1. 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.

2. Purpose
   The purpose of this agreement is to request remote access to CCC internal resources from an external non-CSCU owned device.
3. **Supported Technology**
   Remote access is centrally managed by the CSCU System Office and will use appropriate software and security measures based on access provided and requirements.

4. **Support**
   Remote access to the CCC network is provided as an extension of your normal work environment. Remote access support is provided via the 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 IT Support Center’s Remote Access page for additional resources.

5. **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.
6. **Access Requested**

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

<table>
<thead>
<tr>
<th>Application/System</th>
<th>Requesting Access?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access to documents/files located on a CCC file server (department shares, etc.)</td>
<td></td>
</tr>
<tr>
<td>Internal College/System Web Sites</td>
<td></td>
</tr>
<tr>
<td><strong>List other Applications/Systems:</strong></td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:** Access to user shares or Microsoft applications no longer requires remote access as access is provided through [O365 portal](#). Access to Banner is now available from the [CSCU Protective Enclave](#).

**Citrix Local Access Functions**

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

If needed, select Citrix Local Access Functions being requested:

<table>
<thead>
<tr>
<th>Citrix Local Access Function</th>
<th>Requesting Access?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy and Paste</td>
<td></td>
</tr>
<tr>
<td>Printing locally (e.g. off-site, home printer)</td>
<td></td>
</tr>
<tr>
<td>Saving locally (e.g. off-site, home PC)</td>
<td></td>
</tr>
</tbody>
</table>

**Important Note:** By requesting access, the potential exists for CCC data to be processed, transmitted, stored or printed on the local non-CCC owned device. When using any of these Citrix Local Access Functions, users should not save or print any DCL3 or DCL2 data to non-CCC owned devices. The [CSCU Protective Enclave](#) must be used to access all DCL3 data.
7. Signatures

**Employee**

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 all CSCU policies and standards, 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 request for remote access 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

__________________________________  _____________________________
Signature      Date

Name      Title
**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.).

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Signature  Date

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

**CIO Review / Request Processing**
The Chief Information Officer (CIO) will perform the final review.

Remote Access Request (check one):  [ ] Approved  [ ] Denied  [ ] Modified

Comments (if any): ________________________________________________________

________________________________________________________________________
________________________________________________________________________

___________________________________ _______________________________
CIO Signature     Date

___________________________________
Internal Processing Use Only:
Processed by: _________________________________ Date Processed: _______________

Type of access provided: __________________________________________________________