Security for Mobile Computing and Storage Device Policy

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

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

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.