Title: Access Determination & Control Policy

Purpose

The Access Determination & Control policy identifies the steps necessary to restrict access to Information Technology (IT) systems and data to authorized individuals.

Policy Statement

This policy applies to all Virginia State University employees, students, business partners, third parties, and vendors, who intend to access and use the University IT system to perform their assigned job responsibilities.

Authority, Responsibility, and Duties

A. The Human Resources Department will perform background for all University employees. For contractors, vendors, and business partners, a letter from the user’s Human Resources Department should be provided to the Information Security Officer (ISO) stating a background check was performed and the users passed the background check before establishing user accounts and access privileges.

The Human Resources Department will facilitate the process in which employee job descriptions accurately reflect the assigned duties and responsibilities necessary for defining the required IT system access.

B. The Office of University Technology and Office of Information Technology (OIT) will take the steps necessary to restrict access to University IT systems and data to authorized individuals. At a minimum, these practices shall include the following components:

1. The VSU OneCard is the official identification card for all University employees, students, and contractors. It is used as a controlled access card entry system to restrict access to sensitive IT systems and data housed in the data center.

2. IT system users are required to sign the “Acceptable Use Policy and IT Acceptable Use Standards and User Acknowledgement Agreement” which acknowledges that they are fully aware of security best practices, their roles in protecting the University’s information technology systems and data. Access to University computer technology will not be granted without this agreement.

3. All University employees, students, and contractors who use the University IT systems are required to complete an annual online Security Awareness Training course every twelve (12) months. All newly hired employees are required to complete the Security Awareness Training course within the first 30 days from date of hire or prior to receiving access to the University’s IT systems and data.
4. IT system users are required to formally request and have approved emergency or temporary access to all sensitive IT systems that:
   a. Are documented according to standard practice and maintained on file;
   b. Include access attributes for the account;
   c. Are approved by the System Owner and communicated to the ISO; and,
   d. Expire after a predetermined period, based on sensitivity and risk.

5. Prohibit the use of guest and shared accounts on sensitive IT systems.

6. Prohibit the displaying of user’s last name in the logon screen.

7. Automatically lock accounts that have not been used for a predefined period of time.

8. Any account that is no longer required will be disabled.

9. Disabled accounts will be retained in this state in accordance with VSU’s records retention policy.

10. Current and future applications are/will be configured to clear cached data and temporary files upon exit of the application or logoff of the system.

11. OIT coordinates with Data Owners and the Information Security Office to ensure that every IT system user account is associated with a group defining their access level.

12. OIT and OIT is the owner and coordinates with the Information Security Office in the investigation of any unusual IT system access activity.

13. System Administrators are required to have both a user account and administrative account. The user account should grant him/her the necessary access to perform his/her job responsibilities. If administrative access is required, a supervisor/manager should approve his/her administrative access to perform approved tasks.

14. Local administrator rights should only be granted to authorized IT staff. Any business exceptions should be properly documented and approved by the OIT Network Management and Information Security Officer.

15. Access to credentials for IT system users should be granted to perform their assigned job responsibilities. Access for IT system users should be documented in the access request form and maintained on file.

16. Access credentials are only delivered via a secure means to all users of customer-facing IT systems.

In addition to these components, it is required that at least two individuals have administrative accounts to each IT system in order that continuity of operations is maintained.
C. The Data Owner is required to:

1. Authorize users’ access to University IT system and data based on the principle of least privileges, on sensitivity, and risk.

2. Perform at a minimum yearly periodic review of user authorizations to the sensitive IT systems and data, sign-off, and return the security report with changes to the ISO.

3. Notify ISO within 24 hours when IT system user accounts are no longer required, or when user’s access level requirements change.

4. Maintain copies of all access request authorization forms for all active users and account termination/deletion forms for terminated users in your department. Forward the account termination/deletion forms for the terminated employees, who have access to IT systems, in your department to ISO within 72 hours of termination.

5. Establish separation of duties in order to protect sensitive IT systems and data, or establish compensating controls when constraints or limitations of the University prohibit a complete separation of duties.

6. Data Owners are the only individuals defining user access levels to data, whether roles or groups.

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

1. Maintain all access request authorization and account termination/deletion forms including email communication.

2. Retain documentation of security review until the next scheduled Information Security Audit or 3 years which ever is longer.

3. Retain access request forms for terminated accounts for 1 year after access is terminated.

4. The Information Security Officer (ISO) is required to periodically review the list of persons who have physical access to sensitive IT systems in the data center.

5. The Information Security Officer coordinates with the OIT and OIT in the investigation of any unusual IT system access activity.

Definitions

Data Owner is the individual that has physical, logical and operational control over the Information Technology Resource including data capture, data maintenance, and data
Information Security Officer (ISO) is responsible for overseeing the implementation of the University’s Information Technology (IT) Security program.

Information Technology (IT) System Users includes Commonwealth of Virginia (COV) employees, contractors, vendors, third party vendors, and any other authorized users of IT systems, application, telecommunications networks, data, and related resources.

Least Privilege is the minimum level of data, functions, and capabilities necessary to perform a user’s duties.

Separation of Duties is assignment of responsibilities such that no one individual or function has control of an entire process. It is a technique for maintaining and monitoring accountability and responsibility for IT system and data.

References

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

Virginia State University (VSU):
Policy 6520: Acceptable Use Policy
Policy 6420: Electronic Records and Retention Policy
Policy 6110: IT Resource Security Policy
Policy 6640: Network Monitoring Policy
Policy 6530: Security Awareness Training Policy
Policy 6310: Banner Security Policy
Policy 6630: Data Breach Notification Policy
Policy 6620: IT Security Handling Policy

APPROVED BY: [Signature]  March 13, 2009
President  Date