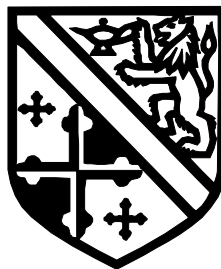




# **Information Technology Security Plan**

**February 2009**



1. **General.** Information security is the protection of technology resources and data from a wide range of threats to ensure business continuity and minimize business risks. The vice president of information technology and assigned directors manage activities to ensure information security is achieved by implementing policies, procedures, controls and organizational structures. Together, these activities are directed to support the constantly changing technology environment of the college by providing comprehensive technology services to advance instruction, college services and business processes.

2. **Objectives.** The objectives of this plan are to identify, assess and mitigate risks to HCC's information assets. In order to achieve these objectives, the following actions are required:

- a. Issuance of college-wide and internal policies and procedures to protect technology resources and information.
- b. Development of business continuity and disaster recovery processes.
- c. Formation of a technology change management committee to address ongoing security topics.
- d. Reporting and recording of security incidents and responses.
- e. Completion of an annual risk assessment.

3. **Information Security Program Coordinator.** The vice president of information technology appoints a primary and alternate information security program coordinator. The coordinators are responsible for assessing the security risks and external threats, recommending actions to minimize those risks, and conducting program reviews to assess the adequacy of internal controls, structures, and business processes to protect college information and technology resources.

4. **Security Policies and Procedures.** The vice president of information technology directs the issuance of college policies and procedures to address:

- a. Business requirements and governing laws and regulations
- b. The protection of college information resources to safeguard against damage, loss and unauthorized disclosure.
- c. The proper use of information technology among employees.
- d. Internal operating procedures within the information technology area.

The vice president of information technology directs the annual review of information security policies and procedures to ensure currency. Reviews will include assessing opportunities for improvement in response to changes to the college's environment, new threats and risks, business processes, legal requirements and technical environment. Refer to college policies *Proper Use of Information Technology* and *Protection of College Information Resources*.

## 5. Asset Management:

a. Inventory. Information technology directors maintain an electronic inventory of key computer assets, including desktops, printers, servers, routers and switches. An inventory is completed annually.

b. Disposal. All computer equipment containing storage media will be checked to ensure that any regulated and confidential information and licensed software has been removed or securely overwritten prior to disposal.

**6. Facility Access and Security.** Most work centers within the information management area maintain confidential or sensitive information and critical technology assets. Highly sensitive areas include the network operations center and administrative information systems (AIS) offices. The following safeguards are required:

a. Access to work centers must be protected by secure key card entry systems. The vice president of information technology and directors maintain a master key to all assigned work centers.

b. Access to the network operations center (NOC) is restricted to employees who maintain or support information technology systems on a reoccurring basis.

c. The vice president of information technology approves requests for unescorted access to the NOC and issuance of key access cards. Attachment 1 identifies those positions that require access to the NOC based upon job requirements.

## 7. Information Security Incident Management:

a. Definition. An information security incident includes, but is not limited to, one of the following events:

- attempts (either failed or successful) to gain unauthorized access to a system or its data
- unwanted disruption or denial of service
- the unauthorized use of a system for the processing or storage of data
- changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent
- Unauthorized disclosure of regulated or confidential information

b. Notification. Information technology employees must immediately notify their supervisor or director upon discovery of a possible or actual information security incident. Employees will immediately notify the vice president of information technology if their supervisor or director is unavailable.

c. Reporting. Responsible information technology staff will initiate timely corrective action, document the incident and record lessons learned to prevent similar incidents from occurring in the future. The vice president of information technology retains documentation related to all information security incidents.

**8. Business Continuity Management.** The objective of business continuity management is to counteract interruptions to business activities, protect critical business processes from the effects of major failures of information systems, and ensure timely resumption after interruption. As such, information technology staff must ensure that redundant systems are in place to support the Colleague enterprise system and the college primary websites (college main website and intranet, Laurel College Center, and Belmont Conference Center).

**9. Disaster Recovery.** The overall objectives of the IT Disaster Recovery Plan are to protect the college information resources, safeguard records, and outline procedures for the recovery of key business processes in the event of a major disaster or other incident that impacts the operations of IT services. The central theme of the plan is to minimize the effect a disaster will have upon on-going operations. This plan responds to both external disasters and operational failures. The Disaster Recovery Team includes employees identified below. These staff members will retain a copy of the disaster recovery plan at their home residence. A copy of the plan is also available on *O:\Disaster Recovery*.

- Vice President for Information Technology
- All directors (AIS, ITS, SCS, and UNS)
- Network administrators
- Colleague Systems and Database Administrator

**10. Employee training and education** While directors and supervisors are ultimately responsible for ensuring compliance with information security practices, information technology staff will work in cooperation with the Human Resources department to develop and maintain training and education programs for all employees who have access to college technology resources and information. Information technology staff members are required to complete three hours of professional development training related to information security. Supervisors will document this training requirement as part of employees' annual plans.

**11. Change Management.** Operational procedures and controls, such as configuration and application management, are critical pieces to manage information security. Therefore, the technology change management committee, chaired by the director of user network services, will consider, evaluate and report on information security issues related to planned changes of the college's computing infrastructure. The committee issues minutes of change management meetings to record planned improvement and outcomes of technology enhancements.

**12. Annual Risk Assessment.** Information technology area directors are responsible for conducting and documenting an annual risk assessment to identify threats that could jeopardize college assets (e.g., a system, data, or process). Upon identification of threats,

information technology staff will initiate actions to reduce the risk or mitigate the consequences of such treats.

Attachment 1 – List of Technology Staff with Access to Network Operations Center

Vice President of Information Technology	
Administrative Information Systems	Director, Administrative Information Systems Senior Programmer Analyst (3) Programmer Analyst (1) Systems Support Technician
Information Technology Services	Director, Information Technology Services Web Services Manager Web Engineer Website Development Specialist Technology Services Manager
Student Computer Support	Director Student Computer Support Server Administrator Coordinator of SCS SCS Tech Support Analyst SCS Network Support Analyst Senior SCS Network Support Analyst Database System Engineer Lead SCS Computer & Network Technician
User Network Services	Director, User Network Services Senior Network Engineer Network Engineer Network Engineer II Senior Computer Specialist II Senior Computer Network Support Tech Computer Network Support Tech Network Administration Coordinator Network Administrator Server Administrator Systems Engineer