

## **Network and Security Monitoring Policy**

### **I. Purpose**

The purpose of this policy is to maintain the integrity and security of the college's network infrastructure and information assets, and to collect information to be used in network design, engineering and troubleshooting.

### **II. Scope**

This policy applies to all users of Augsburg College information resources over networks that cause traffic to traverse the campus network infrastructure. The policy extends from the point of network access to the end-user machine.

Augsburg College considers all electronic information transported over the college network to be private and confidential. Network and system administrators are expected to treat the contents of electronic packets as private and confidential. Any inspection of electronic files, and any action performed following such inspection, will be governed by all applicable federal and state statutes and by college policies.

Faculty, staff and students should be aware that logs are generated by the various Internet services used on campus, including email and web access and network flows. While it is not the policy of Augsburg College to actively monitor Internet activity on the network, it is sometimes necessary to examine such activity when a problem has occurred or when optimizing traffic on the college's Internet links.

### **III. Definitions**

- A. Information Resources – Any information in electronic, audio-visual or physical form, or any hardware or software that makes possible the storage and use of information
- B. Institutional Data – Data that is generated, acquired, or maintained by Augsburg College employees in performance of official administrative job duties.
- C. Packet – Electronic unit of data that is routed between an origin and a destination on a network.
- D. Packet Data – The part of the packet containing user data and other data or information used by applications.
- E. Packet Header - The first part of the packet, which contains protocol, source address, destination address, and other controlling information.
- F. Information Security Officer: Individual responsible to executive management for administering the information security functions within the College. The ISO is the agency's internal and external point of contact for all information security matters. The ISO shall be the Chief Information Officer or their designated representative.

## **IV. Policy**

### **A. Ownership and Responsibilities**

The Department of Information Technology is responsible for the safety and security of data on its network and the equipment used to run the network infrastructure.

This policy applies to all individuals that are responsible for the installation of new information resources, the operations of existing Information Technology resources, and individuals charged with Information Technology resource security.

### **B. Required Monitoring Activities**

- Automated tools will provide real time notification of detected wrongdoing and vulnerability exploitation. Where possible a security baseline will be developed and the tools will report exceptions. These tools will be deployed to monitor:

Internet traffic

Electronic mail traffic

LAN traffic, protocols, and device inventory

Operating system security parameters

- The following files will be checked for signs of wrongdoing and vulnerability exploitation at a frequency determined by risk:

Automated intrusion detection system logs

Firewall logs

User account logs

Network scanning logs

System error logs

Application logs

Data backup and recovery logs

Help desk trouble tickets

Telephone activity – Call Detail Reports

Network printer and fax logs

- The following checks will be performed at least annually by assigned individuals:

Unauthorized network devices

Unauthorized personal web servers

Unsecured sharing of devices

Operating System and Software Licenses

- Any security issues discovered will be reported to the ISO for follow-up investigation.

### **C. Authorized Personnel**

The Information Security Officer and their designated representatives are the only individuals authorized to routinely monitor network traffic, system security logs, or other computer and network security related information.

### **D. Retention**

Electronic logs that are created as a result of the monitoring of network traffic need only be retained until the administrative need for them ends, at which time they should be destroyed. Electronic logs will be retained when required as part of a campus investigation or when required by as part of law enforcement or legal proceedings.

### **IV. Enforcement**

Anyone found to have violated this policy may be subject to appropriate disciplinary action.