Purpose

The Password policy identifies the steps required for password use to protect University IT systems and data and to ensure that all information technology (IT) system users are aware of their responsibilities in effective password management.

Policy Statement

This policy applies to all Virginia State University employees, students, business partners, third parties, and vendors, who intend to access the University's IT systems and data.

Authority, Responsibility, and Duties

All University employees and contractors shall be required to complete an access request form to gain access to University IT systems through the network to transmit, process, and store data. At a minimum, IT system users are required to:

1. Protect all data files from unauthorized use, disclosure, alteration, or destruction.
2. Be responsible for the security, privacy, and control of data within their control or view.
3. Create complex passwords that can not be easily guessed such as family member names, nicknames, and words found in the dictionary. Passwords should be a minimum of 10 characters including 1 character, 1 special character, and 1 number.
4. Prohibit the sharing of passwords, even with a supervisor, co-workers, or Office Information Technology (IT) staff member, to protect them from inadvertent disclosure to others.
5. Notify the Information Security Officer (ISO) if IT system users suspect their user accounts or passwords have been compromised.

The Office of Information Technology (OIT) will apply these password management practices to all accounts on the University IT systems and data.

1. Use passwords on all University IT systems that are classified as sensitive, including local accounts, remote access, and temporary accounts.
2. Configure sensitive University IT systems to allow users to change their initial password upon first time sign on, change their password every 90 days, change their password at will, and prevent the reuse of the same or similar passwords.
3. Define requirements for password length and complexity on all University IT systems that are classified based on sensitivity and risk.

4. Change default passwords immediately after installations.

5. Prohibit the transmission of identification and authentication data without the use of industry accepted encrypted standards.

6. Provide a unique initial password for each new user of sensitive IT systems and deliver the initial password to the IT system user in a secure and confidential manner.

7. Required that forgotten initial passwords be replaced rather than reissued.

8. Prohibit group account IDs and shared passwords on sensitive IT systems and the inclusion of passwords as plain text in scripts.

9. Limit access to files containing passwords to the IT system and its administrators.

10. Suppress the display of all passwords on the screen as they are entered.


12. Implement procedures to handle lost or compromised passwords and/or tokens.

13. Perform routine password cracking sessions on randomly selected resources and inform users of cracked accounts.

Definitions

Authentication is the process of verifying the identity of a user.

Authorization is the process of establishing and enforcing a user's rights and privileges to access specified resources.

Encryption is the process of converting computer data and messages to something incomprehensible by means of a key, so that it can be reconverted only by an authorized recipient holding the matching key.

Information Technology is the telecommunications, automated data processing, databases, the Internet, management information systems, and related information, equipment, goods, and services.
Title: Password Management Policy

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.

Password is a unique string of characters that in conjunction with a logon ID, authenticates a user's identity.

Password Management is the selection, distribution, use, modification, and testing of computer system passwords.

Token is a small tangible object that contains a built-in microprocessor utilized to store and process information for authentication.

References

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

Virginia State University (VSU):
  Policy 6510: Acceptable Use Policy
  Policy 6420: Electronic Records and Retention Policy
  Policy 6110: IT Resource Security Policy
  Policy 6640: Network Monitoring Policy
  Policy 6520: Security Awareness Training Policy
  Policy 6310: Banner Security Policy

APPROVED BY: ___________________________ 1/28/08
President Date

Revision Date: January 28, 2008  Page No:3