Approved: August 22, 2005 Revised: January 15, 2008

Computer Network and System Records, Logs and Structures Policy

Purpose

Due to the mission-critical nature of the data networks and systems of the University, it is necessary to protect these systems from attack by properly securing the internal security structures and records. A number of inferences about the topology and capacity of the internal systems could be made by the theft or inadvertent disclosure of logs, diagrams, maps, status, and capacity of the various components of the infrastructure that could be used to compromise the overall security and integrity of critical University systems. Such inferences could also be made through carefully crafted Freedom of Information Act type requests. This policy ensures that internal security structures and records are kept secure and confidential.

Policy Statement

Massachusetts General Law (i.e., MGL), Chapter 66, Public Records Law, states that every person has a right to inspect, copy or have copies of records of public information. Public records include all documentary data, regardless of physical form or characteristics, made or received by an officer or employee of any municipality or agency of the Commonwealth, unless falling within a statutory exemption. MGL Chapter 4, Section 7 (46n) exempts the following records from the Public Records Law:

> n) records, including, but not limited to, blueprints, plans, policies, procedures and schematic drawings, which relate to internal layout and structural elements, security measures, emergency preparedness, threat or vulnerability assessments, or any other records relating to the security or safety of persons or buildings, structures, facilities, utilities, transportation or other infrastructure located within the commonwealth, the disclosure of which, in the reasonable judgment of the record custodian, subject to review by the supervisor of public records under subsection (b) of section 10 of chapter 66, is likely to jeopardize public safety.

All requests to "inspect, copy or have copies" of records noted below should be referred to University legal counsel for review and direction.

The University of Massachusetts classifies the following information/records as "Operational Only" (i.e., data whose loss, corruption or unauthorized disclosure would not necessarily result in any business, financial or legal loss BUT which the University had determined is critical to its business and requires a higher degree of handling than unclassified data) under University Data and Computing Standards because its improper disclosure could pose a significant security risk, or the data could be used to circumvent security or make inferences about the capabilities and capacities of the network. This information/records relate to the "security or safety of persons or buildings, structures, facilities, utilities, transportation or other infrastructure located within the commonwealth" (e.g., the University) and are therefore, exempt from the Public Records Law by virtue of MGL Chapter 4, Section 7 (46n):

1. **IT Infrastructure Information -** All maps, diagrams, and location information for information technology (i.e., IT) assets including but not limited to: data and telephone network equipment locations, types, revisions, operating systems, power requirements, data capacities and speeds; cable, fiber, and antenna locations, types, and capacities, and coverage; and location of wiring closets or cabinets, servers and data centers. This includes any access information (e.g., security methods or codes, passwords, procedures, or key numbers) for these or similar infrastructure.

2. **Network Structure And Topology Information -** IP address allocation, assignment, and utilization; subnet information and layout; virtual local area network (e.g., VLAN) allocation and utilization; switch, router, server, or other network appliance interface names; and network addresses.

3. **Network And System Configuration Information -** Authorization and authentication system types, methods, and configurations; Router and switch configurations and access-lists (ACL); firewall types; configurations and rules; Intrusion Detection System (i.e., IDS) types configuration and rules; network traffic monitoring and management procedures and methods (e.g. quality of service/guaranteed throughput level - QoS and "packet shaper" information); and network management system capacities, type and configuration, and Voice over IP (i.e., VoIP) activity logs. This applies to any other network "service" such as but not limited to: mail, news, Domain Name Servers (i.e., DNS), Dynamic Host Configuration Protocol (i.e., DHCP), Lightweight Directory Access Protocol (i.e., LDAP), Active Directory (i.e., AD), Remote Authentication Dial-In User Service (i.e., RADIUS) or Kerberos. All logs, logging methods and procedures, and transactional information produced by or for any of these or similar systems are specifically considered critical to the protection of the IT infrastructure.

4. **Procedures And Support Structure Information -** On-call schedules and procedures; incident response procedures (except general incident response policies); internal communication methods (cell-phone and pager numbers and carriers); vendor service contract information and procedures; and closed security and incident response mailing list information, composition, and contents.

Log Retention
Network and system logs related to:

- Payment card (i.e., debit or credit card) transactions must be retained for 1 year.
- Personally identifiable health information (i.e., PHI) must be retained for 6 years.

All other network and system logs will be retained for 90 days and include, but are not limited to:

- Server Operating System Logs (e.g., NT)
- Email Records
- Voice Over IP Activity Logs
- Internet Usage Monitoring Software Logs
- Remote Access Logs
- Network Edge Routers
- Database Transactional Logs
- Firewall Logs
- Intrusion Detection Software Logs
- Software Security Monitoring/Violation Logs

Depending on the type of logged data, it may be appropriate to archive it to external data media. Regular checks followed by archiving of the logged data will ensure that the volume of log files does not grow to an inordinate size.

Staff trained to understand and interpret the specific type of log data should regularly review system/event logs. When feasible and possible, automated tools (e.g., Audit Record Generation and Utilization System - ARGUS) should be used to facilitate log analysis.