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

Purpose

Access to Virginia State University's ("VSU") 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 for all accounts on any information system, application, or other data equipment (hardware or software) supported by the University to achieve and maintain compliance with Virginia Information Technology Agency ("VITA") requirements.

Individual Authority, Responsibility, and Duties

The Information Technology ("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 interests. Refer to Information Security Policy 6110 for roles and responsibilities.

A. System Owner

The System Owner is responsible for implementing and maintaining 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 principles of "least privilege" (amount of access to for one to complete one's tasks and no extra access) and "separation of duties (no overlapping of duties that could create a conflict)." The user accounts must be placed in the appropriately created groups based upon privileges and conditions once determined.
2. Reviewing the information system accounts in accordance with the instant University policy and other applicable policies.
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 yearly basis 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 needs.
5. Reviewing all user accounts for the system based upon any material or environmental change.
6. Working with IT Services and the Security Analyst(s) to determine the cause of unusual IT system access activities. With the assistance of the System Administrator, investigate any unusual IT system access activities and approve changes to access level authorizations.

7. Monitor the use of the system for any other unauthorized behavior and report suspicious behavior to the Chief Information Security Officer ("CISO").
8. Account request must be written and garner approval from Chief Information Officer ("CIO") or other agent for requests to create new accounts. Background checks and other vetting must be completing prior to granting access.
9. Notification of users and/or application owners of any system usage or need-to-know changes such as new users and access termination.
10. If the system is classified as "sensitive", the owner must have an automated process in place to disable inactive user accounts after thirty (30) days of non-usage and have a required time-out on user accounts for session inactivity after thirty (30) minutes.
11. Reviewing privileged roles (such as system administrator, security, etc.) and take appropriate actions to remove assignments no longer applicable.
12. Shared accounts are not permitted and all disabled accounts must be retained in a disabled state for three (3) years.
13. Automatically audit account creation, disabling, and termination. Proper notifications must be sent to stakeholders.
14. Documenting account management practices for service accounts such as granting and administering accounts.
15. Prohibit the creation of guest accounts.
16. Must have all systems display that it is a Commonwealth information system that is audited with expectation of privacy and has strict penalties for unauthorized use (in line with Commonwealth standard messages).
17. 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.
18. If remote access is to be granted on a system, the owner must require user id's and passwords for access and work with the system administrator in the usage and maintenance of same. For sensitive systems, the system owner must require two factor authentication or greater.
19. Determining the physical and logical hardening requirements for any devices that wish to connect through a remote connection and provide a means for secure connection.
20. Determining if wireless access to the system is to be granted and if affirmative, establish usage restrictions, configuration guides and requirements for same. 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.
21. 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.

B. System Administrator

The System Administrator is responsible for implementing and maintaining the following relative to the system he/she administers:

1. Operates solely under the authorization and direction of the system owner
2. He/she is 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.
3. Cooperating with authorized management investigating security incidents.
4. Cooperating and assist the System Owner with maintaining policy and system compliance.
5. Prohibiting the use of a shared account on any system he/she is administering.
6. Disabling accounts in a timely manner.
7. Ensuring that two individuals have administrative rights to any system he/she administers.
8. Automatically auditing account creation, disabling and termination. Proper notifications must be sent to stakeholders.
9. Prohibiting the creation and use of a guest account.
10. Must have logout capabilities and a logout display to aid in reliable termination of authenticated accounts on systems he/she administers.
11. Setting a limit of 10 consecutive invalid logon attempts by a user during a 15 minute time interval. After 10 invalid attempts, the system is automatically locked out for no less than 15 minutes.
12. 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.
13. For sensitive systems, 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.
14. Maintaining auditable records for remote access and administer user names and passwords for remote access authorization.
15. If wireless is restricted to the system he/she administers, then said administrator must assist the owner in disabling all on-board wireless access devices and adapters.

C. Applications Security Administrator

The Applications Security Administrator is responsible for the following relative to the accounts and access he/she administers:

1. Operates solely under the authorization and direction of the system owner

2. Setting up only authorized accounts with the approval of the system owner.
3. Disabling accounts of user's that change roles within the University or are separated from their relationship with VSU.
4. Creating accounts of users that need access to University IT and data resources in conjunction with the system and data owners.
5. Modifying user accounts to accommodate situations such as name changes or access privileges upon written notification from Human Resources.
6. Reviewing existing accounts periodically for validity (at least annually) and obtaining departmental approval/sign-off.
7. 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.

D. Information Security Analyst

1. **Working with the System Owner and other stakeholders to determine any unauthorized access or unusual traffic in regards to a system.**
2. **Investigating any malicious or suspicious traffic per the request of the Data Owner, System Owner or other agent of the University.**

E. Human Resources

Human Resources is responsible for:

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

F. 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.

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. In cases where provisions are clear for Wireless and Remote access, the access enhancements have been enumerated.
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. Additional General Rules and Requirements for All Systems and Users' Associated Accounts

1. The use of shared accounts on all University systems is prohibited. Systems residing on the guest network are exempt for this requirement.
2. 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 CISO; and
   d. The account is set to expire after a predetermined period, based on sensitivity and risk.
3. All accounts must be uniquely identifiable using the assigned user name.
4. All accounts must be set up to require the user to reset the password on the first use.
5. Access to IT systems and data is to be based on the principle of least privilege.
6. All passwords must meet the requirements of the University's Password Policy which is a minimum of eight (8) characters with a mix of numbers, letters and symbols.
7. All account users' identities must be verified using information already on file before resetting a user's password.
8. Accounts for individuals who are on extended leave (more than 30 days) will be disabled in line with the above referenced policy for system owners.
9. Any newly-established user accounts that have not been accessed within 90 days of creation are to be disabled in line with the above referenced policy for system owners.
10. All account access levels must be associated with group membership and must be a member of at least one user group.
11. Deliver access credentials to the user based on information already on file.

12. Displaying of the user's last login name on the logon screen is prohibited.
13. Local Administrator, or the equivalent on non-Microsoft Windows-based IT systems are restricted to authorized IT staff, business or research units with documented exceptions only.
14. 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.
15. 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 the University's Wireless Access Policy and other applicable policies.
16. All users must adhere to the security training policy and attend yearly 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 Requirements for All Users' Accounts on All Systems

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 Requirements for all Users' Accounts on All Systems

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. Further, separation of duties must be maintained.

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 Administer 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

Virginia Information Technology Agency (VITA):
Information Security Standard (SEC 501-09) (02/20/2015)

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: 3/10/16
President