## Purpose

Access to Virginia State University's information systems and data is controlled by the implementation of an appropriate access control policy to manage accounts and define the processes of authentication, authorization, administration, and termination of access rights. The specifics of the responsibility of management to ensure that user access is handled appropriately is outline in this policy.

## Authority, Responsibility, and Duties

The IT Security Program roles and responsibilities are assigned to individuals, and may differ from the actual role title or working title of the individual's position. Individuals may be assigned multiple roles, as long as the multiple role assignments provide adequate separation of duties, provide adequate protection against the possibility of fraud, and do not lead to a conflict of interest. Refer to Logical Access Policy 6310 for details on roles and responsibilities.

### A. System Owner

The System Owner is responsible for ensuring that user access is reviewed annually to determine if access granted is still warranted.

### B. System Administrator

Once notified that an individual has terminated employment or transferred to another department within the university, the System Administrator is responsible for timely removal or adjustment of user access.

### C. Management

Every individual given the management responsibility is required to alert Human Resources when employees under their direction have submitted their resignation. It is also the manager's responsibility to notify Human Resources when employee contracts expire and access is no longer needed.

### D. Human Resources

Human Resources will alert management and key personnel in a timely manner when employees are terminated or transfer within the university. (A monthly list of employees will also be provided by Human Resource for auditing purposes upon request.)

### E. All Users of Electronic Resources and Systems

All users of electronic resources and systems are accountable for any activity performed on a given system. Users are response for returning all University equipment upon termination. Any equipment lost by the user or stolen while under the guardianship of the assigned user must be reimbursed to the University by the user assigned the equipment.

## Definitions

The IT security definitions and terms can be found in the Commonwealth of Virginia (COV) Information Technology Resource Management (ITRM) Glossary. It is referenced on the ITRM Policies, Standards, and Guidelines web page on www.vita.virginia.gov/library.

## General Requirements

The University will:

a. Screen individuals prior to authorizing access to the information system;

b. Disable information system access within 24-hours of employment termination;

c. Terminate/revoke any authenticators/credentials associated with the individual;

d. Retrieve all security-related organizational information system-related property;

e. Retain access to organizational information and information systems formerly controlled by terminated individual;

f. Notify the appropriate organization-defined personnel within an organizationally defined time-period. This policy applies whether access is to the Local Area Network, Wireless "Wi-Fi" Network, and/or Virtual Private Network.

g. Review and confirm ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization;

h. Initiate the transfer or reassignment actions within 24-hours of the formal transfer action;

i. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer;

j. Notify the appropriate organization-defined personnel within organization defined time period;

k. Develop and document access agreements for organizational information systems;

l. Review and update the access agreements on an annual based or more frequently if required to address an environmental change; and

m. Ensure that individuals requiring access to organizational information and information systems:

    1. Sign appropriate access agreements prior to being granted access; and

    2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or on an annual basis or more frequently if required to address an environmental change.

n. Establish personnel security requirements including security roles and responsibilities for third-party providers;

o. Require third-party providers to comply with personnel security policies and procedures established by the organization;

p. Document personnel security requirements;

q. Require third-party providers to notify the appropriate organization-defined personnel of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within an organization defined time period.;

r. Monitor provider compliance, and

s. Employ a formal sanctions process for individuals failing to comply with established information security policies and procedures.

**References**

Virginia Information Technology Agency (VITA):
Information Security Standards (SEC501-09) (05/01/2015)
IT Systems Security Guideline (SEC515-00) (07/17/2008)

Library of Virginia Records Retention and Disposition Schedule for Administrative Records GS-101 located at: http://www.lva.virginia.gov/agencies/records/sched_state/GS-101.pdf

Library of Virginia Records Retention and Disposition Schedule for State Agencies: College and University located at: http://www.lva.virginia.gov/agencies/records/sched_state/GS-111.pdf

**Approval By**: _____ **Date:** 10/4/17
**President**