Major Information Security Incident Response Policy

(Issued on November 6, 2006 by Chancellor Herzog)

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 (CIRT) 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.

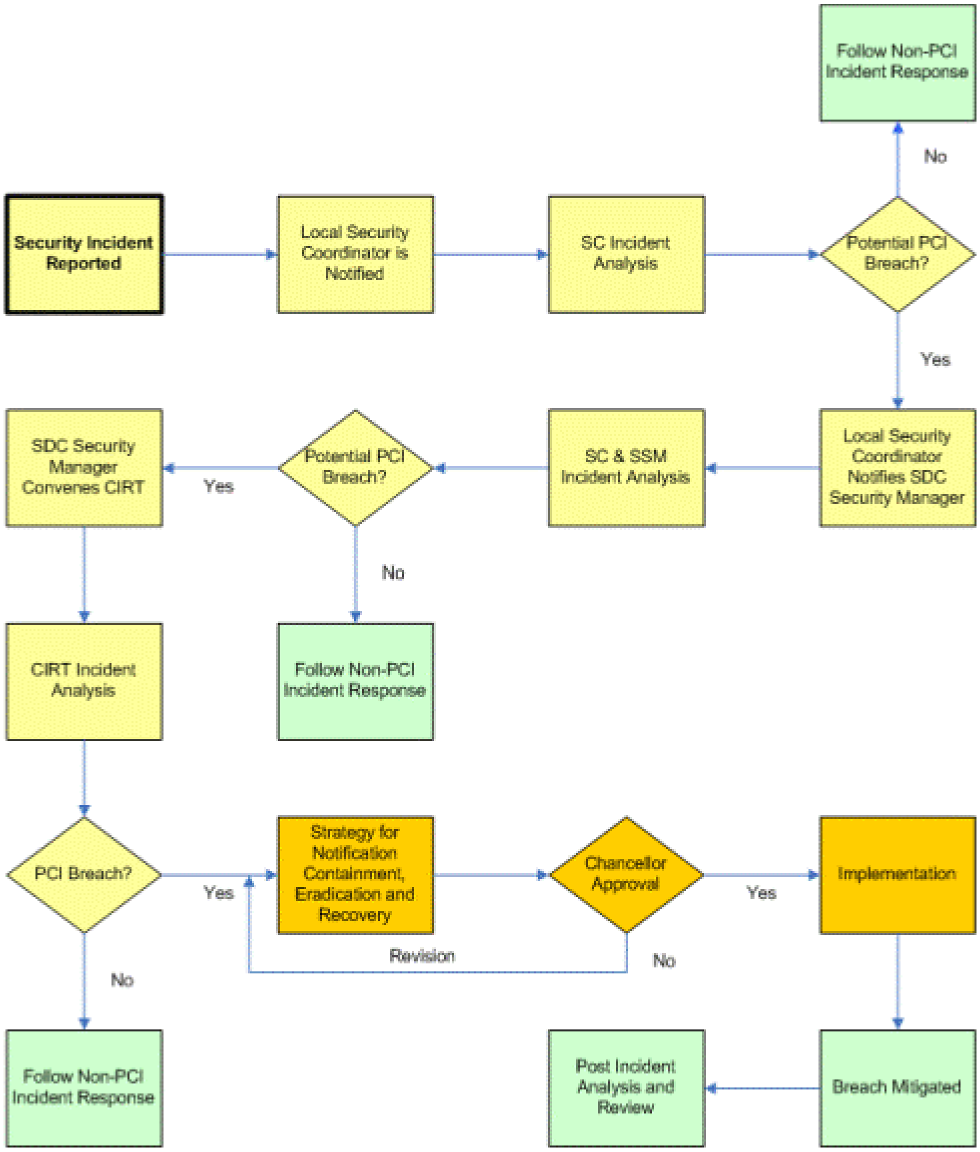
III. INFORMATION SECURITY INCIDENT

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


Follow Non-PCI Incident Response
No
Security Incident Reported
Local Security Coordinator is Notified
SC Incident Analysis
Potential PCI Breach?
Yes
SDC Security Manager Convenes CIRT
Yes
Potential PCI Breach?
SC & SSM Incident Analysis
Local Security Coordinator Notifies SDC Security Manager
No
CIRT Incident Analysis
Follow Non-PCI Incident Response
PCI Breach?
Yes
Strategy for Notification Containment, Eradication and Recovery
Chancellor Approval
Yes
Implementation
Revision
No
No
Follow Non-PCI Incident Response
Post Incident Analysis and Review
Breach Mitigated

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.