ADM 405
Security Policy #5

Network Security

Purpose of Policy

The purpose of the policy is to describe the physical safeguards applicable for each server, desktop computer system and wireless computer system used to access, transmit, receive and store PII and sensitive college data to ensure that appropriate security is maintained and that access is restricted to authorized employees.

Network Security

The College will take reasonable and appropriate steps to prevent unauthorized access to workstations, servers and portable devices including laptops, CD-ROMs, DVDs, USB Drives, etc. that store or access PII and sensitive college data.

1) Workstations and laptops that are in common areas that store or access PII and/or sensitive college data should be physically placed with the monitor so that it prohibits unauthorized people from viewing confidential information such as logins, passwords, PII and/or sensitive college data.

2) Workstations and laptops that are in common areas that store or access PII and sensitive college data should utilize privacy screens to prevent unauthorized access to the data.

3) In addition, encryption should be used when sending any PII and/or sensitive college data across public networks and wireless networks. Public networks include email and Internet access.

4) Portable devices and media should be concealed from view when offsite to prevent theft.

5) All network servers, application servers, routers, database systems, device management system hardware, and other servers should be located in a room or an area that can be physically secured by lock and key or any other appropriate security mechanism to limit access to only authorized personnel.

6) All workstations, servers and portable devices will run end-point and protection software. The software must be current and up to date. Employees must use and keep active current versions of approved anti-virus / anti-malware software scanning tools to detect and remove malicious software from workstations and files. Employees must not disable these

tools unless specifically directed by computer support personnel to do so in order to resolve a particular problem.

7) A network firewall should be in place to protect PII and/or sensitive college data. The firewall protection should be up to date. Firewalls should be monitored and alerts should be triggered in the event of unauthorized intrusion or suspected intrusion.

8) Log files from network equipment should be stored and retained. Log files from network equipment include; firewalls, network servers, desktops, laptops and other devices. The required length of retention of log files may vary depending on federal, state or industry regulations.

9) All workstations, servers and portable devices, where feasible, must implement a security patch and update procedure to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected.

10) Periodic network vulnerability scans should be performed on all internal as well as external (Internet facing servers, websites, etc.) systems, as possibly required by GLBA. Results of the vulnerability scans should be analyzed and known vulnerabilities should be remediated and/or patched.

11) Reasonable and appropriate steps will be taken to prevent unauthorized access to workstations, servers and portable devices from misuse and physical damage, vandalism, power surges, overheating monitoring.

    a. All facilities that store systems that contain PII and/or sensitive college data, should have appropriate smoke and/or fire detection devices, sprinklers or other approved fire suppression systems, and working fire extinguishers in easily accessible locations throughout the facility.

    b. All servers that contain PII and/or sensitive college data, should be connected to an Uninterrupted Power Supply (UPS) to prevent server crashes during power outages or spikes. Servers should be configured to shut down in a controlled manner if the power outage is for an extended period of time.

    c. All systems should be connected to surge protectors, where feasible, to protect against power spikes and surges.

12) A user identification and password authentication mechanism shall be implemented to control user access to the system. **(See Security Policy #6 - Access Control).**

13) Employees who suspect any inappropriate or unauthorized use of workstations should immediately report such incident or misuse to the Security Officer.