Information **T**echnology
Policy & Procedures

Security Practices on Remote Access Services

1.0 Purpose

These practices define the requirements to authorize a user to connect to Central Connecticut State University's wired and wireless networks, or to access a University resource from an off campus location. These requirements are intended to comply with the State of Connecticut's Personal Wireless Device Policy and to reduce the University exposure to damages from unauthorized access of University resources. Damages include but are not limited to the loss of sensitive or confidential information, damage to public image and damage to critical University systems.

2.0 Scope

This policy applies to all employees, contractors, vendors and agents with a Central Connecticut State University owned or personally owned computers used to connect to the University network or access a University resource that is not available to the general public.

This policy applies to short term (less than 24 hours) remote access connections used to do work on behalf of the University as well as projects or research that use University resources.

This policy **does apply** to smart phones, PDA, or tablet devices that connect to the University's email servers for the sole purpose of reading and sending email.

Remote access includes but is not limited to Virtual Private Network (VPN), direct connections to servers or workstations, remote desktop, accessing network shares (department or personal), and application portals such as https://apps.ccsu.edu.

3.0 Policy

1. The acceptable use policy for use of computer resources applies to all forms of remote access. This policy can be found here http://www.ct.edu/files/it/BOR_IT-001.pdf.

2. The storage of Personally Identifiable Information (PII) or confidential information is strictly prohibited. Confidential information includes but is not limited to information covered by PCI, HIPPA, or FERPA. This data can only be stored on your department's secured network drive.

    a. Additionally, printing of PII or confidential information to public printers is prohibited.

3. Remote access to public applications in Citrix (i.e. Word, Excel, etc.) will be automatically granted to all University personnel.

4. Access to remote administrative applications (i.e. Remote Desktop) will only be granted on an as needed basis and only to those resources that are requested.

a. Log in to https://hsm.ccsu.edu and complete the Remote Opt-in Request.

b. Access will be for a limited period of time not to exceed 1 year. Prior to the end date an email will be sent to you asking if access is still needed. You must confirm that access is still need or it will be automatically removed.

i. All access is automatically ended on October 31st.

5. Remote sessions will automatically be disconnected if idle or after a maximum of 12 hours of use.

6. You are responsible for ensuring the workstation and network you use is secure. This includes current patches and anti-virus definitions.

7. When using a mobile device including, but not limited to, cell phones, PDA, and tablets to remotely access a University resource (including email) they must be protected by a lock screen.

a. The device must at a minimum automatically lock after 15 minutes of inactivity.

b. The screen may be unlocked by a passcode/PIN. If a PIN is used it must be at least four (4) digits long.

c. It is recommended, but not required, that the device be protected by encryption.

d. The prohibition against storing PII or confidential data in section 2 applies to mobile devices as well.

8. Lost or stolen equipment (including that which is personally owned) must be reported to the CIO or his/her designee immediately.

9. You are responsible for ensuring that all University data is properly removed from any computer you may have used to access such data.

10. Requests for exception to this policy should be directed to the CIO or his/her designee.

Additional Resources

State of Connecticut Personal Wireless Device Policy –

http://www.ct.gov/opm/lib/opm/secretary/personaltelecommunicationsdeviceswebversion3.pdf

---

Practices are based off of NIST special Publication 800-114 11/2007, State of Maryland Depart of Information Technology Remote Access Policy 2.0 9/2009, SANS Institute Remote Access Policy 2006 and Georgia Health Sciences Medical Center (GHSMC) Mobile Device and Remote Access Policy 10/2012