Connecticut Community Colleges

Information Technology

Policies, **Standards**, Procedures, etc.

Citrix Remote Access Agreement

Document Type:	Standard (STAND)	Revision Date: 6/10/2011
Endorsed By:	Information Technology Policy Committee	

Table of Contents

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.

Purpose

The purpose of this agreement is to request remote access via Citrix to the CCC network from an external device.

Supported Technology

All remote access will be centrally managed by System Data Center (SDC) and will use appropriate security measures based on access requirements. At this time, the CCC utilizes Citrix to provide remote access functionality for administrative functions. This is done via a secure web connection (https://ris.commnet.edu).

Support

Remote access to the CCC network is provided as an extension of your normal work environment. Remote access support is provided via the BOR IT Support Center. If you are having issues connecting remotely outside of normal business hours, the following must be observed:

1. 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.
2. Go to the Citrix Support Site for online documentation and contact information for support.

Access Restrictions

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

The following are requirements to access DCL3 data:

- Can only be accessed using a secured CCC system meeting DCL3 security standard. This includes remote access to Internet Native Banner, which requires additional approval by the Appropriate CCC Authority.
- Network access is only through a secured network
- Wireless networks need to be secured from unauthorized access and encrypted with WPA2

Remote Access Form

Fill in the systems, applications, etc. that you are requesting remote access to:

Application/System	Requesting Access? (yes or no)
Microsoft Office Suite (Outlook, Word, Excel, Powerpoint, Access)	
Access to documents/files located on a CCC file server (user/department shares, etc.)	
Internal College/System Web Sites	
Internet Native Banner ***Note: requires additional approval**	
List Other Applications/Systems:	

Access to Local Citrix Functions

By design, the Citrix Remote Information Services (RIS) environment contains restrictions on the use of some "local access functions". The restrictions are in place as a security precaution to limit the possibility of sensitive data being stored on non-CCC owned devices. These "local access functions" are:

- Copy and Paste
- Printing locally (e.g. off-site, home printer)
- Saving locally (e.g. off-site, home PC)

Although the security risks still exist for these functions, in some instances, these functions are needed in order to effectively work remotely using the Citrix RIS environment.

Select the Local Access Functions being requested:

Local Access Function	Requesting Access? (yes or no)
Copy and Paste	
Printing locally (e.g. off-site, home printer)	
Saving locally (e.g. off-site, home PC)	

Important Note: By requesting the "local access functions", the potential exists for CCC data to be processed, transmitted, stored or printed on my local non-CCC owned device. When using these "local access functions", users should not save or print any DCL3 and DCL2 data to off-site (non-CCC owned) devices. DCL3 data can only be stored on CCC network shares and printed on CCC printers. If DCL3 and DCL2 data needs to be accessed using Citrix, the user is responsible to ensure appropriate security precautions are taken to protect the data in accordance with CCC policies, standards and procedures (www.commnet.edu/it/policy).

Employee Information

Please clearly outline why remote access is required and what level of service is required:

_____

_____

_____

Name (Print): Last: _____ First: _____

NetID: _____ College: _____

Department: _____

Job Title: _____

I have read, understand and am fully aware of the terms of this agreement and the Remote Access Policy, and consent to adhere to the requirements outlined therein. I understand that use of remote access may permit me to engage in CCC business outside of my normal work hours and agree not to assert such use for the purpose of seeking additional compensation, time off or a schedule adjustment, unless such work was done with prior supervisory approval.

_____ _____

Employee Signature Date

Responsible Manager / Approval Authority

This remote access request must be approved and signed by the employee's unit manager, supervisor, or department head before moving forward.

Remote Access Request (check one): ☐ **Approved** ☐ **Denied** ☐ **Modified**

Comments (if any): _____

_____

_____

_____ _____

Name Title

_____ _____

Signature Date

Approval for access to Internet Native Banner

Due to the inherent risks associated with remote access to Internet Native Banner, additional approval is required by the Appropriate CCC Authority (Chancellor, College President or designee).

INB Remote Access Request (check one): ☐ **Approved** ☐ **Denied** ☐ **Modified**

Comments (if any): _____

_____ _____

Name Title

_____ _____

Signature Date

IT Dean/Director

The IT Dean/Director needs to be aware of this request, in order to assist in providing access to documents/files located on a CCC file server (user/department shares, etc.).

_____ _____

Name Title

_____ _____

Signature Date

Note: Please email this completed/signed form to the BOR IT Support Center for signature by the CIO.

CIO Review / Request Processing

The Chief Information Officer (CIO), on behalf of the Chancellor, will perform the final review.

Remote Access Request (check one): ☐ **Approved** ☐ **Denied** ☐ **Modified**

Comments (if any): _____

_____ _____

System CIO Signature Date

Internal Processing Use Only:

Processed by: _____ Date Processed: _____