**Purpose**

This Information Technology (IT) Security Policy defines the roles and responsibilities for management and protection of the security of the University’s IT systems, as required by the *Information Technology Security Policy (COV ITRM Policy SEC519-00)*.

**Policy Statement**

This policy applies to all University personnel whether an employee, contractor, or student. It is everyone’s responsibility to understand the requirements, responsibilities, processes, and procedures defined in this policy and the accompanying manual, and to remain in complete compliance with this Information Security Program.

**Authority, Roles, and Responsibilities**

A. The **University President**:

1. In Accordance with Commonwealth policy, assumes responsibility for the overall security of VSU’s systems, applications, and data.

2. Will designate an Information Security Officer to oversee the Information Security Program.

B. The **Information Security Officer (ISO)** is required to:

1. Maintain the University’s IT security program such that it is sufficient to protect the University’s IT systems, and that is documented and effectively communicated.
   
   a. The component areas of University Security Program will be incorporated into the University Information Security Program manual ISO Manual ISEC6110-01, and its associated documentation.

2. Review and approve the University’s Business Impact Analyses (BIAs), Risk Assessment (RA), and the IT components of the University’s Continuity of Operations Plan (COOP), to include the IT Disaster Recovery Plan.

3. Maintain compliance with Virginia Information Technology Agency (VITA) policies and standards.

4. Review and approve the University’s Security Plans for all systems and ensure that these systems are adequately protected against IT security risks.
5. Develop and maintain an IT security awareness and training program for University employees, contractors, and students.

6. Coordinate and provide IT security information to the Chief Information Security Officer of the Commonwealth (CISO) as required.

7. Implement and maintain the appropriate balance of protective, detective and corrective controls for University’s IT systems commensurate with data sensitivity, risk and systems criticality.

8. Mitigate and report all IT security incidents in accordance with §2.2-603 of the Code of Virginia and VITA requirements and take appropriate actions to prevent recurrence.

9. Designate an Incident Respond Team that includes the appropriate expertise for responding to cyber attacks, viruses, and network security breaches.

10. Establish a program of IT security safeguards for the operation and security of the University’s data network including specification, configuration, and management of all devices connecting to the University’s network.

11. Collaborate with the University Technology Coordinating Committee (UTCC) on the implementation of the University’s Information Technology (IT) Security Program.

C. The Office of University Technology (OUT) is required to manage and maintain the campus backbone network. OUT security roles and responsibilities include but may not be limited to:

1. Monitor the campus network traffic, primarily for the purpose of network maintenance, optimization, unauthorized intrusions, and overall security of the Commonwealth of Virginia.

2. Inform the CIO and ISO of traffic patterns, which pursuant to best practices, procedures and standards, may indicate a potential or actual threat to the network backbone and University IT Resources.

E. The System Owner is responsible for managing operations and maintenance for University IT systems. In respect to IT Security, the System Owner is required to:

1. Ensure that all IT system users complete required IT security awareness and training activities prior to, or as soon as practicable after, receiving access to the system, and no less than annually, thereafter.
2. Manage system risk and developing any additional IT security policies and procedures required to protect the system in manner commensurate with risk.

3. Maintain compliance with University IT security policies and standards in all IT system activities.

4. Maintain compliance with requirements specified by Data Owners for the handling of data processed by the system.

5. Designate a System Administrator, Application Administrator, and Database Administrator for the system as applicable.

G. The **System Administrator** is required to implement, manage, and/or operate a system(s) at the direction of the System Owner, and/or Data Owner. The System Administrator assists the University in the management of the day-to-day administration of the University’s IT systems and implements security controls and other requirements of the University IT security program. Except for those systems identified as “Infrastructure”, the support provided at this level is typically limited to maintaining system hardware, operating systems, middleware, backups, system recovery, and maintaining system security controls.

H. The **Application Administrator** is required to manage the application that is hosted on local or remote servers at the direction of the System Owner, and/or Data Owner. The Application Administrator is responsible for the day-to-day administration of the application that runs on University owned or contracted resources. This level of administration includes, but is not limited to, the provisioning of accounts, application maintenance, training, and maintaining security controls.

I. The **Database Administrator** is required to manage the database that is hosted on local or remote servers at the direction of the System Owner, and/or Data Owner. The Database Administrator is responsible for the day-to-day administration of the database that runs on University owned or contracted resources. This level of administration includes, but is not limited to, the management of accounts, provisioning of databases and tables, system monitoring and tuning, backup and recovery, and maintaining database security controls.

J. The **Data Owner** is responsible for the policy and practice decisions regarding data and is required to:

1. Evaluate and classify sensitivity of data.

2. Define protection requirements for the data based on the sensitivity of data, any legal or regulatory requirements, and business needs.
3. Communicate data protection requirements to the System Owner.

4. Define requirements for access the data.

K. The **Data Custodians** are the individuals in physical or logical possession of data for Data Owners. Data Custodians are responsible for the following:

1. Protect the data in their possession from unauthorized access, alteration, destruction, or usage.

2. Establish, monitor, or operate University IT systems in a manner consistent with University IT security policies and standards.

3. Provide Data Owners with reports, when necessary and applicable.

L. The **IT Systems Users** are all users of University IT system including employees, students, and contractors. These users are responsible for the following:

1. Read and comply with University IT security program requirements.

2. Report breaches of IT security, actual or suspected, to their management and/or the Information Security Officer (ISO).

3. Take reasonable and prudent steps to protect the security of IT systems and data to which they have access.

**Definitions**

A. **Information Technology Resource** is a resource used for electronic storage, processing or transmitting of data, as well as the data itself.

B. **System Owner** is the individual designated by the governing UTCC committee having the responsibility for determining the purpose and function of the IT Resources within the organization for which they are responsible. The Manager has policy level responsibility for managing a segment of the University’s IT Resources. Depending on the requirements of the organization, the System Owner may also act as the Data Owner and/or the IT Systems Administrator.

C. **Data Owner** is the individual that has physical, logical and operational control over the Information Technology Resource including data capture, data maintenance, and data
D. **Systems Administrator** is the University staff member that, under the direction of the Data Owner, has day-to-day operational responsibility for system hardware, operating systems, and system security.

E. **Application Administrator** is the University staff member that, under the direction of the Data Owner, has day-to-day operational responsibility for data capture, maintenance, dissemination, and application security.

F. **Database Administrator** is the University staff member that, under the direction of the Data Owner, has day-to-day operational responsibility for all database provisioning, maintenance, tuning, and database security.

G. **Information Security Officer (ISO)** is the individual responsible for the development, implementation, oversight, and maintenance of the VSU information security program.

H. **Security** is the measures taken to reduce the risk of (1.) unauthorized access to IT Resources, via either logical, physical, managerial, or social engineering means; and (2.) damage to or loss of IT Resources through any type of disaster, including cases where a violation of security or a disaster occurs despite preventive measures.
References

Virginia Department of Human Resources Management:
 Policy 1.75 – Use of Internet and Electronic Communications Systems

Virginia Information Technology Agency (VITA):
 Information Technology Security Policy (ITRM Policy SEC519-00)
 Information Technology Security Standard (ITRM Policy SEC501-01)

Virginia State University (VSU):
 Policy 6010: Acceptable Use Policy
 Policy 6020: Electronic Records and Retention Policy
 ISO Manual ISEC6110-01

APPROVED BY: ____________________________   ____________________________
                      President                              Date

Revision Date: January 19, 2010
Page No: 6