Title: Logical Access Control and Account Management Policy Policy: 6310

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 purpose of this policy is to establish the requirements for managing access and all accounts for any information system, application, or data supported by the University.

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 Information Security Policy 6110 for roles and responsibilities.

A. System Owner

The System Owner is responsible for the following relative to the system he/she owns:

1. The roles, attributes and associated access levels for the system must be established based on the principle of "least privilege" and "separation of duties". The user accounts must be placed in the appropriately created groups based upon privileges.
2. Submitting written account requests to the Chief Information Officer (CIO) or designee to create new accounts. Background checks and other vetting must be completed prior to granting access.
3. Reviewing and either approving or denying the access requests to their system based upon least privilege and need-to-know principles.
4. Reviewing on a periodic basis (at least annually) all user accounts for the system for the appropriate privilege levels given the individual's role in the University, proper group membership on the system, active or inactive status and separation of duties.
5. Reviewing all user accounts for the system based upon any material or environmental change.
6. Notification of users and/or application owners if any system usage or need-to-know changes such as new users and access termination.
7. Monitoring the use of the system for any unauthorized behavior and report suspicious behavior to the Information Security Officer (ISO).
8. Determining the cause of unusual IT system access activities. With the System Administrator, investigate any unusual IT system access activities and approve changes to access level authorizations.
9. Determining whether wireless and/or remote access to his or her system will be permitted and any/all applicable usage restrictions associated with same. For sensitive systems, the system owner must also have means to monitor and encrypt remote and wireless connection activity to the system.

10. Determining the physical and logical hardening requirements for any devices that wish connect through a remote connection and provide a means for secure connection.
11. Determining if wireless access to the system is to be granted and if affirmative, establish usage restrictions, configuration guides and requirements. If the system is a sensitive system, authentication and encryption must be deployed. If wireless is not to be permitted, on-board wireless devices on the system must be disabled.
12. For sensitive systems with wireless permissions, restricting the wireless broadcasting to the best of his/her ability to prevent the reception of the signal outside of the boundaries.
13. Requiring that the IT system users complete any system unique security training prior to, or as soon as practicable after, receiving access to the system, and no less than annually, thereafter
14. Managing system risk and developing any additional information security policies and procedures required to protect the system in a manner commensurate with risk.
15. Maintaining compliance with COV Information Security policies and standards in all IT system activities.
16. Maintaining compliance with requirements specified by Data Owners for the handling of data processed by the system
17. Designating a System Administrator for the system.

B. Data Owner

The Data Owner is the agency manager responsible for the policy and practice decisions regarding data, and is responsible for the following:

1. Evaluate and classify sensitivity of the data.
2. Define protection requirements for the data based on the sensitivity of the data, any legal or regulatory requirements, and business needs.
3. Communicate data protection requirements to the System Owner.
4. Define requirements for access to the data.
5. Protecting the data in their possession from unauthorized access, alteration, destruction, or usage
6. Establishing, monitoring, and operating IT systems in a manner consistent with COV Information Security policies and standards.

C. System Administrator

The System Administrator is responsible for the following relative to the systems he/she administers under the direction of the System Owner and Data Owner:

1. Using an administrative account only when performing system administration and a separate user level account for other non-system related tasks.
2. Cooperating with authorized management investigating security incidents.

3. Cooperating with and assist the System Owner with maintaining policy and system compliance.
4. Prohibiting the use of a shared account on any system he/she is administering.
5. Ensuring that two individuals have administrative rights to any system he/she administers
6. Disabling accounts in a timely manner.
7. Automatically auditing account creation, disabling and termination. Proper notifications must be sent to stakeholders.
8. Prohibiting the creation and use of guest accounts for sensitive systems
9. Setting a limit of 3 consecutive invalid logon attempts by a user during a 15 minute time interval. After 3 invalid attempts, the system is automatically locked out for no less than 30 minutes.
10. Assisting the system owner with the proper display of warning banners and messages in line with Commonwealth standards prior to allowing users to access the logon screen of any given system he/she administers.
11. For sensitive system, the system administrator is responsible, in conjunction with the system owner, for having a way to disconnect and/or disable remote access to the system within 60 minutes.
12. Maintaining auditable records for remote access and administer user names and passwords for remote access authorization.
13. If wireless is restricted to system he/she administers, then said administrator must assist the owner in disabling all on-board wireless access devices and adapters.
14. Setting up only authorized accounts with the approval of the manager/supervisor and system owner.
15. Disabling accounts of user's that change roles within the University or are separated from their relationship with VSU.
16. Modifying user accounts to accommodate situations such as name changes or access privileges.
17. Reviewing existing accounts periodically for validity (at least annually) and obtaining departmental approval/sign-off.
18. Conducting an independent audit review for accounts and access administered:
    a. Providing a list of accounts and access privileges he/she administers when requested by authorized management.
    b. Ensuring proper background investigations are in order as required by the University's Background Investigation Policy.
    c. Cooperating with authorized management investigating security incidents.
19. Creating accounts of users that need access to University IT and data resources in conjunction with the system and data owner.

D. Information Security Officer (ISO)

1. Provide security consulting services for Systems Owner and Security Administrator to ensure that user access roles are appropriate to safeguard university data and systems.
2. Assist System Owners with assessing reported suspicious behavior identified on their systems.

E. Human Resources

Human Resources is responsible for:

1. Providing timely information regarding new employees and termination or modification of employment status (i.e. Medical Leave, etc.) to managers and system administrators.
2. Providing a monthly list of employees' change of status for the purpose of auditing system accounts upon request.

F. Procurement

Procurement is responsible for:

1. Providing timely information regarding new and termination contractors or modification of contractor status to managers and system administrators.
2. Providing a list of terminated employees/contractors for the purpose of auditing system accounts upon request.

G. All Users of Electronic Resources and Systems

All users of electronic resources and systems are accountable for any activity on the system performed with the use of their account. All users of VSU IT systems including, but not limited to, faculty, staff and contractors are responsible for the following:

1. Reading and complying with the university's information security program requirements.
2. Reporting breaches of IT security, actual or suspected, to their agency management and/or the ISO.
3. Taking reasonable and prudent steps to protect the security of IT systems and data to which they have access.

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.

Policy Statements

1. This Logical Access Control policy applies to all information systems, applications, and data housed within or supported by the University, and to all individuals who have access to those systems, applications or data, including employees (permanent, temporary, contractual, faculty, administrators and students).
2. This policy applies whether access is to the Local Area Network, Wireless "Wi-Fi" Network, and/or Virtual Private Network.
3. Access to University data that has been requested by other third parties or other state or federal agencies is controlled by the University Information Security Policies and on Interoperability agreements.
4. It is the policy of the University that all user accounts and access to systems will be managed and controlled according to the requirements identified in the following sections.

A. General Requirements

1. If the University system is classified as sensitive, the use of guest accounts is prohibited.
2. The use of shared accounts on all University systems is prohibited.
3. If the University system is classified as sensitive, requests for and approvals of emergency or temporary access is required such that:
    a. The access is documented according to standard practice and maintained on file;
    b. Access attributes for the emergency account are included in the documentation;
    c. Approval by the System Owner is communicated to the ISO; and
    d. The account is set to expire after a predetermined period, based on sensitivity and risk.
4. All accounts must be uniquely identifiable using the assigned user name.
5. All accounts must be set up to require the user to reset the password on the first use.
6. Access to IT systems and data is to be based on the principle of least privilege.
7. All passwords must meet the requirements of the University's Password Policy.
8. All accounts must have a password expiration that complies with the University's Password Policy which is a minimum of (8) characters with a mix of numbers, letters (one letter must be uppercase letter) and symbols.
9. All account users' identities must be verified using information already on file before resetting a user's password.
10. Accounts for individuals who are on extended leave (more than 30 days) will be disabled.
11. Disable logical access rights upon suspension of personnel for greater than 1 day for disciplinary purposes.
12. Any newly-established user accounts that have not been accessed within 90 days of creation are to be disabled. **(AC-2 (3))**
13. The use of guest or shared accounts on sensitive systems is prohibited.

14. All account access levels must be associated with group membership and must be a member of at least one user group.
15. Deliver access credentials to the user based on information (access request form) already on file.
16. Displaying of the user's last login name on the logon screen is prohibited.
17. Local Administrator, or the equivalent on non-Microsoft Windows-based IT systems are restricted to authorized IT staff and business or research units with documented exceptions only.
18. System Administrators are required to have both an individual administrative account and at least one user account and require that administrators use their administrative accounts only when performing tasks that require administrative privileges.
19. If a service or hardware account is not used for interactive login with the system, the account is exempt from the requirement to change the password at the interval defined in the VSU Password Policy.
20. If the system is to utilize a Wireless Local Area Network (WLAN), the following must be met:
    a. Client devices connecting to the WLAN must utilize two-factor authentication
    b. WLAN infrastructure must authenticate each client and must utilize authorization infrastructure such as Active Directory, to authorize access.
    c. Only Commonwealth of Virginia owned or leased equipment may connect to the internal WLAN and any systems located therein
    d. Must adhere to University's Wireless Policy and other applicable policies
21. All users must adhere to the security training policy and attend annual security awareness training. If additional training is required based upon environmental factors, all users must attend and complete the training that is applicable to them.

B. Authentication

Authentication is the process of ensuring that the individual is who he/she claims to be. Proper identification is required, and must be reviewed and accepted by an appropriate authority before an individual may receive an account for access to any VSU system.

1. Identification must be verified by presenting a government-issued identification credential that includes a recent photograph. Acceptable forms of identification include a state-issued driver's license or state-issued identification card, a passport, or a military identification card. In order to be accepted, any identification credential submitted for these purposes must be valid and unexpired.

2. A background investigation, in accordance with the University's Human Resources (HR) Background Investigation Policy, must be completed prior to creating a user account.

C. Authorization

Authorization is the process of providing permission to perform specific functions with respect to the use of servers, application systems, or accessing data. Each authorization action must be documented according to this policy, and such documentation must be retained for a minimum of three years beyond the termination of that authorization.

1. IT Access Request Form with the user's name, employer (if other than VSU), department, phone and email, the system name(s), and role of the user.
2. IT Access Request Form must be signed by the user, the user's supervisor or VSU contact (if non-employee), data owner, and the system owner.
3. IT Security Identifier Form must have one response to the security challenge question and signed by the user.
4. An Information Technology Acceptable Use Standard and User Acknowledgement, signed by the user.
5. Role-based authorization must be based on the principle of "least privilege" referring to the concept that users will have system access and functions necessary to complete their job responsibilities.

D. Administration and Termination of Accounts and Access

Every change in the employment status of members of the workforce (including employees, faculty, consultants, contractors, interns, etc.) must be reported immediately by the employing manager to Technology Services and Human Resources.

1. Upon notification, the Applications Security Administrator shall disable user accounts for terminated or separated employees, effective on the last day of work at the University.
2. Supervisors or Managers must submit department transfer forms or account modification forms. Upon receipt, the Applications Security Administrator shall modify the account access as designated by the supervisor or manager to maintain the principle of least privilege.
3. Accounts must be deactivated upon termination. They must be retained on the system in accordance with the records retention policy for 3 years, but in a disabled state with no access to systems or data.
4. Maintain in writing all status change notifications and authorizations.

References

Title: Logical Access Control and Account Management Policy Policy: 6310

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:** 9/6/17

President