Information Security Program

Purpose

The purpose of this document is to recapitulate the steps taken by the college to:

• ensure the security and confidentiality of customer information;

• protect against any anticipated threats to the security or integrity of such information; and

• guard against the unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

Coordination of Information Security Program

The responsibility for maintaining information security within the college rests with the Director of Information Services. In concert with the director are the Network Administrator and the Systems Analyst/Programmer who have responsibility within their own specific areas.

• *Network Administrator* – This individual oversees and administers the campus data network and the access to off-campus computing resources. In addition he manages and supports higher-level Internet resources (DNS and IP assignments, e-mail, FTP and WWW servers.)
• *Systems Analyst/Programmer* – This individual administers the implementation and ongoing maintenance and support of the SCT PowerCAMPUS software that is the administrative database for all electronic records on campus.

Risk Identification

A key segment of information security is the identification of reasonable, foreseeable internal and external risks to the security, confidentiality and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information and to assess the sufficiency of any safeguards in place to control these risks.

• Internal Risks
1. Packet Sniffers
2. Theft of passwords
3. Viruses
4. Unauthorized access to restricted areas

• External Risks
1. Hackers
2. Viruses
3. Unauthorized access

Safeguard Implementation

Certain tools have been put in place or are in the process of being installed to assess and control the identified risks including but not limited to:

• utilization of Server 2000 and Server 2003 software and their built-in security features;
• the use of passwords and requiring them to be changed periodically;
• consolidating servers in the Computer Information Center for improved security and administration;
• limited access to the Computer Information Center;
• restricting access to those administrative software modules which are germane to the needs of the individual;
• users being routinely encouraged to use discretion about sharing data and access to that data;
• periodic and automatic updating of virus definitions on individual computers;

• the use of SSL (Secure Socket Layer) encryption;
• the use of a firewall to restrict network access from external sources;
• the continual monitoring of that firewall;
• the use of a traffic shaping device (Packeteer) to monitor and control network traffic flow;
• continually monitoring the availability of servers, Windows, CERT (Computer Emergency Response Team) and Linux security updates and patches and the application of those updates to insure the most up-to-date operating software available;
• the daily backup of servers with storage of those backups in other locations on campus; and
• a separate Disaster Recovery Plan to assist in the event of a major disaster which would render the college computer hardware and/or software inoperable.