1.1 IT Policy Common Provisions

Document Type: Policy (PLCY)  
Endorsed By: Information Technology Policy Committee  
Promulgated By: Chancellor Herzog  
Date: 4/29/2011  
Date: 6/16/2011

Table of Contents

I. Introduction
II. Purpose
III. Organization of Policies
IV. Scope
V. General Responsibilities
VI. Roles and Responsibilities
VII. General Provisions
   1. Access to IT Policies
   2. Policy Interdependencies
   3. Policy Authority
   4. No Expectation of Privacy
   5. Access Restrictions
   6. Violations of Law and Policy
VIII. Exceptions
IX. Disclaimer
X. Notice to Users
XI. Revision History

I. Introduction

Information Technology policies, standards and procedures promote consistency, efficiency and effectiveness in delivering secure IT services in support of the CCC educational mission.

*IT Policies* delineate institutional requirements regarding what should be done. Implementation of policies require standards and procedures to become successfully operational. In this way, policies shape our day-to-day business practices.

*IT Standards* provide specific guidance about how things need to be done. Standards specify technical architectures and operational requirements. Standards and guidelines change as technology and the institution's technical architecture changes.

*IT Procedures* are detailed, step-by-step instructions for performing specific tasks which implement the policy in the context of established standards. Procedures change in response to changes in standards or in response to events which indicate shortcomings in established procedures.

Compliance with IT Policy is mandatory. Every CCC staff, faculty, and student should understand and follow CCC policies. Failure to follow a policy can result in disciplinary action up to and including termination. Special approval from an *Appropriate CCC Authority* must be granted for exceptions to approved policies. Policies may change over time in response to the changing needs of the institution.
II. Purpose

Information Technology Policy provides the framework for the development and implementation of the CCC system-wide IT Services and the Information Security Program. This document details the general provisions, responsibilities, etc., which are applicable to all specific IT policies unless otherwise noted.

III. Organization of Policies

IT Policies are clustered into several policy areas for organizational purposes. These policies should be viewed as an integrated whole, rather than as individual unrelated policies.

IV. Scope

IT Policy applies to:

- All IT resources owned or managed by the CCC
- All IT resources provided by the CCC through contracts and other agreements with the CCC
- All users and uses of CCC IT resources

IT resources are not isolated to computerized records but include information on any media including but not limited to electronic, magnetic, optical or paper media.

In support of IT Policies, standards and procedures shall be developed, published and maintained. Where IT Standards and Procedures do not exist, each college is responsible for policy implementation.

IT Standards and Procedures can be extended by the colleges with more restrictive requirements but the extensions must be consistent with all higher-level standards and procedures and may not invalidate, diminish or oppose such higher level standards and procedures.

VI. Responsibilities

Chancellor

IT Policies are issued by the Chancellor of the CCC after consultation with appropriate councils, including the Council of Presidents and the Information Technology Policy Committee (ITPC).

Information Technology Policy Committee (ITPC)

The ITPC is a high-level, representative policy committee that is charged with reviewing and recommending to the Chancellor all policies related to CCC IT resources.

CIO Management Advisory Committee (CIO/MAC)

The CIO/MAC is a standing management-level advisory committee charged by the Chancellor to review, discuss, refine and ultimately approve, key operational strategies for addressing enterprise network infrastructure, information security, and other strategic IT initiatives as deemed appropriate.

Information Security Program Office (ISPO)

The Information Security Program Office (ISPO) is responsible for the development, implementation and maintenance of a comprehensive Information Security Program for the Connecticut Community Colleges. This includes security policies, standards and procedures which reflect best practices in information security for higher education.

VII. General Provisions

1. Access to IT Policies

The office of the Chief Information Officer (CIO), in consultation with ITPC, will provide an information framework in which IT policies, standards and procedures will be generally accessible to the CCC community for review and reference.

2. Policy Interdependencies
The CCC is an agency within the State of Connecticut and is required to comply with state regulations, such as No Expectation of Privacy and Record Retention Schedules. The CCC is also required to comply with federal regulations, such as Federal Education Rights and Privacy Act (FERPA). Each organizational layer includes interdependencies in the development and implementation of CCC Policies, Standards and Procedures.

CCC Policies, Standards and Procedures may extend state and federal requirements but cannot contravene them without explicit exceptions stated in the higher-level policies.

3. Policy Authority

The Chancellor has been granted the authority to promulgate IT policies by Board of Trustees (BOT) in the BOT Information Technology Resources Policy, Section 2.8.1.

4. No Expectation of Privacy

There is no expectation of privacy in the use of CCC IT resources. The CCC reserves the right to inspect, monitor and disclose all IT resources including files, data, programs and electronic communications records without the consent of the holder of such records. State of CT Electronic Monitoring Notice.

5. Access Restrictions

Use of CCC IT resources may be wholly or partially restricted or rescinded by CCC without prior notice and without the consent of the user under conditions such as

- when required by and consistent with law
- when there is reason to believe that violations of law or the CCC policies have taken or may take place
- when there are compelling circumstances

Restriction of use under such conditions is subject to appropriate procedures or approval of Appropriate CCC Authority.

6. Violations of Law and Policy

The CCC considers any violation of IT policy to be a serious offense and reserves the right to copy and examine any files or information resident on CCC IT resources to ensure compliance. Violations of IT policy should be reported to the Appropriate CCC Authority.

Sanctions of Law

Both federal and state laws prohibit theft or abuse of IT resources. Abuses include but are not limited to unauthorized entry, use, transfer, tampering with the communications of others, and interference with the work of others and with the operation of IT resources. Violations of law may result in criminal penalties.

Disciplinary Actions

Violators of IT Policy may be subject to disciplinary action up to and including dismissal or expulsion pursuant to applicable Board policies and collective bargaining agreements.

VIII. Exceptions

The only exceptions to this policy and related IT policies, are noted within the policies found here.

IX. Disclaimer

CCC disclaims any responsibility for and does not warranty information and materials residing on non-CCC systems or available over publicly accessible networks. Such materials do not necessarily reflect the attitudes, opinions or values of CCC, its faculty, staff or students.

X. Notice to Users

As laws change from time to time, IT Policy may be revised as necessary to reflect such changes. It is the responsibility of users to ensure that they have reference to the most current version of the IT Policy.

XI. Revision History
Network Policy
(Issued on March 5, 2007 by Chancellor Herzog)

I. INTRODUCTION

II. GENERAL PROVISIONS
   A. PURPOSE
   B. SCOPE
   C. DEFINITIONS
   D. RESPONSIBILITIES
   E. VIOLATIONS OF LAW AND POLICY
   F. NO EXPECTATION OF PRIVACY

III. WIRED AND WIRELESS NETWORKS

IV. WIRELESS NETWORKS ONLY

V. NETWORK ACCESS

VI. DISCLAIMER

VII. NOTICE TO USERS

I. INTRODUCTION

This Policy governs wired and wireless networks within the Connecticut Community Colleges (CCC). Furthermore, it defines network access from CCC owned and Non-CCC owned devices. In developing this policy, careful consideration was made in balancing many variables including security, risk, ease-of-use, and cost in an academic computing environment.

II. GENERAL PROVISIONS

   A. PURPOSE

   The purpose of this Policy is to:
   • Ensure that CCC network resources are used for purposes appropriate to the CCC mission and goals;
   • Prevent disruptions to and misuse of CCC network resources;
   • Ensure that the CCC community is aware that use of CCC network resources is subject to state and federal laws and the CCC policies; and
   • Ensure that network resources are used in compliance with those laws and the CCC policies.

   B. SCOPE

   This Policy applies to:
   • All network resources owned or managed by the CCC;
   • All network resources provided by the CCC through contracts and other agreements with the CCC; and
   • All users and uses of CCC network resources.

   C. DEFINITIONS

   The following terms are used in this Policy. Knowledge of these definitions is important to an understanding of this Policy:

   Appropriate CCC Authority: Chancellor, College President or designee.

   Authorized Networks: Networks that are explicitly installed and operated or authorized by the cognizant CCC IT authority.

   Cognizant CCC IT Authority: IT authority designated by the appropriate CCC Authority.
Compelling Circumstances: Circumstances in which time is of the essence or failure to act might result in property loss or damage, adverse effects on CCC resources or services, loss of evidence of one or more violations of law or of CCC policies or liability to CCC or to members of the CCC community.

Discreet User Authentication: Generic, pre-expired user accounts that are valid for a day and are used exclusively for public library devices.

Limited User Authentication: To be used only for a limited number (5-6) of unauthenticated, CCC-owned library computers that have a hard-wired network connection.

Internet Available Resources: Internet services which are available over http, https and all CCC Internet available resources (for example: Banner Self-Service, Libris, WebCT, college websites, etc.)

Isolated User Authentication: To be used in a restricted-use, isolated, high-tech classroom, where authorized. The instructor is responsible for insuring that the students follow the CCC IT policies.

Network Active Component: Network devices that forward or moves packets along or between networks such as Wireless Access Points, switches, routers, etc.

Network Resources: This includes, but is not limited to, wired and wireless networks, network addresses, network ports, network infrastructure, network active components, the devices that are connected to the network, etc.

Non-CCC Owned Devices: Any device that uses CCC network resources and is not owned by the CCC.

Vetted: A computer that has been inspected against and has passed a list of security requirements. For example, a vetted computer is up-to-date with operating system service packs and patches, is running an anti-virus program and is up to date with anti-virus definition files.

Wireless Network: Local area network technology that uses radio frequency spectrum to connect computing devices to CCC wired networks and the Internet.

Wireless Resources: Wireless access points, antennas, cabling, power, and network hardware associated with the deployment of a wireless network and the devices that connect wirelessly to it.

D. RESPONSIBILITIES

Policy. This Policy was issued by the Chancellor of the CCC after consultation with appropriate councils, including the Council of Presidents and the Information Technology Policy Committee.

Implementation. In support of this Policy, system standards and procedures shall be developed, published and maintained. And where CCC standards and procedures do not exist, each college is responsible for policy implementation.

Informational Material. Each college shall ensure that users of CCC IT resources are aware of all IT policies, standards, and procedures as appropriate.

E. VIOLATIONS OF LAW AND POLICY

The CCC considers any violation of this Policy to be a serious offense and reserves the right to copy and examine any files or information resident on CCC IT resources to ensure compliance. Violations of this policy should be reported to the appropriate CCC authority.

Sanctions of Law. Both federal and state law prohibit theft or abuse of IT resources. Abuses include (but are not limited to) unauthorized entry, use, transfer, tampering with the communications of others, and interference with the work of others and with the operation of IT resources. Any form of harassing, defamatory, offensive, illegal, discriminatory, obscene, or pornographic communication, at any time, to any person is also prohibited by law. Violations of law may result in criminal penalties.

Disciplinary Actions. Violators of this Policy may be subject to disciplinary action up to and including dismissal or expulsion pursuant to applicable Board policies and collective bargaining agreements.

F. NO EXPECTATION OF PRIVACY

There is no expectation of privacy in the use of CCC IT resources. CCC reserves the right to inspect, monitor, and disclose all IT resources including files, data, programs and electronic communications records without the consent of the holder of such records.

III. WIRED AND WIRELESS NETWORKS

All network resources are under the purview of the cognizant CCC IT authority. Only network resources
explicitly managed or authorized by the cognizant CCC IT authority are permitted. As such, unless authorized:

- devices can not run network services (including but not limited to DHCP, WINS, DNS, Active Directory Domain Controllers).
- the use of any device in "promiscuous mode" is not permitted.
- extending the network (including but not limited to hubs, wireless access points, modems) is not permitted.

All network resources must:

- be physically secured from theft or vandalism, that are owned by CCC;
- employ active network management (including but not limited to usage, activity, access);
- be secured from unauthorized access;
- adhere to all applicable health, building, fire codes and federal and state regulations;
- have upgradeable firmware for devices that have active components; and
- employ appropriate operating system service packs and patches to comply with the End User Device Security Policy.

IV. WIRELESS NETWORKS ONLY

Wireless networking is not a strategic replacement for a wired network. In the future, wired technologies are likely to improve significantly faster than those of wireless. A wireless network must be an augmentation of a wired network and is only appropriate for "common or transient areas" where students, staff, and faculty gather. Those areas include, but are not limited to: instructional labs, public areas, and research labs.

Due to the limited and shared bandwidth constraint of wireless networks, it is only appropriate for applications that have very low bandwidth requirements such as general email and web browsing. The shared bandwidth constraint also limits the number of users connected to a wireless network at one time.

The FCC does not license use of the frequencies used by wireless devices and therefore other devices that use the same frequencies may disrupt wireless communications. These devices include but are not limited to cordless phones, microwave ovens, and personal network devices. Areas with high interference from such devices may not be suitable for wireless networks.

Wireless Networks must:

- be centrally administered as a component of the local area network (LAN);
- be regularly scanned for rogue APs; and
- use supported radio frequency bands.

Access Points must:

- be physically secured from access to the data port by locked security boxes;
- be physically located towards the center of the intended coverage area so that radio waves do not radiate beyond the perimeter of the intended coverage area;
- be managed over a hard wired administration port and never over the wireless network;
- have wireless access to the administration port disabled at all times;
- have passwords changed initially and at regular intervals thereafter; and
- be configured to have encryption enabled; where encryption keys must be changed at regular intervals and must not be posted publicly.

V. NETWORK ACCESS

Prior to attempting to access CCC IT resources, users must be presented with the IT Resource Access Message. Encrypted user authentication is then required and subsequent access is based on the following chart. The cognizant CCC IT authority determines the appropriate access.

<table>
<thead>
<tr>
<th>Ref #</th>
<th>Device Ownership</th>
<th>Device Auth</th>
<th>User Auth</th>
<th>Vetted</th>
<th>Access</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CCC owned</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Access based on credentials/permissions.</td>
<td>CCC workstations (default).</td>
</tr>
</tbody>
</table>

Network Access Chart
<table>
<thead>
<tr>
<th></th>
<th>CCC owned</th>
<th>Yes</th>
<th>Limited</th>
<th>Yes</th>
<th>Internet available resources only</th>
<th>Exclusively for library public devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>CCC owned</td>
<td>Yes</td>
<td>Limited</td>
<td>Yes</td>
<td>Internet available resources only</td>
<td>Exclusively for Isolated, high-tech classes where authorized</td>
</tr>
<tr>
<td>3</td>
<td>Non-CCC owned</td>
<td>None</td>
<td>None</td>
<td>No</td>
<td>Internet available resources only</td>
<td>Exclusively for non-CCC owned devices</td>
</tr>
</tbody>
</table>

**VI. ACCESS RESTRICTIONS**

Use of CCC IT resources may be wholly or partially restricted or rescinded by CCC without prior notice and without the consent of the user under conditions such as:

- when required by and consistent with law;
- when there is reason to believe that violations of law or the CCC policies have taken or may take place; or
- when there are compelling circumstances.

Restriction of use under such conditions is subject to appropriate procedures or approval of appropriate CCC authority.

**VI. DISCLAIMER**

CCC disclaims any responsibility for and does not warranty information and materials residing on non-CCC systems or available over publicly accessible networks. Such materials do not necessarily reflect the attitudes, opinions or values of CCC, its faculty, staff or students.

**VII. NOTICE TO USERS**

As laws, technology and standards change from time to time, this Policy may be revised as necessary to reflect such changes. It is the responsibility of users to ensure that they have reference to the most current version of CCC Policies.

**Revision History**

Obsolete Wireless Policy
Security for Mobile Computing and Storage Device Policy

INTERIM (Issued and Effective on October 9, 2007 by Chancellor Herzog)

I. INTRODUCTION

II. GENERAL PROVISIONS
   A. SCOPE
   B. DEFINITIONS
   C. RESPONSIBILITIES
   D. VIOLATIONS OF LAW AND POLICY
   E. NO EXPECTATION OF PRIVACY

III. SECURITY REQUIREMENTS FOR PCI DATA

IV. ADDITIONAL SECURITY REQUIREMENTS FOR PCI IDENTITY DATA

V. GENERAL SECURITY REQUIREMENTS

VI. FUTURE SECURITY REQUIREMENTS

VII. NOTICE TO USERS

I. INTRODUCTION

This Security for Mobile Computing and Storage Device Policy within the Connecticut Community Colleges ("CCC") is established to ensure the security of Protected Confidential Information ("PCI" or "PCI Data") that may be stored on those devices. This is an interim policy that may be modified as additional operational and technical solutions are developed to address the issues. Ultimately, all CCC IT policies will be subject to the appropriate internal discussions and review before becoming permanent.

II. GENERAL PROVISIONS

A. SCOPE

This policy covers all CCC employees, whether permanent or non-permanent, full or part-time, and all consultants or contracted individuals retained by any of the CCC, who have access to PCI (herein referred to as "users").

This policy covers mobile computing devices and mobile storage devices (herein referred to as "mobile devices"). This includes both CCC owned devices as well as non-CCC owned devices used by employees or others in the conduct of CCC business.

B. DEFINITIONS

The following terms are used in this Policy. Knowledge of these definitions is important to an understanding of this Policy:

CCC Authority - the Chancellor, a College President or his/her designee.

Mobile Computing Device - The term "mobile computing device" refers to a portable computing or telecommunications device that can execute programs. This definition includes, but is not limited to, notebooks, palmtops, PDAs, IPods, BlackBerry devices, and cell phones with internet synching/browsing capability.

Mobile Storage Device - The term "mobile storage device" includes but is not limited to, mobile computing devices, diskettes, magnetic tapes, external/removable hard drives, flash cards (e.g., SD, Compact Flash), thumb drives (USB keys), jump drives, compact disks, digital video disks, etc.

Non-CCC Owned Device - Any mobile computing or mobile storage device that the CCC did not purchase and/or does not own.

Protected Confidential Information - Data, which if exposed to any security risk or otherwise disclosed, would violate Federal or State law or CCC contract or policy. PCI data includes
   - PCI Identity Data, as described in the next definition,
• Non-Public Directory Information,
• Academic Data,
• Other confidential data which may be further defined as part of a comprehensive Data Classification Policy.

**PCI Identity Data** - PCI Identity Data is a sub-set of the broader PCI category, and includes the following data elements which, if improperly disclosed, could be used for identity theft or to cause financial harm to an individual or the CCC if used in conjunction with other available information (e.g. name, address, telephone number, etc.):

- Social Security Number
- Date of Birth
- Mother’s Maiden Name
- Student Loan Data
- Bank Account Numbers
- Credit Card Numbers

**Data Classification Policy** - A policy which defines high level categories of data for the purpose of managing data and information assets with regard to their level of confidentiality and criticality. PCI, as defined in this policy, is the first category to be defined as part of a comprehensive CCC data classification policy. When the CCC policy is fully developed, it will address additional categories such as information that is for internal use only and information that is available to the public.

**Secure Mobile Device** - A mobile device that has a sufficient level, as defined by this policy and CCC standards, of access control and protection from malware and strong encryption capabilities to ensure the protection and privacy of CCC data that may be stored on the mobile device.

**C. RESPONSIBILITIES**

**Policy.** This Interim Policy was issued by the Chancellor of the CCC under authority provided by the Board of Trustees.

**Implementation.** In support of this Policy, system standards and procedures shall be developed, published and maintained.

**Responsibilities.** The Chancellor and each College President is responsible for ensuring that all users are advised of this policy, and for taking appropriate steps to ensure compliance with this policy.

**D. VIOLATIONS OF LAW AND POLICY**

The CCC considers any violation of this policy to be a serious offense and reserves the right to copy and examine any files or information resident on CCC IT resources to ensure compliance. Violations of this policy should be reported to the appropriate CCC Authority.

**Sanctions of Law.** Both federal and state law prohibit theft or abuse of IT resources. Abuses include (but are not limited to) unauthorized entry, use, transfer, tampering with the communications of others, and interference with the work of others and with the operation of IT resources. Any form of harassing, defamatory, offensive, illegal, discriminatory, obscene, or pornographic communication, at any time, to any person is also prohibited by law. Violations of law may result in criminal penalties.

**Disciplinary Actions.** Violators of this Policy may be subject to disciplinary action up to and including dismissal or expulsion pursuant to applicable Board policies and collective bargaining agreements.

**E. NO EXPECTATION OF PRIVACY**

There is no expectation of privacy in the use of CCC IT resources. CCC reserves the right to inspect, monitor, and disclose all IT resources including files, data, programs and electronic communications records without the consent of the holder of such records.

**III. SECURITY REQUIREMENTS FOR PCI DATA**

The security requirements for **all PCI Data** are:

A. No PCI shall reside on any mobile device except as set forth in this policy.

B. PCI that resides on any mobile device used for CCC business shall be:
   1. Limited to the minimum data necessary to perform the business function;
   2. Stored only for the time needed to perform the business function;
   3. Protected from unauthorized access and disclosure in accordance with this and other applicable CCC IT policies, using all reasonably available security precautions, including appropriate access control and
protection from viruses and malware. Users shall not bypass or disable these security mechanisms under any circumstances;
4. Subject to additional security standards that will be developed for protecting PCI data as outlined in Section VI. FUTURE SECURITY REQUIREMENTS.

IV. ADDITIONAL SECURITY REQUIREMENTS FOR PCI IDENTITY DATA

Additional security requirements which apply only to PCI Identity Data are:

A. No PCI Identity Data shall reside on any mobile device used for CCC business until standards for secure mobile devices have been developed and implemented in the CCC System; except that CCC business necessity requires that certain PCI Identity Data may reside on mobile devices until such standards are implemented, provided that all other current CCC IT policies are followed and all reasonably available security precautions are taken, and limited to the following circumstances:
   1. Secure backup storage of College or System data required to ensure data retention or continuity of operations in the event of data loss;
   2. Transmission of data via mobile storage device necessary to comply with Federal or State laws or regulations;
   3. Other circumstances as approved by the CCC Authority, in accordance with the requirements that follow.

B. Users are required to consult with the appropriate CCC Authority before placing any PCI Identity Data on a mobile device used for CCC business.

C. Each College and the System Office must obtain a signed, formal acknowledgement from users of mobile devices which contain PCI Identity Data indicating that they have understood and agreed to abide by this policy.

D. Users must adhere to the following restrictions and requirements before placing PCI Identity Data on any mobile device:
   1. The CCC Authority must assess and determine, in advance:
      a. That the storing of CCC PCI Identity Data on the mobile device is necessary to conduct College or System Office business operations;
      b. That reasonable alternative means to provide the user with access to that CCC PCI Identity Data for the required purpose and timeframe are not readily available;
      c. That the business need necessitating storage of PCI Identity Data on the mobile device outweigh(s) the associated risk(s) of loss or compromise.
   2. The CCC Authority must maintain a written record of the assessment and determination.

E. Any PCI Identity Data placed on a mobile device shall be documented and tracked by the CCC Authority. The information tracked shall include the identification of the individual authorizing storage of the data on the mobile device, the authorized user of the mobile device, the fixed asset inventory tag of the mobile device where applicable, information about the stored data, and the final disposition of that data.

V. GENERAL SECURITY REQUIREMENTS

A. Users in the possession of mobile devices, which contain PCI during transport or use in public places, meeting rooms and other unprotected areas, must take all reasonable and appropriate precautions to protect and control these devices from unauthorized physical access, tampering, loss or theft and shall not leave such devices unattended in such areas.

B. Each College and the System Office must maintain an inventory to identify all mobile devices which contain PCI and the types of data maintained on such devices.

C. Colleges and the System Office, and Users of mobile devices, shall follow the reporting, investigation and other guidelines outlined in the CCC Major Information Security Incident Response Policy, or other applicable policies that may be adopted from time to time, for lost or stolen mobile devices which may contain PCI.

D. In the event that a mobile device which may contain PCI is lost, stolen, or misplaced, and/or the user has determined that unauthorized access has occurred, the user must immediately notify his or her supervisor and the College or System Office IT Security Coordinator of the incident. The Security Coordinators designated under the CCC Major Information Security Incident Response Policy are responsible for initial coordination and evaluation of information security incidents in accordance with that policy.

VI. FUTURE SECURITY REQUIREMENTS

As soon as possible, in conjunction with the CCC Information Security Risk Assessment currently underway, the CCC
System will develop and implement the following security requirements for PCI Data:

A. Standards for secure mobile devices, including:
   1. Standards for encryption tools and methods to be utilized to further enhance the security of data stored on mobile devices.
   2. Standards for configuration of CCC owned mobile devices to allow only the minimum features, functions, and services needed to carry out agency business requirements.
   3. Standards for configuration of all CCC owned mobile computing devices with approved and properly updated software-based security mechanisms as applicable, including anti-virus, anti-spyware, firewalls, and intrusion detection.

B. Inventory standards for documentation and tracking of mobile devices which contain PCI.

C. A formal, documented security awareness and training program to further ensure compliance with this and other information security policies.

VII. NOTICE TO USERS

This Policy may be revised from time to time as necessary to reflect changes in law or other requirements. It is the responsibility of users to ensure that they have reference to the most current version of the CCC Policies as posted on the CCC system website (http://www.commnet.edu/IT/Policy).
2.3 Remote Access Policy

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

Table of Contents

I. Introduction
II. Purpose
III. Common and General Provisions Apply
IV. Scope
V. Support Technology
VI. Application Process
VII. Access Restrictions
VIII. Requirements
IX. Support
X. Enforcement
XI. Revision History

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 Policies 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
Remote Access Policy

- 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
Acceptable Use Policy
(Issued on December 16, 2002 by Chancellor Herzog)

I. INTRODUCTION

II. GENERAL PROVISIONS

A. PURPOSE

B. SCOPE

C. DEFINITIONS

D. RESPONSIBILITIES

E. VIOLATIONS OF LAW AND POLICY

F. NO EXPECTATION OF PRIVACY

III. ACCEPTABLE USE

IV. ACCESS RESTRICTIONS

V. DISCLAIMER

VI. NOTICE TO USERS

I. INTRODUCTION

This Policy governs the acceptable use of Connecticut Community Colleges (CCC) Information Technology (IT) resources. These resources are a valuable asset to be used and managed responsibly to ensure their integrity, security, and availability for appropriate academic and administrative use.

Users of CCC IT resources are responsible for using those resources in accordance with CCC policies and the law. Use of CCC IT resources is a privilege that depends upon appropriate use of those resources. Individuals who violate CCC policy or the law regarding the use of IT resources are subject to loss of access to those resources as well as to CCC disciplinary and/or legal action.

II. GENERAL PROVISIONS

A. PURPOSE

The purpose of this Policy is to:

• Ensure that CCC IT resources are used for purposes appropriate to the CCC mission and goals;
• Prevent disruptions to and misuse of CCC IT resources;
• Ensure that the CCC community is aware that use of CCC IT resources is subject to state and federal laws and the CCC policies; and
• Ensure that IT resources are used in compliance with those laws and the CCC policies.

B. SCOPE

This Policy applies to:

• All IT resources owned or managed by the CCC;
• All IT resources provided by the CCC through contracts and other agreements with the CCC; and
• All users and uses of CCC IT resources.

C. DEFINITIONS

The following terms are used in this Policy. Knowledge of these definitions is important to an understanding of this Policy:

Appropriate CCC Authority: Chancellor, College President or designee.

Compelling Circumstances: Circumstances in which time is of the essence or failure to act might result in property loss or damage, adverse effects on IT resources, loss of evidence of one or more violations of law or of the CCC policies or liability to the CCC or to members of the CCC community.
IT Resources: This includes, but is not limited to, computers, computing staff, hardware, software, networks, computing laboratories, databases, files, information, software licenses, computing-related contracts, network bandwidth, usernames, passwords, documentation, disks, CD-ROMs, DVDs, magnetic tapes, and electronic communication.

D. RESPONSIBILITIES

Policy. This Policy was issued by the Chancellor of the CCC after consultation with appropriate councils, including the Council of Presidents and the Information Technology Policy Committee.

Implementation. In support of this Policy, system standards and procedures shall be developed, published and maintained. And where CCC standards and procedures do not exist, each college is responsible for policy implementation.

Informational Material. Each college shall ensure that users of CCC IT resources are aware of all IT policies, standards and procedures as appropriate.

E. VIOLATIONS OF LAW AND POLICY

The CCC considers any violation of acceptable use to be a serious offense and reserves the right to copy and examine any files or information resident on CCC IT resources to ensure compliance. Violations of this policy should be reported to the appropriate CCC authority.

Sanctions of Law. Both federal and state law prohibit theft or abuse of IT resources. Abuses include (but are not limited to) unauthorized entry, use, transfer, tampering with the communications of others, and interference with the work of others and with the operation of IT resources. Any form of harassing, defamatory, offensive, illegal, discriminatory, obscene, or pornographic communication, at any time, to any person is also prohibited by law. Violations of law may result in criminal penalties.

Disciplinary Actions. Violators of this Policy may be subject to disciplinary action up to and including dismissal or expulsion pursuant to applicable Board policies and collective bargaining agreements.

F. NO EXPECTATION OF PRIVACY

There is no expectation of privacy in the use of CCC IT resources. CCC reserves the right to inspect, monitor, and disclose all IT resources including files, data, programs and electronic communications records without the consent of the holder of such records.

III. ACCEPTABLE USE

In making acceptable use of CCC IT resources you must:

- use resources solely for legitimate and authorized administrative and academic purposes.
- protect your User ID and IT resources from unauthorized use. You are responsible for all activities on your User ID or that originate from IT resources under your control.
- access only information that is your own, that is publicly available, or to which you have been given authorized access.
- use only legal versions of copyrighted software in compliance with vendor license requirements.
- use shared resources appropriately. (e.g. refrain from monopolizing systems, overloading networks with excessive data, degrading services, or wasting computer time, connect time, disk space, printer paper, manuals, or other resources).

In making acceptable use of CCC IT resources you must NOT:

- use CCC IT resources to violate any CCC policy or state or federal law.
- use another person's IT resource, User ID, password, files, or data.
- have unauthorized access or breach any security measure including decoding passwords or accessing control information, or attempt to do any of the above.
- engage in any activity that might be harmful to IT resources or to any information stored thereon, such as creating or propagating viruses, disrupting services, damaging files or making unauthorized modifications to computer data.
- make or use illegal copies of copyrighted materials or software, store such copies on CCC IT resources, or transmit them over CCC networks.
- harass or intimidate others or interfere with the ability of others to conduct CCC business.
- directly or indirectly cause strain on IT resources such as downloading large files, unless prior authorization from the appropriate CCC authority is given.
- use CCC IT resources for personal purposes including but not limited to, monetary gain, commercial or political purposes.
- engage in any other activity that does not comply with the general principles presented above.
IV. ACCESS RESTRICTIONS

Use of CCC IT resources may be wholly or partially restricted or rescinded by CCC without prior notice and without the consent of the user under conditions such as:

- when required by and consistent with law;
- when there is reason to believe that violations of law or the CCC policies have taken or may take place; or
- when there are compelling circumstances.

Restriction of use under such conditions is subject to appropriate procedures or approval of appropriate CCC authority.

V. DISCLAIMER

CCC disclaims any responsibility for and does not warranty information and materials residing on non-CCC systems or available over publicly accessible networks. Such materials do not necessarily reflect the attitudes, opinions or values of CCC, its faculty, staff or students.

VI. NOTICE TO USERS

As laws change from time to time, this Policy may be revised as necessary to reflect such changes. It is the responsibility of users to ensure that they have reference to the most current version of the CCC Acceptable Use Policy.

Portions of this policy are based on language contained in the Acceptable Use Of Information Systems At Virginia Tech dated June 16, 2000. The CCC gratefully acknowledges Virginia Tech for permission to use its policy.
Electronic Communication Policy

(Issued on December 16, 2002 by Chancellor Herzog)

I. INTRODUCTION

II. GENERAL PROVISIONS

A. PURPOSE

B. SCOPE

C. DEFINITIONS

D. RESPONSIBILITIES

E. VIOLATIONS OF LAW AND POLICY

III. ALLOWABLE USERS

IV. ALLOWABLE USES

V. ACCESS RESTRICTIONS

VI. NO EXPECTATION OF PRIVACY

VII. ADMINISTRATION

A. SECURITY

B. RETENTION AND ARCHIVING

VIII. DISCLAIMER

IX. NOTICE TO USERS

I. INTRODUCTION

The Connecticut Community Colleges (CCC) encourages the use of electronic communications to share information and knowledge in support of CCC mission and goals. To this end, CCC provides and supports interactive, electronic communications resources and services.

II. GENERAL PROVISIONS

A. PURPOSE

The purpose of this Policy is to:

- Ensure that CCC electronic communications resources are used for purposes appropriate to the CCC mission and goals;
- Prevent disruptions to and misuse of CCC electronic communications resources and services;
- Ensure that the CCC community is aware that use of CCC electronic communications resources is subject to state and federal laws and the CCC policies; and
- Ensure that electronic communications resources are used in compliance with those laws and the CCC policies.

B. SCOPE

This Policy applies to:

- All electronic communications resources owned or managed by CCC including the content of electronic communications, electronic attachments and transactional information associated with such communications;
- All electronic communications resources provided by CCC through contracts and other agreements with CCC;
- All users and uses of CCC electronic communications resources; and
- All CCC electronic communications records in the possession of CCC employees or other users of
C. DEFINITIONS

The following terms are used in this Policy. Knowledge of these definitions is important to an understanding of this Policy:

**Appropriate CCC Authority:** Chancellor, College President or designee.

**Compelling Circumstances:** Circumstances in which time is of the essence or failure to act might result in property loss or damage, adverse effects on electronic communications resources or services, loss of evidence of one or more violations of law or of CCC policies or liability to CCC or to members of the CCC community.

**Electronic Communication:** Any communication that is broadcast, created, sent, forwarded, replied to, transmitted, stored, held, copied, downloaded, displayed, viewed, read, or printed by one or several electronic communications services, including, e.g., e-mail and telephone.

**Electronic Communications Records:** Electronic transmissions or messages created, sent, forwarded, replied to, transmitted, distributed, broadcast, stored, held, copied, downloaded, displayed, viewed, read, or printed by one or several electronic communications services. This definition of electronic communications records applies equally to the contents of such records, attachments to such records, and transactional information associated with such records.

**Electronic Communications Resources:** Any combination of telecommunication equipment, transmission devices, electronic video and audio equipment, encoding or decoding equipment, computers and computer time, data processing or storage systems, computer systems, servers, networks, input/output and connecting devices, and related computer records, programs, software, and documentation that supports electronic communications services.

**Electronic Communications Services:** Any messaging, collaboration, publishing, broadcast, or distribution system that depends on electronic communications resources to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print electronic records for purposes of communication across electronic communications network systems between or among individuals or groups, that is either explicitly denoted as a system for electronic communications or is implicitly used for such purposes.

D. RESPONSIBILITIES

**Policy.** This Policy was issued by the Chancellor of the CCC after consultation with appropriate councils, including the Council of Presidents and the Information Technology Policy Committee.

**Implementation.** In support of this Policy, system standards and procedures shall be developed, published and maintained. And where CCC standards and procedures do not exist, each college is responsible for policy implementation.

**Informational Material.** Each college shall ensure that users of CCC electronic communications resources are aware of all Information Technology policies, standards and procedures as appropriate.

E. VIOLATIONS OF LAW AND POLICY

The CCC considers any violation of this electronic communications policy and/or law to be a serious offense and reserves the right to copy and examine any files or information resident on CCC electronic communications resources to ensure compliance. Violations of this policy should be reported to the appropriate CCC authority.

**Sanctions of Law.** Both federal and state law prohibit theft or abuse of electronic communications resources. Abuses include (but are not limited to) unauthorized entry, use, transfer, tampering with the communications of others, and interference with the work of others and with the operation of electronic communications resources. Any form of harassing, defamatory, offensive, illegal, discriminatory, obscene, or pornographic communication, at any time, to any person is also prohibited by law. Violations of the law may result in criminal penalties.

**Disciplinary Actions.** Violators of this Policy and/or law may be subject to disciplinary action up to and including dismissal or expulsion pursuant to applicable Board policies and collective bargaining agreements.

III. ALLOWABLE USERS

CCC students, faculty, staff, and others affiliated with CCC (including but not limited to those in program
or contract relationships with CCC) may be authorized to use CCC electronic communications resources and services.

IV. ALLOWABLE USES

CCC encourages the use of electronic communications resources for legitimate and authorized academic and administrative purposes and makes them widely available to the CCC community. To insure the reliable operation of these resources, their use is subject to the following:

- Contents of all electronic communications shall conform to laws and CCC policies regarding protection of intellectual property, copyright, patents and trademarks.
- Using electronic communications resources for any purpose restricted or prohibited by laws, regulations or CCC policies is prohibited.
- Using electronic communications resources for personal purposes, including monetary gain, or for commercial purposes that are not directly related to CCC business or otherwise authorized by appropriate CCC authority is prohibited.
- Usage that directly or indirectly causes strain on the electronic communications resources is prohibited.
- Capturing, opening, intercepting or obtaining access to electronic communications, except as otherwise permitted by the appropriate CCC authority is prohibited.
- Using electronic communications to harass or intimidate others or to interfere with the ability of others to conduct CCC business is prohibited.
- Users of electronic communications resources shall not give the impression that they are representing, giving opinions or otherwise making statements on behalf of CCC unless authorized to do so.
- Directly or by implication, employing a false identity (the name or electronic identification of another), except under the following circumstances, is prohibited:

  A supervisor may direct an employee to use the supervisor’s identity to transact CCC business for which the supervisor is responsible. In such cases, an employee’s use of the supervisor’s electronic identity does not constitute a false identity.

  A user of the CCC electronic communications services may not use a pseudonym (an alternative name or electronic identification for oneself) for privacy or other reasons, unless authorized by an appropriate CCC authority for business reasons.

- Forging e-mail headers or content (i.e., constructing an e-mail so it appears to be from someone else) is prohibited.
- Unauthorized access to electronic communications or breach any security measure is prohibited.
- Interfering with the availability of electronic communications resources is prohibited, including but not limited to the following: (i) sending or forwarding e-mail chain letters or their equivalents in other electronic communications services; (ii) "spamming," i.e., sending electronic junk mail or junk newsgroup postings; (iii) "letter-bombing," i.e., sending an extremely large message or sending multiple messages to one or more recipients to interfere with the recipient’s use of electronic communications resources; or (iv) intentionally engaging in other practices such as "denial of service attacks," i.e., flooding the network with traffic.

V. ACCESS RESTRICTIONS

Use of CCC Electronic Communications resources or services may be wholly or partially restricted or rescinded by CCC without prior notice and without the consent of the user under conditions such as:

- when required by and consistent with law;
- when there is reason to believe that violations of law or the CCC policies have taken or may take place; or
- when there are compelling circumstances.

Restriction of use under such conditions is subject to appropriate procedures or approval of appropriate CCC authority.

VI. NO EXPECTATION OF PRIVACY

No Expectation of Privacy. Electronic communications are not personal or private. Therefore, users should have no expectation of privacy in the use of CCC electronic communications resources. CCC reserves the right to inspect, monitor, and disclose all electronic communications records without the consent of the holder of such records.
Authorized Inspection. During the performance of their duties, electronic communications support personnel periodically need to monitor transmissions or observe certain transactional information to ensure the proper functioning and security of CCC electronic communications resources and services. On these occasions, such personnel may see the contents of electronic communications. Except as provided in this Policy or allowed by law, electronic communications support personnel are not permitted to seek out the contents of electronic communications or of transactional information where not germane to the foregoing purposes or to disclose or otherwise use what they have seen.

VII. ADMINISTRATION

Electronic communications support personnel are required to follow CCC standards and procedures when implementing and managing CCC electronic communications resources or services.

A. SECURITY

CCC attempts to provide secure and reliable electronic communications services. Managers of electronic communications resources are expected to follow sound professional practices in providing for the security of electronic communications records, data, application programs and systems under their jurisdiction based on existing policies, procedures and guidelines. However, users should be aware that electronic communications systems may not be totally secure.

B. RETENTION AND ARCHIVING

Electronic communications records are subject to laws, regulations and CCC records management and archiving policies in administering the retention, disposition, disclosure and storage of all records.

CCC does not maintain central or distributed electronic archives of all electronic communications sent or received. Electronic communications are normally backed up, if at all, only to assure system integrity and reliability, not to provide for future retrieval, although back-ups may at times serve the latter purpose incidentally. Managers of electronic communications services are not required by this Policy to routinely retrieve electronic communications from such back-up facilities for individuals. Employees who have obligations to retain records in accordance with retention schedules promulgated by the State should know that electronic records are subject to the same rules as paper records. See, "Electronic & Voice Mail Management and Retention Guide for State and Municipal Government Agencies" for more information.

VIII. DISCLAIMER

CCC disclaims any responsibility for and does not warranty information and materials residing on non-CCC systems or available over publicly accessible networks. Such materials do not necessarily reflect the attitudes, opinions or values of CCC, its faculty, staff or students.

IX. NOTICE TO USERS

As laws change from time to time, this Policy may be revised as necessary to reflect such changes. It is the responsibility of users to ensure that they have reference to the most current version of the CCC Electronic Communications Policy.

Portions of this policy are based on language contained in the University of California's Electronic Communications Policy dated November 17, 2000. The CCC gratefully acknowledges the University of California for permission to use its policy.
Password Policy

(Issued on February 9, 2004 by Chancellor Herzog)

I. INTRODUCTION

II. GENERAL PROVISIONS

A. PURPOSE

B. SCOPE

C. DEFINITIONS

D. RESPONSIBILITIES

E. VIOLATION OF POLICY

III. PASSWORD CRITERIA

IV. PASSWORD PROTECTION

V. DISCLAIMER

VI. NOTICE TO USERS

I. INTRODUCTION

This Policy governs password creation, usage and protection within the Connecticut Community Colleges (CCC).

User authentication is the means by which an Information Technology (IT) Resource authorizes a user by verifying that the user provided the correct identity. The following factors can be used to authenticate a user. Any of these by themselves or in any combination can be used:

- Something you know – password, Personal Identification Number (PIN)
- Something you have – Smartcard
- Something you are – fingerprint, voice scan etc.

Passwords are the most widely used user authentication factor. They are an important aspect of computer security by providing the front line of protection for user accounts. A weak password may result in the compromise of CCC’s entire network. As such, all authorized users of CCC IT Resources are required to take appropriate steps, as outlined below, to select and secure their passwords.

II. GENERAL PROVISIONS

A. PURPOSE

The purpose of this Policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

B. SCOPE

This Policy applies to:

- All individual users (CCC students, faculty, staff, and others affiliated with CCC, including but not limited to those in program or contract relationship with CCC), who use the IT resources provided by CCC.
- All IT resources owned or managed by Connecticut Community Colleges (CCC).

C. DEFINITIONS

The following terms are used in this Policy. Knowledge of these definitions is important to an understanding of this Policy:

**IT Resources:** This includes, but is not limited to, computers, computing staff, hardware, software, networks, computing laboratories, databases, files, information, software licenses, computing-related contracts, network bandwidth, user IDs, passwords, documentation, disks, CD-ROMs, DVDs, magnetic
tapes, and electronic communication.

**Password:** A string of characters which serves as authentication of an individual's identity, which may be used to grant, or deny, access to private or shared data.

**Password History File:** An encrypted file that contains previous passwords used by the User ID.

**Password Lifetime:** The length of time a password may be used before it must be changed.

**Strong Password:** Strong passwords are constructed of a sequence of upper and lowercase letters, numbers, and special characters, depending on the capabilities of the operating system or application. Typically, the longer the password the stronger it is. Passwords must be unique across all IT resources and not easily tied back to the user such as: User ID, given name, social security number, telephone, employee number, phone or office numbers, address, nicknames, family or pet names, birth date, license plate number, etc.

**User Account:** The user account is made up of the User ID and password.

**User:** The individual requesting a user account in order to perform work in support of a CCC program or a project, by accessing the CCC computer network.

**User ID:** Also referred to as a username. A User ID identifies the user on the system and has an associated password.

**D. RESPONSIBILITIES**

**Policy.** This Policy was issued by the Chancellor of the CCC after consultation with appropriate councils, including the Council of Presidents and the Information Technology Policy Committee.

**Implementation.** In support of this Policy, system standards and procedures shall be developed, published and maintained. And where CCC standards and procedures do not exist, each college is responsible for policy implementation.

**Informational Material.** Each college shall ensure that users of the CCC IT resources are aware of all IT policies, standards and procedures as appropriate.

**E. VIOLATION OF POLICY**

The CCC considers any violation of this Policy to be a serious offense and reserves the right to copy and examine any files or information resident on CCC IT resources to ensure compliance. Violations of this policy should be reported to the appropriate CCC authority.

**Disciplinary Actions.** Violators of this Policy may be subject to disciplinary action up to and including dismissal or expulsion pursuant to applicable Board policies and collective bargaining agreements.

**III PASSWORD CRITERIA**

When composing a password, it must adhere to the following standards:

- Passwords must be a minimum of eight (8) characters.
- Passwords must be complex and difficult to guess. (strong passwords must be used)
- Password must not be reused. (verified against a password history file that is set to the maximum size that the system supports)
- Password must be changed every ninety (90) days. (maximum lifetime)

When using a user account, the following standards must be enforced:

- User accounts must be locked out for a period of time after a maximum of five (5) unsuccessful attempts to gain access to a user account.
- If any part of the logon process (User ID, Password, etc.) is incorrect, the user must not be given specific feedback indicating the source of the problem. Instead, the user must simply be informed that the entire logon process was incorrect.
- Passwords issued by a password administrator must be pre-expired, forcing the user to choose another password before the logon process is completed.

**IV PASSWORD PROTECTION**
All passwords shall be treated as sensitive, confidential CCC information and therefore must be protected as such:

- All vendor-supplied default passwords for software, application and devices must be changed before any IT resource is used on the CCC’s network.
- Passwords must not be reset by a password administrator without the user first providing definitive evidence substantiating his or her identity.
- Passwords issued by a password administrator must be unique and must be sent via a communications channel other than the channel used to log-in to the system.
- Passwords must never be shared or revealed to anyone other than the authorized person, Passwords must not be written down on any medium.
- Passwords must not be stored in readable form in batch files, automatic log-in scripts, software macros, terminal function keys, devices without access control, dial-up communications programs, Internet browsers, cookie files or in other locations where unauthorized individuals might discover or use them.
- Users must refuse all offers to place a cookie on their computer so that they can automatically log on the next time they visit the site.
- Passwords must immediately be changed if the user suspects their user ID or password has been disclosed to an unauthorized person or if a system has been compromised or is under the suspicion of having been compromised.

V. DISCLAIMER

CCC disclaims any responsibility for and does not warranty information and materials residing on non-CCC systems or available over publicly accessible networks. Such materials do not necessarily reflect the attitudes, opinions or values of CCC, its faculty, staff or students.

VI. NOTICE TO USERS

As laws, technology and standards change from time to time, this Policy may be revised as necessary to reflect such changes. It is the responsibility of users to ensure that they have reference to the most current version of CCC Policies.
4.1 Data Management Policy

Table of Contents

I. Introduction
II. Purpose
III. IT Policy Common Provisions Apply
IV. Data Classification
V. Access Restrictions
VI. Data Management Roles
VII. Data Domains
VIII. Data Access Responsibilities
IX. State Record Retention
X. Revision History

I. Introduction

Data Management addresses the activities of capturing, storing, protecting, using, disseminating, and destroying data. Good data management requires a governance context within which to operate; and data management policies, standards and procedures provide guidance for the routine handling and protection of institutional data and media containing that data. Data management practices should improve efficiencies, reduce risks associated with handling data, and ensure institutional compliance with applicable regulations, such as state of CT record retention schedules. Good data management also minimizes misuse, misinterpretation, or unnecessary restrictions of access to institutional data.

Data Classification is the foundation for making decisions about data. Classification determines which security, storage, backup and other controls to implement. For example, public data needs less security than data that if compromised could cause identity theft or financial fraud.

II. Purpose

This policy describes the general strategy and responsibility for managing CCC data at the System Office and at the Colleges.

III. IT Policy Common Provisions Apply

IT Policy Common Provisions, policy 1.1, apply to this specific policy, unless otherwise noted.

IV. Data Classification

Data Classification is the process of grouping data elements together by risk level. The CCC System has identified four Data Classification Levels (DCL) from 0 to 3. Appropriate security controls will be applied to each classification level. Increasingly restrictive data management and security practices are required for each level, with DCL0 requiring limited protection to DCL3 (formerly - Protected Confidential Identity Data) requiring the most protection.

Data Classification Levels

<table>
<thead>
<tr>
<th>Data</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
</table>


<table>
<thead>
<tr>
<th>Classification Level (DCL)</th>
<th>Identity Data with:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>3</strong> DCL3 (Protected Confidential)</td>
<td>• Social Security number</td>
</tr>
<tr>
<td></td>
<td>• Bank account or debit card information</td>
</tr>
<tr>
<td></td>
<td>• Credit card number &amp; cardholder information</td>
</tr>
<tr>
<td></td>
<td>• Student Loan Data</td>
</tr>
</tbody>
</table>

Level 3 is protected confidential data, which comprises identity and financial data that, if improperly disclosed, could be used for identity theft or to cause financial harm to an individual or the CCC.

Security at this level is very high (highest possible).

<table>
<thead>
<tr>
<th>2 DCL2 (Restricted)</th>
<th>Identity Data with:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Birth date</td>
</tr>
<tr>
<td></td>
<td>• Mother's maiden name</td>
</tr>
<tr>
<td></td>
<td>• Academic records (e.g. Grades, Test scores, Courses taken, etc.)</td>
</tr>
<tr>
<td></td>
<td>• Student Records (e.g. Advising records, Disciplinary actions)</td>
</tr>
<tr>
<td></td>
<td>• Employee Records</td>
</tr>
</tbody>
</table>

Level 2 is restricted data that is available for disclosure, but only under strictly controlled circumstances.

Such information must typically be restricted due to proprietary, ethical or privacy considerations.

An example of such restrictions is the FERPA guidelines that govern publication and disclosure of student information.

Security at this level is high.

| 1 DCL1 (Internal) | • Internal memos |
|                  | • Minutes of meetings |
|                  | • Internal project reports |

Level 1 is internal data that has not been approved for general circulation outside the CCC where its disclosure would inconvenience the CCC, but is unlikely to result in financial loss or serious damage to credibility.

Security at this level is controlled but normal.

| 0 DCL0 (Public) | • Advertising |
|                | • Public Directory Information |
|                | • Press Releases |
|                | • Job postings |
|                | • Campus Maps |
|                | • Network Identification (NetID) |

Level 0 is public data that has been explicitly approved for distribution to the public. Disclosure of public data requires no authorization and may be freely disseminated without potential harm to the CCC.

Security at this level is minimal.

**V. Access Restrictions**
Access to DCL3 data is restricted and can only be accessed using a secured CCC system meeting DCL3 security standard. Systems accessing DCL1 and DCL2 data need to be up to date with all required security standards.

VI. Data Management Roles

Data management is reliant on users understanding data management requirements and following appropriate data management procedures. To facilitate management of data the CCC has defined the following three data management roles and responsibilities.

- **Data Steward**
- **Data Manager**
- **Data User**

Data management roles are not exclusive and a single user could occupy all three roles. Responsibility for ensuring data is managed appropriately for a functional area is the responsibility of the Data Steward. The Data Steward can optionally assign daily operational functions to a Data Manager or perform the activities themselves.

**Data Steward**

A Data Steward has planning and policy responsibilities for data within a specific functional area(s) or data domain. Data Stewards have responsibility for understanding, protecting and granting access to CCC data. More specifically he/she:

- Authorizes Data Users for their data domain(s)
- Verifies CCC policies are being adhered to by the practices used in their functional area(s) for managing and protecting data

**Data Manager**

A Data Manager has day-to-day responsibilities for data management within a specific functional area(s) or data domain. Data Managers have responsibility for understanding, protecting and managing access to CCC data. More specifically he/she:

- Consults with data users about the meaning and interpretation of data elements
- Defines data (name, location, aliases, classification, metadata)
- Produces data (capture, generate, normalize, renew, label, document)
- Assures complete, accurate, valid, and timely data collection
- Provides accessible, meaningful, and timely machine-readable institutional data for CCC use
- Mentors and trains staff
- Resolves problems associated with data
- Evaluates security, backup / recovery, and disaster recovery procedures

**Data User**

A data user has operational requirements to access data and use data in performance of his/her assigned duties. More specifically he/she:

- Retrieves, assembles and distributes data to other authorized data users
- Protects data with encryption techniques
- Monitor data usage
- Correct data

VII. Data Domains

- All CCC data will be viewed as belonging to or originating from a specific functional area, also referred to as a data domain.
- Each data domain will have a Data Steward, Data Manager and Data Users.
- The originating data domain is considered the authoritative source for that data.
- The following data domains are identified:
  - Academic Records
  - Admissions
  - Bursars
  - Development (Fundraising)
  - Facilities
  - Finance
  - Financial Aid
  - Human Resources
Data Management Procedures

- System-wide Data Management standards and procedures will be developed for each Data Domain.

VIII. Data Access Responsibilities

Responsibilities for all users with access to CCC data:

- Protect CCC data from unauthorized disclosure, corruption, or loss.
- Use CCC data for legitimate and authorized purposes.
- Access only CCC data for which you have been given authorized access.
- Employees will need to attend a Data Management course as part of a comprehensive Information Security awareness program.

IX. State Record Retention

The CCC complies with State of Connecticut record retention schedules. State Record Retention schedules are located at http://www.cslib.org/publicrecords/retstate.htm

X. Revision History
4.2 Data Storage and Retention Policy

Document Type: Policy (PLCY)
Endorsed By: Information Technology Policy Committee
Promulgated By: Chancellor Herzog

Date: 4/29/2011
Date: 6/16/2011

Table of Contents

I. Introduction
II. Purpose
III. IT Policy Common Provisions Apply
IV. Roles and Responsibilities
V. Specific Provisions
   1. Data on Protected Storage
   2. Data Backups and Off-site Storage
   3. Data Storage
   4. Data Retention
   5. Data Disposal
VI. Revision History

I. Introduction

All institutional data will be stored, backed-up, archived and disposed of in a manner consistent with its sensitivity, requirements and best practices. Data classification is a key component for making consistent and appropriate decisions related to data storage and retention.

Unneeded non-authoritative data (duplicate copies, outdated records, non-business-related files, test data) accumulate in operational locations need to be removed when no longer needed. Purging not only saves IT resources, but also avoids the possibility of compromising sensitive data in these sources that may not be as well protected as the authoritative masters.

II. Purpose

The purpose of this policy is to direct the implementation of standards and procedures for storing, archiving, and disposing of institutional data.

III. IT Policy Common Provisions Apply

IT Policy Common Provisions, policy 1.1, apply to this specific policy, unless otherwise noted.

IV. Roles and Responsibilities

Records Retention Specialist

The functional Records Retention Specialists keep abreast of record retention requirements, and advise functional and technical areas about those requirements. Consult your college’s Records Management Liaison Officer (RMLO) for questions on records retention.

Security Assurance

Security Assurance reviews and evaluates functional areas for compliance with documented policies and procedures.
V. Specific Provisions

1. Data on Protected Storage
   - Data classified as DCL2 (Restricted) and DCL3 (Protected Confidential) will be stored only in approved locations and on approved equipment or storage facilities.
   - CCC employees will refrain from making duplicate copies or shadow files of authoritative data resources.
   - Temporary duplicate copies of electronic data created for legitimate reasons must be protected in a like manner to the authoritative data, and removed in a timely manner.
   - Standards for storing electronic data containing sensitive data will be created and periodically reviewed.
   - Standards for storing hardcopy containing sensitive data will be created and periodically reviewed.
   - Periodic reviews will be performed by Security Assurance to ensure compliance with data management policies, standards and procedures.

2. Data Backups and Off-site Storage
   - All data located on CCC-owned IT Resources will be backed-up on a regular basis consistent with data classification standards applicable to the data being backed-up.
   - Backups of any CCC data whose loss would impact the operation or viability of the CCC will be taken off-site or written off-site to a secure location in a timely manner.
   - Any backup media containing DCL3 data taken off-site or backup data sent off-site will be encrypted.

3. Data Storage
   - The need to retain data in locations will be reviewed on an ongoing basis.
   - Data no longer needed for routine operations, but which must be retained, will be archived in a timely manner.
   - The Information Security Program Office (ISPO) in collaboration with Data stewards will develop criteria for deciding when data can be archived.
   - ISPO in collaboration with Data stewards will develop procedures for archiving of data.

4. Data Retention
   - Data Stewards and Data Managers will be knowledgeable about standards, and procedures regarding retention of data.
   - ISPO in collaboration with Record Retention Specialists will develop procedures to ensure that required data is always accessible, especially as backup media ages, previously supported media is discontinued, supported data formats and standards change, and security controls change.

5. Data Disposal
   - The need to retain operational and archived data will be reviewed on an ongoing basis.
   - Data no longer needed for routine operations and which need not be retained in archive will be destroyed in a timely manner in compliance with State record retention policies.
   - Archived data which need no longer be retained will be destroyed in a timely manner in compliance with State record retention policies.
   - ISPO in collaboration with functional Record Retention Specialists will develop procedures for disposing of data in compliance with State record retention schedules.

VI. Revision History
Major Information Security Incident Response Policy
(issued on November 6, 2006 by Chancellor Herzog)

I. INTRODUCTION

II. GENERAL PROVISIONS
   A. PURPOSE
   B. SCOPE
   C. DEFINITIONS
   D. RESPONSIBILITIES
   E. VIOLATIONS OF LAW AND POLICY
   F. NO EXPECTATION OF PRIVACY

III. INFORMATION SECURITY INCIDENT

IV. INCIDENT RESPONSE PROCESS

V. INITIAL INCIDENT SEVERITY DETERMINATION

VI. COMPUTER INCIDENT RESPONSE TEAM (CI RT)

VII. CI RT RESPONSIBILITIES

VIII. EMERGENCY RESPONSE

IX. DISCLAIMER

X. NOTICE TO USERS

I. INTRODUCTION

This policy governs how major information security incidents will be addressed at the Connecticut Community Colleges (CCC). The following are covered by this policy:

- Determination if the potential exists for exposing Protected Confidential Information (PCI).
- If the potential exists to expose PCI, how the Computer Incident Response Team (CI RT) will handle the incident.

It is crucial that any information security incident is evaluated to determine its severity. The evaluation will determine the course of action to take based on CCC policy and Federal and State law.

A major information security incident is defined as an information security incident that exposes data that is classified as PCI. PCI is data, which exposed to any security risk or otherwise disclosed, would violate Federal or State law or CCC contract or policy. The following are examples of PCI and is not a complete list:

- Non-Public Directory Information
- Social Security Number
- Date of Birth
- Mother's Maiden Name
- Student Loan Data
- Bank Account Numbers
- Credit Card Numbers
- Academic Data

II. GENERAL PROVISIONS

A. PURPOSE

The purpose of this Policy is to:
• Ensure that all information security incidents are evaluated to determine the CCC exposure;
• Ensure that the information security incidents are handled in a timely manner and if the incident has on-going exposure, mitigation steps are prudently taken in a timely manner;
• Prevent disruptions to and misuse of CCC Information Technology (IT) resources; and
• Ensure that IT resources are used in compliance with those laws and the CCC policies.

B. SCOPE

This Policy applies to:

• All IT resources owned or managed by the CCC;
• All IT resources provided by the CCC through contracts and other agreements with the CCC; and
• All users and uses of CCC IT resources.

C. DEFINITIONS

The following terms are used in this Policy. Knowledge of these definitions is important to an understanding of this Policy:

Appropriate CCC Authority: Chancellor, College President or designee.

Compelling Circumstances: Circumstances in which time is of the essence or failure to act might result in property loss or damage, adverse effects on IT resources, loss of evidence of one or more violations of law or of the CCC policies or liability to the CCC or to members of the CCC community.

CCC System Security Manager (SSM): The System Security Manager is responsible for overall coordination of information security incidents with the CCC system. Contact information for the SSM can be located at address on security page when added.

Computer Incident Response Team (CIRT): A team of senior managers from the System Office and the colleges that is assembled to evaluate and manage potential major information security incidents at the colleges and System Office.

Expeditiously: The time to address the incident should be as soon as possible depending on the potential exposure of the incident. For a major information security incident, time is critical the initial determination if PCI data potentially could be exposed should occur with hours.

IT Resources: This includes, but is not limited to, computers, computing staff, hardware, software, networks, computing laboratories, databases, files, information, software licenses, computing-related contracts, network bandwidth, usernames, passwords, documentation, disks, CD-ROMs, DVDs, magnetic tapes, and electronic communication.

IT Security Coordinator (SC): The Security Coordinator is responsible for Initial coordination and evaluation of information security incidents at a College or System Office. Contact Information for the SC can be located at http://www.internal.commnet.edu/policy/security-coordinators.pdf Each College will have at a minimum one SC and preferably a backup.

Major Security Incident? Any information security incident that could potentially expose PCI. The standard is the incident has potential to expose information and not that information has actually been exposed.

Non-CCC Owned Device? Is any device that the CCC did not purchase or explicitly accept management of the device. An example would be computers or laptops owned by faculty, staff and students.

Non-Public Directory Information: Is directory information that would not generally be available to the public such as an e-mail address. For more information on what is public directory information, please see the Connecticut Community Colleges Policy Manual, Section 5.7 Item 5.

Protected Confidential Information (PCI): Is data, which exposed to any security risk or otherwise disclosed, would violate Federal or State law or CCC contract or policy.

D. RESPONSIBILITIES

Policy. This Policy was issued by the Chancellor of the CCC after consultation with appropriate councils, including the Council of Presidents and the Information Technology Policy Committee.

Implementation. In support of this Policy, system standards and procedures shall be developed, published and maintained. And where CCC standards and procedures do not exist, each college is responsible for policy implementation.
Informational Material. Each college shall ensure that users of CCC IT resources are aware of all IT policies, standards and procedures as appropriate.

E. VIOLATIONS OF LAW AND POLICY

The CCC considers any violation of this policy to be a serious offense and reserves the right to copy and examine any files or information resident on CCC IT resources to ensure compliance. Violations of this policy should be reported to the appropriate CCC authority.

Sanctions of Law. Both federal and state law prohibit theft or abuse of IT resources. Abuses include (but are not limited to) unauthorized entry, use, transfer, tampering with the communications of others, and interference with the work of others and with the operation of IT resources. Any form of harassing, defamatory, offensive, illegal, discriminatory, obscene, or pornographic communication, at any time, to any person is also prohibited by law. Violations of law may result in criminal penalties.

Disciplinary Actions. Violators of this Policy may be subject to disciplinary action up to and including dismissal or expulsion pursuant to applicable Board policies and collective bargaining agreements.

F. NO EXPECTATION OF PRIVACY

There is no expectation of privacy in the use of CCC IT resources. CCC reserves the right to inspect, monitor, and disclose all IT resources including files, data, programs and electronic communications records without the consent of the holder of such records.

III. INFORMATION SECURITY INCIDENT

An information security incident is defined as any incident that potentially exposes PCI to anyone who has not been authorized to access the data or anyone who abuses the access they have been granted. An incident may occur from an external or internal source. The following are examples of security breaches and is not a complete list:

- A system is breached by an external hacker
- A virus, worm, rootkit, keylogger etc. compromises a system
- A laptop is lost or stolen
- A user gains access to unauthorized data through technical or social engineering
- A backup tape has been lost or stolen
- A thumb drive, CD, etc. is lost or stolen
- A user uses his/her access in a non-authorized manner
- Data is sent by e-mail to non-authorized users
- A hard copy report is lost or stolen that contains PCI data

As the examples illustrate above a security incident may occur from an accidental occurrence or a malicious activity.

IV. INCIDENT RESPONSE PROCESS
V. INITIAL INCIDENT SEVERITY DETERMINATION

Any information security incident needs to be investigated to determine if any PCI may have been exposed. Any incident that may potentially expose PCI needs to follow the Major Information Security Incident Handling standards and procedures. The following process is used to determine if the incident is a major incident:

- Any CCC Staff, Faculty or Student suspecting that an information security incident has occurred needs to notify expeditiously their campus or system office IT Security Coordinator or designee.
- The IT Security Coordinator will expeditiously perform an initial review to determine if the incident may have compromised PCI. If the review determines conclusively that no PCI was compromised, the college will follow their normal procedures. If the review determines that PCI was potentially compromised then the IT Security Coordinator will contact the CCC System Security Manager or designee.
- The CCC System Security Manager will review the incident with the IT Security Coordinator. If the CCC System Security Manager determines that PCI may have been compromised, then he/she will expeditiously convene the Computer Incident Response Team (CIRT).
- Next Steps? CIRT analysis see section VII

VI. COMPUTER INCIDENT RESPONSE TEAM (CIRT)

The CIRT evaluates and manages information security incidents that have potentially exposed PCI. The team membership is the following:

Core Team Membership
• Chief Information Officer
• Director of Labor Relations/Counsel
• Assistant Chancellor
• Director of Technical Services
• Security Manager
• Chief Financial and Administrative Officer
• Chief Academic Officer

College Membership per Incident as Appropriate:
• Information Security Coordinator
• College Department Head of department involved in the incident

Additional Membership as Appropriate:
• Based on the incident, the core team may add other College, System Office or external resources to the team.

VII. CIRT RESPONSIBILITIES

The CIRT will be responsible for the following in handling a potential major security incident:

• Analysis
  • Incident Analysis
  • Incident Documentation
  • Incident Prioritization
  • Incident Notification

• Containment and Eradication and Recovery
  • Choosing a Containment Strategy
  • Evidence Gathering and Handling
  • Identifying the Attacker
  • Eradication and Recovery

• Post-Incident Analysis
  • Lessons Learned
  • Using Collected Incident Data
  • Evidence Retention

Further details on how potential major incidents will be responded to can be found in the Major Information Security Incident Response Standards and Procedures Documents.

VIII. EMERGENCY RESPONSE

In the event that a security incident has compelling circumstances the Chief Information Officer or his/her designee is authorized to take the necessary technical steps to mitigate the incident to stop further exposure.

IX. DISCLAIMER

CCC disclaims any responsibility for and does not warranty information and materials residing on non-CCC systems or available over publicly accessible networks. Such materials do not necessarily reflect the attitudes, opinions or values of CCC, its faculty, staff or students.

X. NOTICE TO USERS

As laws change from time to time, this Policy may be revised as necessary to reflect such changes. It is the responsibility of users to ensure that they have reference to the most current version of the CCC Acceptable Use Policy.
5.2 Vulnerability Management Policy

Table of Contents

I. Introduction
II. Purpose
III. IT Policy Common Provisions Apply
IV. Roles and Responsibilities
V. Specific Provisions
   1. Patch and Update Management
   2. Email Threat Management
   3. Internet Browser Threat Management
   4. Vulnerability Awareness Training
   5. Asset Classification and Inventory
   6. End-user Device and Server Intrusion Detection and Prevention
   7. Sensitive Data Loss Prevention
   8. End-user Device and Server Vulnerability Scanning and Threat Mitigation
   9. Network Intrusion Detection and Prevention
  10. Log Management
  11. File Integrity Management
  12. Network Vulnerability Scanning and Threat Mitigation
  13. Employee-related Vulnerabilities

VI. Revision History

I. Introduction

IT resources can be exploited in order to steal sensitive data, damage systems, or deny access to those resources. Vendors, recognizing vulnerabilities in their products, create software patches and other strategies which are distributed to their customers. Diligent customers implement those patches and strategies to prevent successful attacks from hackers. Unfortunately, as technologies evolve, new vulnerabilities are discovered, which must in turn be mitigated. Some vulnerability can be managed only with add-on security software and other specialized tools.

Non-technical vulnerabilities may also exist in the manner in which employees control access to sensitive data and computer systems.

Risks to the IT infrastructure must be actively managed. The tasks involved, which can be time-consuming and mundane, are never-the-less essential to the overall health of the IT enterprise and the safety of its data. All employees must take responsibility for reducing technical and non-technical risks.

II. Purpose

This Information Technology Policy directs the establishment of vulnerability management practices in order to
proactively prevent the exploitation of vulnerabilities and potential loss of CCC sensitive data. The CCC System will create and document systematic and accountable practices to maintain control programs and applications, to evaluate installed and new devices and systems for vulnerabilities, and to mitigate other technical and non-technical vulnerabilities. The goals of this effort are to implement stronger protection for CCC IT resources, ensure compliance with best practices, and reduce the impact of threats to the CCC and its constituents.

III. IT Policy Common Provisions Apply

IT Policy Common Provisions, policy 1.1, apply to this specific policy, unless otherwise noted.

IV. Roles and Responsibilities

All CCC Employees

All CCC employees will control access to sensitive information in both electronic system and hardcopy format.

Information Technology Managers

Information Technology staff at the Colleges and at the System Office will oversee, support, and assist with the maintenance and security of server and workstation operating systems, network device control programs, applications, and data within their assigned areas.

System Data Center (SDC)

The SDC staff and management will track, acquire, vet and distribute software patches and updates for all approved operating systems, for network devices, and for those applications, which are system-wide implementations across the CCC System. In addition, the SDC will provide guidance and support for reducing risk and mitigating vulnerabilities.

College IT Staff

Responsible college IT staff will patch and update servers, end-user devices and network devices under college management, using tools and code provided by the SDC or local tools for non system-wide implementations. In cases where the SDC does not provide authoritative support, College IT staff will track, acquire, vet and install patches and updates in a timely manner. College IT staff will implement risk reduction strategies and will mitigate detected vulnerabilities.

V. Specific Provisions

1. Patch and Update Management

The SDC and College IT staff will install only approved software. All installed software will be maintained in a timely manner at supported levels, with appropriate patches and updates, in order to address vulnerabilities and to reduce or prevent any negative impact on CCC operations.

2. Email Threat Management

The CCC e-mail system will be actively managed for spam, malware and inappropriate content. Suspicious email will be quarantined to prevent disruption to the email system or network.

3. Internet Browser Threat Management

Internet access will have controls implemented to inform users about potentially malicious sites and actively stop access to known malicious sites.

4. Vulnerability Awareness Training

Vulnerability awareness training is required for all staff, faculty and students as part of a comprehensive education and awareness program.

5. Asset Classification and Inventory

The SDC and College IT Staff will maintain a master inventory of software and IT equipment, along with an asset classification system. Vulnerability management strategies appropriate to each asset class will be used,
6. End-user Device and Server Intrusion Detection and Prevention

All end-user devices and servers that access or store sensitive data will have technology deployed to prevent, detect, repair, and manage malicious software and unauthorized intrusions.

7. Sensitive Data Loss Prevention

All IT resources that are used to access and store sensitive data will have technology deployed to verify the data is accessed, stored, copied, printed, transmitted, discarded and otherwise handled in a secure and authorized manner.

8. End-user Device and Server Vulnerability Scanning and Threat Mitigation

IT Resources used to access, transmit and store sensitive data will be periodically scanned to verify they are free of vulnerabilities and up to date with all software versions and patches.

9. Network Intrusion Detection and Prevention

The CCC network is actively managed and technology is deployed to detect and prevent unauthorized intrusion or access to sensitive data, and the transmission of malicious software or inappropriate content.

10. Log Management

Logs created by servers, firewalls, network devices, control programs and applications will be analyzed, secured and maintained for a period of time to assist with troubleshooting and forensic assessments.

11. File Integrity Management

Files containing sensitive data will be managed to ensure only appropriate access and authorized changes are allowed. When necessary, all access to files containing sensitive data will be logged and reviewed.

12. Network Vulnerability Scanning and Threat Mitigation

All changes to the network will be approved, recorded, monitored, and verified. The network will be actively managed to detect network vulnerabilities and unauthorized changes or extensions to the network.

13. Employee-related Vulnerabilities

Employees will adhere to approved standards and procedures for accessing, using and managing sensitive data and other IT resources.

VI. Revision History