriate disclosure, and 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,
- Monitor the security of BSU information systems,
- 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 and remediation 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 promptly respond to virus infections, system break-ins, system outages, and similar information security problems.