

Network Monitoring Guidelines

1. Purpose	1
2. Scope	1
3. Guidelines	1
4. Reference	3
5. Revision History	4
6. Approvals	4

1. Purpose

The purpose of this document is to outline university policy regarding the monitoring, logging, and retention of network [packets](#) that traverse [university networks](#). The University of Texas at Austin takes all reasonable measures to assure the integrity of private and confidential electronic information transported over its networks. The goals of this policy are to maintain the [confidentiality](#), [integrity](#), and [availability](#) of the university's network infrastructure and information assets. Any inspection of electronic data packets, and any action performed following such inspection, will be governed by all applicable federal and state statutes and by university and UT System policies and regulations.

2. Scope

This policy applies to all [IT Custodians](#) and [IT Owners](#) of department or enterprise [information technology resources](#) (including, but not limited to, any networking devices, network monitoring devices, computers acting as network monitoring devices, [intrusion detection systems](#), other packet sniffing devices, logs of other devices such as firewalls, and flow detectors monitoring network activity) operating on a university network.

3. Guidelines

1. Two groups on campus are authorized to routinely monitor traffic on university networks. These groups are *Information Technology Services-Networking* and the *Information Security Office (ISO)*. Additional campus IT staff may be approved to access and monitor specific traffic on specific networks for which they are responsible. Authorization must be attained from the respective IT Owner(s) of the given College, School, or Unit and the Office of Institutional

Network Monitoring Guidelines

Document Version: Approved

Relations and Legal Affairs or the Office of Compliance. The individual(s) must also complete a [Position of Special Trust form](#) and undergo a standard background check if not already completed. This approval shall also be communicated to the ISO and ITS-Networking. Authorized personnel must demonstrate a need for and an understanding of the operation of network monitoring devices.

2. Authorized staff shall use network monitoring devices only to detect:
 - known patterns of attack or compromise;
 - the improper release of confidential employee or student data;
 - or to troubleshoot and analyze network-based problems.

Authorized staff may also analyze certain network-based anomalies to determine the security risk to the university and conduct statistical/operational studies. All monitoring shall be as narrow in scope as possible.

3. Authorized staff may not exceed specified scope of monitoring (for example, users, address ranges, protocols, signatures). Only ITS-Networking and the ISO may monitor public networks and inter-campus networks.
4. Personnel authorized to analyze network traffic shall not disclose any information realized in the process without approval of the respective Vice President or department head and the Office of Institutional Relations and Legal Affairs or the Office of Compliance (with the exception of escalation to the ISO or ITS-Networking for investigation or assistance).
5. No authorized personnel shall use network monitoring devices to monitor employee electronic transmissions for job performance evaluation, or as part of an unofficial investigation, without first receiving signed approval from the Office of the Vice President for Employee and Campus Services and the Office of Institutional Relations and Legal Affairs.
6. The ISO will be the contact for resolution of security-related anomalies or other suspicious activity noticed by representatives in ITS-Networking or in other departments.
7. All monitoring points will be architected, approved, and configured by ITS-Networking. Monitoring points and associated devices may not be extended physically or virtually (such as through a VPN) or changed without written approval from ITS-Networking. ITS-Networking shall maintain written records of all monitoring points, architectures, and agreements.
8. Monitored data and usage logs will not be stored past the period of active investigation. ITS-Networking and the ISO may store incident related data as required. Unrelated monitored data may not be stored by anyone except as required by law. ITS-Networking and the ISO may store aggregated data and usage logs for operational, compliance, and statistical purposes. Usage logs must be purged as per campus policies.
9. Monitoring data stores and logs may not be accessible from the public Internet. All personnel must show due care in protection, handling, and storage of all monitored data and logs. Off campus access to monitoring data stores and logs must be authorized and updated by ITS-Networking as part of the monitoring point agreement.
10. ITS-Networking and the ISO have the authority to discontinue service to any network or network device that:
 - is in violation of this policy,
 - has demonstrated an operational hindrance or threat to UTnet, or
 - is a threat to the Internet community, in general.

In such cases, ITS-Networking or the ISO shall notify the local [IT-Networking Custodian](#) of the disconnection. In less threatening situations, ITS-Networking and ISO representatives will contact the local network administrator and inform them of specific actions that must be taken to avoid imminent disconnection. If corrective actions are not implemented as soon as possible, ITS-Networking or the ISO may discontinue service.

11. All normal requests for monitoring assistance from external agencies shall be coordinated through the ISO. Exceptional/urgent requests are to be directed to ITS-Networking (24x7x365), which will comply as appropriate and inform the ISO as lawfully allowed.
12. ITS-Networking will be responsible for the architecture and operations of all network facilities/functions required for [Lawful Intercept](#) assistance and compliance, and will be responsible for executing all requests as coordinated through the ISO. Departments will comply with all ITS-Networking requirements and assist ITS-Networking to fulfill its legal obligations.
13. Misuse or destruction of information technology resources can vary in severity and appropriate disciplinary actions should be taken in proportion to the severity of the incident. It is not the role of Information Technology professionals to carry out disciplinary actions as the result of an incident, but it is their role to monitor resources, to identify potential incidents and to bring such incidents to the attention of appropriate University of Texas at Austin officials. The following guidelines apply:
 - Suspected incidents involving student, faculty, or staff misuse of information technology resources should be brought to the attention of the ISO.
 - If an investigation involving review of the content of a faculty member, staff member, or student's files is required, written permission will be obtained from the Office of Legal Affairs and other departments, as necessary.
 - If it is determined that a misuse violation has occurred by a student, faculty, or staff member, this should be brought to the attention of the ISO. The ISO will consult with either the Human Resource Services or Student Judicial Services, as needed, and in the case of criminal violations, the University Police Department.
 - Violations by non-affiliates will be referred to the appropriate authorities. The Office of Legal Affairs may be contacted to provide direction in terms of identifying the appropriate authority.
 - Issues of departmental non-compliance may be reported to the respective executive management, the Office of Internal Audit, or the Office of the President.

4. Reference

- [UT Austin Acceptable Use Policy](#)
- [Information Resources Use and Security Policy](#)
- [Data Classification Standard](#)
- [Minimum Security Standards for Systems](#)
- ISO Incident Management Procedures
- ITS-Networking Policy & Procedures
- [UT System Policy 165](#)
- [UT System Policy 131](#)
- 18 U.S.C. § 2510: Electronic Communications Privacy Act

Network Monitoring Guidelines

Document Version: Approved

5. Revision History

Version	Date	New	Original
Network Monitoring Guidelines	3/2/2011	Converted web page to PDF	No changes
(online)	10/1/2009	Updated visual appearance to new template. Corrected any out of date links to ensure they are pointing to the most current policy documents.	
(online)	07/02/2008	Replaced reference to "Security Sensitive form" with "Position of Special Trust form"	The individual(s) must also complete a Security Sensitive Form
(online)	9/14/2007	Added this Change Log. Removed "Telecommunications and" from ITS-Networking and updated all references to ITS-Networking. Changed reference in section I. Purpose and References sections to UTS-165. Removed references to BPM 53, 66 and 67 (consolidated into UTS 165). Changed reference from UT System 67 to UTS 131 Added links to electronic documents.	"Information Technology Services- Telecommunications and Networking", "ITS-TN." "UT System Business Procedures Memorandum 53 UT System Business Procedures Memorandum 66 UT System Business Procedures Memorandum 67"

6. Approvals

Name	Role	Members	Date
Information Technology Services - Networking	Approval		9/14/2007
Chief Information Security Officer	Approval	Cam Beasley	9/14/2007