Remote Access Policy

Document Type:	Policy (PLCY)		
Endorsed By:	Information Technology Policy Committee	Date:	4/29/2011
Promulgated By:	Chancellor Herzog	Date:	6/20/2011

I. Introduction

Where warranted, certain Connecticut Community Colleges (CCC) internal resources may be remotely accessible for those employees who perform CCC business from a remote location, such as home or when traveling. While measures have been taken to secure this type of connection, remote access is inherently a security risk. Consequently, policy, standards and procedures are required to minimize this risk.

II. Purpose

The purpose of this policy is to define requirements for connecting to the Connecticut Community Colleges (CCC) network from external devices via remote access technology. These requirements are designed to minimize the potential exposure to the CCC from unauthorized use and/or malicious attack that could result in loss of information or damage to critical applications.

III. IT Policies Common Provisions Apply

All provisions identified in the IT Policy Common Provisions apply to this specific policy, unless otherwise noted.

IV. Scope

This policy applies to all CCC employees, contractors and other affiliates (vendors, agents, etc.) who utilize CCC, or personally owned devices to remotely access the CCC network. This policy applies to remote access connections used to perform work-related activities on behalf of the CCC. Employment at CCC does not automatically guarantee the granting of remote access privileges.

Remote access is the ability to securely access systems, applications or data that can normally only be accessed within the internal CCC network. Examples of these applications are as follows:

- Internal Administrative/Academic Systems
- Internal websites
- Documents/Files located on internal file servers
- Local college resources
- Servers

Remote Access to the CCC resources is provided on a volunteer basis and is considered an extension to your current work environment. It is not intended to be a replacement to said environment.

V. Supported Technology

All remote access will be centrally managed by System Data Center (SDC) and will use appropriate security measures based on access requirements.

VI. Application Process

All employees requiring remote access for business purposes must go through an application process that clearly outlines why the access is required and what level of service the employee needs should his/her application be accepted. The Remote Access Agreement must be approved and signed by the employee’s unit manager, supervisor, or department head before submission to the local IT department. The local IT department will submit the application to the Chief Information Officer (CIO), on behalf of the Chancellor, for final review.

VII. Access Restrictions

Remote Access to DCL3 data (formerly referred to as PCI Identity Data) is restricted and can only be accessed using a secured CCC system meeting DCL3 security standard. This type of access requires additional approval by the Appropriate CCC Authority.

VIII. Requirements

It is the responsibility of all individuals with remote access privileges to ensure that their remote access device and connection is given the same security considerations as their on-site connection and CCC device. It is imperative that any remote access device/connection used to conduct CCC business be utilized appropriately, responsibly, and ethically. Therefore, the following requirements must be observed:

1. Regularly review all CCC Information Technology Policies for details of protecting information when accessing the CCC network via remote access methods, and acceptable use of the CCC network.

2. Employees will use secure remote access procedures. Employees agree to never disclose their passwords to anyone, particularly to family members if business work is conducted from home. Refer to the CCC Password Policy for additional requirements.

3. All remote access users using personal devices connected to the CCC network must maintain all required security standards on said devices including, but not limited to:

    - Valid and up to date virus protection
    - Malware protection
    - Maintaining current OS and application security patches

4. All remote access users using personal devices connected to the CCC network will notify the appropriate IT staff of possible infections while accessing services remotely.

5. The remote access user also agrees to immediately report to their manager and local IT department any incident or suspected incidents of unauthorized access and/or disclosure of CCC resources.

6. All remote access connections must include a “time-out” system. In accordance with CCC security policies, remote access sessions will time out after a specified period of inactivity. The

time-out will require the user to reconnect and re-authenticate in order to re-enter company networks.

7. The remote access user also agrees to and accepts that his or her access and/or connection to CCC networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. As with in-house computers, this is done in order to identify accounts/computers that may have been compromised by external parties.

8. The remote access user also understands that there may be specific rules listed in the remote access application that must also be adhered too. These rules are specific to the application you are using to connect to the CCC network.

IX. Support

Remote access to the CCC network is provided as an extension of your normal work environment. Remote access support is provided during Normal Business Hours. If you are using remote access to provide off-hours support and you experience issues with connectivity, you may have to travel to your office to provide said support.

X. Enforcement

Failure to comply with this policy may result in the suspension of remote access privileges, disciplinary action, and possibly termination of employment.

XI. Revision History