Vulnerability Management Policy

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

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