UNIVERSITY OF SOUTH CAROLINA
Division of Information Technology

University Information Security Office

Secure Remote Access Guidelines

Issued Date: 30 June 2015

Effective Date: 30 June 2015

Purpose

This document informs readers of risks associated with remote access, and provides guidance on meeting the state's remote access requirements.

Scope

This guidance is intended for organizational units managing remote access to University data classified as *Confidential* or *Restricted*[1].

Adherence to this guidance does not absolve an organizational unit of its obligation to meet additional relevant compliance requirements (such as PCI-DSS[2] for credit card information or the HIPAA Security Rule[3] for electronic protected health information). Organizational units should refer to appropriate industry guidance to determine what, if any, additional safeguards are necessary.

The Information Security Office offers consulting services to organizational units in the planning, implementation, and assessment of safeguards.

Background

When unencrypted data is sent or received over the Internet, it can be exposed to unauthorized parties without the knowledge of the sender or the intended recipient. When data is accessed remotely, it is difficult to distinguish between a legitimate user and someone using stolen credentials. Stolen credentials are a leading cause for data breaches. For these reasons, organizations require specific safeguards (such as encryption and multifactor authentication) for individuals accessing data remotely.

In accordance with South Carolina Provisos 117.113 (2014) and 101.32 (2014), the state's Division of Information Security has issued security requirements[4] for all state agencies, published in April 2014 and effective July 2016. The requirements are wide reaching and based on the NIST Special Publications 800 series[5]. Per University policy, *Responsibility and Acceptable Use of Data, Technology, and User Credentials*, the University Information Security Office may issue guidance on implementing appropriate safeguards. Following this guidance is optional, however compliance with the state's requirements is not.

[1] According to Policy on Data and Information Governance, I.C.5
[2] https://www.pcisecuritystandards.org/security_standards/documents.php?document=pci_dss_v2-0#
[3] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/
[4] http://dis.sc.gov/PoliciesAndProcedures/Pages/default.aspx#Standards
[5] http://csrc.nist.gov/publications/PubsSPs.html

Definitions

Remote Access

The ability of an organization's users to access its nonpublic computing resources from locations other than the organization's facilities[6].

User

Any person(s) accessing University information technology assets, including but not limited to: students, faculty, staff, contractors, clients, consultants, invited guests, and others working at or for the University.

Related Roles and Responsibilities (from USC policy)

IT Staff / Data Custodians

- System administrators or staff assigned the responsibility of maintaining or supporting University information systems or assets will be responsible for implementing requirements outlined in [Responsibility and Acceptable Use of Data, Technology, and User Credentials] and established standards and procedures[7].
- Data Custodians will implement policies, standards, guidelines, and other requirements applicable to Institutional Data and information systems through their respective roles[8].

Data Steward

- Data Stewards determine data classification of data elements and information systems[9].

- [E]ach Data Steward is responsible for the following with respect to Institutional Data under his or her care: understand and apply security and privacy standards, guidelines, and practices; determine data classification of data elements…[10]

[6] Per NIST Special Publication 800-46 Rev. 1 (http://csrc.nist.gov/publications/PubsSPs.html)
[7] Policy on Responsibility and Acceptable Use of Data, Technology, and User Credentials
[8] Policy on Data and Information Governance, I.B.6
[9] Policy on Responsibility and Acceptable Use of Data, Technology, and User Credentials, II.A.7
[10] Policy on Data and Information Governance, I.B.3

Recommended Safeguards

DIS Control ID[11]	SC State Policy Control	Recommendation
2.116	Each organizational unit must implement encryption of data in motion to protect remote connections.	• TLS (https) for Web applications • SSH and RDP for OS access • VPN Client for remote access to network[12]
2.201	Each organizational unit must document allowed methods for remote access to the network and information systems.	• Organizational unit Procedure
2.202	Each organizational unit must utilize automated mechanisms to enable management to monitor and control remote connections into networks and information systems.	• OSSEC client for enterprise log monitoring[13] • UTS and organizational unit managed VPN solutions
2.203	Each organizational unit must require Virtual Private Network (VPN) or equivalent encryption technology establish remote connections into the organizational unit's private networks.	• UTS and organizational unit managed VPN solutions
2.204	Each organizational unit must restrict remote access to its private networks and systems to the mechanisms and protocols approved by the organizational unit.	• UTS and/or organizational unit managed firewalls[14] • UTS and/or organizational unit Network Access Control (NAC)[15]
2.205	Each organizational unit must require two-factor authentication for remote connections by Virtual Private Network (VPN) or other such tunneling technologies.	• DUO Security multi-factor authentication solution is available to all fac/staff and affiliates[16]

[11] Unique identifier for controls listed in Division of Information Security's standards (http://dis.sc.gov/PoliciesAndProcedures/Pages/default.aspx#Standards)
[12] UTS VPN https://sc.edu/about/offices_and_divisions/university_technology_services/services/network/vpn.php
[13] UISO OSSEC https://www.uts.sc.edu/itmanagers/documentation.shtml
[14] UTS Firewalls https://sc.edu/about/offices_and_divisions/university_technology_services/services/network/firewall.php
[15] UTS NAC http://www.sc.edu/about/offices_and_divisions/university_technology_services/support/help/wiredinstruction.php
[16] USC Multi-factor Authentication http://sc.edu/securecarolina/multifactor/

DIS Control ID[11]	SC State Policy Control	Recommendation
2.401	Each organizational unit must use multifactor authentication for remote user authentication to non-public systems, such that one factor is generated by a device other than the device from which the user connects.	• DUO Security multi-factor authentication solution is available to all fac/staff and affiliates
7.103	Each organizational unit only allows the use of handheld computing devices that have the ability to be remotely wiped / erased, for use with non-public organizational unit data.	• Whole Disk Encryption Winmagic solution is available for endpoint computers • Organizational unit procedure to require and train the user to set up "iCloud: Erase your device" and "Android Device Manager" on each authorized device.
7.117	Each organizational unit must develop a process for users to notify designated personnel when a device is lost or stolen. The process must include remote wiping / erasing of handheld computing devices.	• Notification is required by policy IT 3.00 to support the Information Security Office's responsibility for incident response • Organizational unit procedure to perform remote wipe / erasure
11.207	Each organizational unit ensures that information systems are sufficiently monitored to detect attacks and/or signs of potential attacks, including unauthorized network local or remote connections.	• OSSEC for enterprise host monitoring • Snort sensors to be deployed at each internet connection for network intrusion detection[17]

Contacts

http://security.sc.edu

Revision History

Author	Date	Comments
John Sturgis	29 June 2015	Draft Revision
Kyle S. Brown	29 June 2015	Formatting for publication

[17] USC Security Monitoring https://sc.edu/about/offices_and_divisions/university_technology_services/services/security/security_monitoring.php