X-1.00-POLICY ON INFORMATION TECHNOLOGY SECURITY

I. PURPOSE

The BSU Information Technology ("IT") Security Policy is the basis for the University's IT security program. This policy establishes the framework to ensure that institutional IT infrastructure, resources, and services are managed and utilized securely. These resources include information, information systems, computing platforms, network and telecommunication services. This policy also ensures that the University complies with state laws and regulations regarding the use of and security of information resources.

II. APPLICABILITY

The BSU IT Security Policy applies to all University information technology resources, infrastructure, services, and all users who access those resources. While the policy applies to all Information Technology resources, it especially pertains to University systems and services that support critical business functions and maintain sensitive personal and institutional information. Each member of the University community is responsible for the security and protection of electronic IT resources over which he or she has control.

III. DEFINITIONS

INFORMATION TECHNOLOGY RESOURCES. IT resources include all University-owned computers, application software, systems software, databases, IT appliances, peripheral equipment, the data communication infrastructure, the voice communications infrastructure, classroom technology resources and infrastructure, business technology resources and infrastructure, telecommunication services and devices including e-mail, voice mail, multimedia equipment, etc. They may be standalone or networked and may be single-user or multi-user systems.

UNIVERSITY COMMUNITY. All BSU students, employees, partners, official guests and affiliates.

OFFICIAL GUESTS AND AFFILIATES. Guests: The University may invite guests to participate in activities that enhance the University's mission. Examples include visiting faculty and dignitaries, conference invitees and officials of outside entities. Affiliates include those to whom access may be granted based upon a specific function or role related to the University. Examples include: state and federal auditors and inspectors; USM institutions; University foundation; affiliated organizations; and contractors and consultants.

SENSITIVE INFORMATION. The University uses the following categories of sensitive information.

Restricted. This classification applies to the most sensitive University information that is intended for use strictly within BSU. Unauthorized disclosure could seriously and adversely impact the University, the University Community of students, faculty and employees, partner institutions and suppliers. Examples include merger and land acquisition documents, attorney-client privileged documents and trade restricted inventions such as certain computer applications development.

Confidential. This classification applies to sensitive personal and business information that is intended for use within BSU. Its unauthorized disclosure could adversely impact BSU or individuals. Information that some people would consider to be private is included in this classification. Examples: all personal information described in Annotated Code of Maryland, State Government Article, §10-1301(c); student transcript data, student requests for data privacy, unpublished internally-generated market research, computer passwords and internal audit reports.

Internal Use Only. This classification label applies to all other information that does not clearly fit into the previous two classifications. While its unauthorized disclosure is against rules, it is not expected to seriously or adversely impact BSU or its employees, suppliers, business partners or its customers. Examples include the BSU employee telephone directory, computer inventory numbers, new employee training materials and internal rule manuals.

Public. This classification applies to information that is releasable to the public in accordance with the Maryland Public Information Act, Annotated Code of Maryland, General Provisions Article, §§ 4-101, et seq. Examples include, but are not limited to, class schedules, catalogs and brochures, advertisements, job opening announcements, employee salary information and press releases.

IV. GENERAL PROVISIONS

The integrity of BSU IT resources must be protected against threats such as unauthorized intrusions, malicious misuse or inadvertent compromise. BSU establishes and maintains a security program that enhances and protects the integrity, confidentiality and availability of BSU's IT resources and complies with applicable federal and state laws. The program consists of the following elements:

- Risk assessments of IT resources
- Disaster Recovery Plan
- Access controls to computing environments and electronic data
- Backup and recovery
- Network and systems security
- Monitoring, incident response, and reporting
- Media disposal and re-use

- IT purchasing and acquisition standards
- Security awareness training
- Organizational responsibilities

The University will implement separate procedures that address acceptable use of IT resources, sanctions for the misuse and abuse of University IT resources, privacy of electronic information, use of electronic mail (E-mail), Disaster Recovery and Business Continuity and others. The Vice President for Information Technology or a designee has the authority to prevent a resource or system from accessing the University IT infrastructure, services or systems, if such access poses a risk to IT security.

V. RELATED POLICIES

- USM IT Security Standards http://www.usmd.edu/usm/adminfinance/itcc/USMITSecurityStandards.pdf
- Bowie State University Procedures for the Acceptable Use of Electronic Messaging
- Bowie State University Information and Data Privacy Procedures