VIRGINIA COMMONWEALTH UNIVERSITY

VCU

Remote Access Standard

Responsible Office: VCU Technology Services, Information Security
Initial Standard Approved: 08/2008
Current Revision Approved: 11/14/2016

Standard Statement and Purpose

In order to protect sensitive University information assets and minimize the risk of security incidents, uncontrolled access to certain University systems used to process, transmit, and store sensitive University information assets are restricted from locations that are external to the University and / or its security zone. In order ensure secure and reliable access to these systems from external locations, this standard delineates requirements for remote access to University information resources and the secure transmission of Category I and II data between a remote location and a resource in the University environment.

This Standard should be used in conjunction with the documents listed in the Related Documents section.

Noncompliance with this standard may result in disciplinary action up to and including termination. VCU supports an environment free from retaliation. Retaliation against any employee who brings forth a good faith concern, asks a clarifying question, or participates in an investigation is prohibited.

Table of Contents

Who Should Know This Standard

All faculty, staff, and students with the need to remotely access internal University information resources are responsible for knowing this standard and familiarizing themselves with its contents and provisions.

Definitions

Category I Information
Information protected under federal, state or industry regulations and / or other civil statutes, where if lost may require breach notification and cause potential regulatory sanctions, fines and damages to the institution's mission and reputation.

Category II Information
All proprietary data that if improperly released has the potential to cause harm to the institution, its mission or its reputation, but do not require breach notifications, and security or privacy of such data is not regulated or required by law or contract. Such data includes proprietary and properly de-identified research information, business related email or other communication records, financial information, employee performance records, operational documentations, contractual information, intellectual property, internal memorandums, salary information, and all other information releasable in accordance with the *Virginia Freedom of Information Act (Code of Virginia 2.2-3700)*.

Controlled Unclassified Information (CUI)
Information from federal agencies that requires the protection delineated under the NIST SP800-171 standards. These types of information typically are received as a part of a research project, and are required through the Federal Acquisition Regulation clauses. Although dubious at the moment, the U.S. National Archive is made the authoritative source for the definition of CUI, and the list of potentially covered information can be found at the National Archive CUI Registry: https://www.archives.gov/cui/registry/category-list.html

Criminal Justice Information (CJI)
Information regulated under the FBI Criminal Justice Information Services (CJIS) Security Standard, this includes any information provided by the FBI CJIS necessary for law enforcement and civil agencies to perform their missions including, but are not limited to biometric, identity history, biographic, property, and case / incident history data. Like many other regulations, CJIS Security Standards also carries a transient property, where whether an organization receives the data directly or indirectly from a third party, such data will be regulated by the security standards. The VCU Police Department and certain research projects may have access or store these data.

Data Custodian
The Data Custodians can have both a business and/or technical role, though it is typically considered a business role. The Data custodians are responsible for entering, modifying and maintaining data in the enterprise databases and information systems.

Data Steward
Data stewards are appointed by and report to the data trustees. Data stewards have knowledge of and work in accordance with numerous University rules and policies across the institution, including university policies on information security and privacy. Data stewards are essentially Executive Subject Matter Experts (ESMEs) for the business domains under their authority.

Data Trustee
Data Trustees will carry out plans and policies to implement appropriate data management practices as defined by industry regulations, federal and state statues, and University policies and procedures. Data trustees are high-level employees (e.g., vice presidents, vice provosts, and deans) appointed by and reporting to the President, including but not limited to Provost and Senior Vice President of Academic Affairs, Vice President of Finance, Vice President of Administration, Vice President of Research, or Senior Vice President of Health Sciences.

Federal Information Security Management Act (FISMA)
Federal Information Security Management Act (FISMA) requires the use of the National Institute of Science and Technology (NIST) Special Publication (SP) 800-53 as a common security framework for the management of various information belonging to federal government. The framework outlines the expected security controls for information that are rated at the low, moderate, or high level, where each level requires additional controls to be implemented. This regulation can impact the research projects involving federal government data, or projects that are funded by federal government. The moderate and high level controls are a set of minimal baseline set to handle any data with medium to high sensitivity.

Internal Management Sponsor
Within the context of this document, an Internal Management Sponsor is a VCU employee who is responsible for the verification, monitoring, and certification all contractors that are granted access to University resources. This role is usually at the level of the Authoritative Unit Head.

Internal University Resources
Within the context of this document, internal university resources refer to those computer and network resources that are accessible from the University networks, but are otherwise unavailable directly from other locations, such as an employee's home, a coffee shop, or another University.

Multi-Factor Authentication
Multi-factor authentication refers to the approach to authentication that requires the presentation of two or all of the three authentication factors: Something you know (e.g. password), something you are (e.g. Finger print), something you have (e.g. an ID, token or key).

Payment Card Industry Data Security Standard (PCI-DSS)
Payment Card Industry Data Security Standard is a set of comprehensive requirements for enhancing payment card data security. Compliance with the PCI DSS helps to alleviate vulnerabilities that put cardholder data at risk.

Remote Administrative Access
Within the context of this document, remote administrative access refers to the access to the underlying operating system or management interface of an IT system. Remote administrative access allows a system administrator to make changes to a system's functionality and security. Examples of remote administrative access includes Microsoft Remote Desktop Connections (RDC), Secure Shell Host (SSH), Remote Assistance Systems, and access to web based administration pages.

Sanctioned Public Facing Web Servers

Within the context of this document, a sanctioned public facing web server is an Internet-accessible server hosting web applications (e.g. websites) and provisioned following review and approval by the Information Security Office.

Security Zone
Within the context of this document, a security zone refers to a physical and / or logical segment that separates an area designed to handle a particular category of information from another. Examples of security zones include a dedicated and sealed network used to handle credit card information, or a dedicated and lockable room used to handle sensitive research projects.

System Owner
A system owner is an employee with the oversight responsibility for the management of an IT system. The system owner is typically not the administrator managing the system, but rather the departmental business manager and sponsor of the system. The system owner holds the authority to provision, de-provision, or modify the IT system to address specific business needs.

Virtual Private Network (VPN)
Within the context of this document, Virtual Private Network (VPN) refers to VCU's VPN installation that allows an individual from outside of the VCU network to access internal VCU network resources following the successful authentication of the individual.

Contacts

VCU Technology Services (Technology Services) officially interprets this standard. Technology Services is responsible for obtaining approval for any revisions through the appropriate governance structures. Please direct policy questions to the VCU Information Security Office (infosec@vcu.edu).

Standard Specifics and Procedures

The following requirements apply to access to internal university resources from off-campus.

A. General (Category III Systems)

The following requirements apply to general remote access to the University environment.

1. **Inactive Virtual Private Network (VPN) sessions time-out of no more than 48 hours.**
   All VPN sessions must be terminated after no more than 48 hours of inactivity. (J13)

B. Category II Systems

In addition to the requirements in the General (Category III Systems) Section, remote access to Category II data must also adhere to the following requirements:

1. **Except for sanctioned public facing web servers, remote access to all University Category I and Category II systems and devices require multi-factor authentication using the University's approved secure technology.**

2. **VPN for remote access.**
   All individuals requiring remote access to internal university resources from off-campus locations must use VCU centrally managed VPN utilizing multi-factor authentication. (J9, J10)

C. Category I Systems

In addition to the requirements in the Category II Systems Section, remote access to Category I data must also adhere to the following requirements:

1. **Remote access / method of access need formal authorization and approval.**
   The Data Steward in conjunction with the System Owner must approve all employee remote access requests. An internal management sponsor must approve all contractor remote access requests. All approved requests for employees and contractors must be recorded with the Data Stewards or System Owners or their designees. All remote access methods must be reviewed and approved by the Information Security Office. (F12)

D. Special Requirements

The following requirements apply to remote access to systems used to handle specific data types; all data types listed in this section are considered Category I data and must also adhere to the requirements listed in the Category I Systems Section.

1. **Require Multi-factor authentication for remote administrative access regardless of location.**
   Remote administrative access to the following data types requires multi-factor authentication regardless of location. The above requirement applies to CUI, FISMA (low+mod+high), and PCI-DSS data. (J11, J25)

2. **VPN configuration must not allow split-tunnel**
   VPN into networks containing the following data types must direct all user traffic through the VPN tunnel, including both traffic intended for the assets residing on internal network, as well as assets residing on other networks, including but not limited to the Internet.
   This requirement applies to CUI, FISMA (mod+high), and CJI data. (J26)

Forms

1. VCU Information Security Policy Exception Form

Related Documents

Information Technology Policies are located in the University's Policy Library. The Information Technology Policy Framework contains VCU Technology Policies, Standards and Baseline requirements.

1. Computer Network and Resources Use Policy
2. Information Security Policy
3. Exposure and Breach of Information Policy
4. Data Classification Standard
5. Network Management and Security Policy

Revision History

This Standard supersedes the following archived Standards:

Approval/Revision Date	*Title*
August 2008	Security Standard for Remote Access

FAQs

There are no FAQs associated with this policy and procedures.