Title: Remote Access Policy

Purpose

The Remote Access policy identifies the steps required for the secure uses of remote access within the University enterprise network.

Policy Statement

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

Authority, Responsibility, and Duties

All University employees and contractors shall be required to complete a remote access request form to gain access to University IT systems through the network to transmit, process, and store data. At a minimum, Information Technology (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 cannot 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. 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) is required to provide secure remote access to the University enterprise network. At a minimum, the following practices are required to be followed:

1. Protect the security of all remote access to the University’s sensitive IT systems and data by means of encryption including session initiation, identification, authentication, and all exchanges containing sensitive data.

2. Protect the security of remote file transfer of sensitive data to and from University IT systems by means of encryption.

3. Document requirements for use of remote access, setting up remote access accounts, and creating connections for using remote access on the IT system user computers.

Revision Date:
4. Document requirements for the physical and logical hardening of remote access devices.

5. Require that IT system users complete remote access request forms. These IT system users should be provided a unique user ID and password prior to using the University's remote access capabilities.

6. Perform annual audits on remote access accounts and retain remote access documentation of security review until the next scheduled Information Security Audit or 3 years which ever is longer.

7. Maintain all remote access request authorization and account termination/deletion forms for active and terminated accounts for 1 year.

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.

Harden is the process of implementing software, hardware, or physical security controls to mitigate risk associated with Commonwealth of Virginia (COV) infrastructure and/or sensitive IT systems and data.

Information Security Officer (ISO) is responsible for overseeing the implementation of the University's Information Technology (IT) Security program.

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

Information Technology (IT) System Users includes Commonwealth of Virginia (COV) employees, contractors, vendors, third party vendors, 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.
References

Virginia Information Technology Agency (VITA):
Information Technology Security Standard (ITRM Standard 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
Policy 6630: Data Breach Notification Policy
Policy 6620: IT Security Handling Policy
Policy 6710: IT System and Data Backup and Restoration Policy
Policy 6410: Data Storage Media Protection & Encryption Policy

APPROVED BY: [Signature]
President
Date: 1/24/08