Virginia State University
Policies Manual

Title: Remote Access Policy Policy: 6320

Purpose

The purpose of the Remote Access policy is to establish and document usage restriction, configuration/connection requirements, and implementation guidance for remote access to the Virginia State University (VSU) Virtual Private Network (VPN). The intent is to provide secure and authorized remote connections and access to sensitive Information Technology (IT) data, systems, and resources while conducting University business.

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 interests. Refer to Information Security Policy 6110 for roles and responsibilities.

A. Technology Services

The Technology Services department is required to manage secure remote access technology to the University enterprise network.

1. Maintain hardening and configuration consistent with standards published by the Center for Internet Security.
2. Route all the access control points for remote access through a managed network access control point.
3. Perform regular review of audit logs.
4. Authorize the execution of privilege commands and access to security relevant information via information via remote access only and document the rationale for each such access in the security plan.
5. 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.
6. Require user name and password for Identification, Authentication and Authorization of credentials for usage of VPN services.
7. Protect the security of remote file transfer of sensitive data to and from University IT systems by means of encryption.
8. Provide the capability to expeditiously disconnect or disable remote access to the IT system within 60 minutes.
9. Document requirements for the physical and logical hardening of remote access devices.
10. 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.

11. Where supported by features of the system, terminate a user session after 30 minutes of Inactivity. Where not supported by features of the system, mitigating controls must be implemented or an exception must be filed.
12. Perform annual audits on remote access accounts and retain remote access documentation of security review until the next scheduled Information Security Audit or three years whichever is longer.
13. Maintain all remote access request authorization and account termination/deletion forms for active and terminated accounts for one year.
14. Monitor remote access connections for any unauthorized connections.

B. All Information Technology System Users

All IT system users will take steps to protect all data files from unauthorized use, disclosure, alteration, or destruction and be responsible for the security, privacy, and control of data within their control or view. At a minimum, IT system users are required to:

1. Obtain authorization from a supervisor or management by completing the Access Request form for secure VPN access.
2. Protect all data files from unauthorized use, disclosure, alteration, or destruction.
3. be responsible for the security, privacy, and control of data within their control or view.
4. Use approved VPN client software and/or approved supported Internet browser(s).
5. Notify the IT help desk and Information Security Officer (ISO) if IT system users suspect their user accounts or passwords have been compromised.

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/librarv.

Policy Statements

A. This policy applies to all Virginia State University employees, business partners, third-party vendors, and contractors who intend to remotely access the University's IT systems, data, and resources.

B. It is the policy of VSU that remote access processes and procedures for all University information systems will be consistent with current best practices and University IT Security Policies as follows:

   1. Remote access to the University's sensitive IT systems and data is protected by encryption in a manner consistent with VSU Data Storage Media Protection and Encryption Policy. This encryption requirement applies to both session initiation (i.e., identification and authentication) and to all exchanges containing sensitive data.

2. The security of remote file transfer of sensitive data to and from the University is protected by means of encryption.
3. The requirement for use of remote access and for remote access to sensitive data is consistent with the VSU and the Commonwealth of Virginia (COV) policies, standards, guidelines and procedures.
4. When connected to internal networks from VSU guest networks or non-VSU networks, data transmission shall only use full tunneling and not use split tunneling.
5. IT system users are required to obtain authorization and a unique user ID and password prior to using the University's remote access capabilities.
6. Physical and logical hardening of remote access devices is consistent with standards published by the Center for Internet Security.
7. Monitoring and logging is enabled and logs are maintained of all remote access.
8. Where supported by features of the system, session timeouts are implemented after a period of no longer than 30 minutes of inactivity and less, commensurate with sensitivity and risk. Where not supported by features of the system, mitigating controls are implemented.
9. Where possible, the remote sessions for accessing sensitive data or development environments employ two-factor authentication and are audited.
10. Remote Access privileges may be suspended or disabled if found a user violates the policies of the University or of the COY.

References

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

Approval By: ______________________________ Date: 5/10/16
President