

**University of Utah**  
**Office of Information Technology**  
**Network Monitoring Policy**

November 15, 2001

I. PURPOSE

The purpose of this document is to outline University policy regarding the monitoring, logging and retention of network packets that traverse the Campus Network Backbone. The goals of this policy are:

- A. To maintain the integrity and security of the University's network infrastructure and information assets,
- B. To collect information to be used in network design, engineering, troubleshooting and usage-based accounting.

This policy acts in conjunction with the Information Resources Policy (PPM 1-15), and provides additional information with regard to the practice of the monitoring, of University network activity. Compliance with the policies referenced herein is required for connection to the Campus Network Backbone, as well as the use of and access to University of Utah Information Resources by any University of Utah department, division, or organization.

II. INTRODUCTION

The University of Utah considers all electronic information transported over the University 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 University policies.

III. REFERENCES

Network Communications (NetCom) Network Connection Procedures  
Office of Information, Network Connection Policy  
Policy and Procedures 1-15: Information Resources Policy  
Policy and Procedures 1-12: University Institutional Data Management Policy  
18 U.S.C. § 2510: Electronic Communications Privacy Act  
Utah Code Ann. § 76-6-703: Utah Computer Crimes Act  
Utah Code Ann. § 63-2-101 et seq.: Government Records Access and Management Act ("GRAMA")

IV. 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. See PPM 1-15.
- B. Institutional Data – Data that is generated, acquired, or maintained by University employees in performance of official administrative job duties. See PPM 1-12.
- C. ISO – Institutional Security Office

- D. Inter-network Communications – Communications that must traverse areas of network operations that are not under the immediate control of the local department and/or division network administrator
- E. Intra-network Communications – Communications that remain local to the network under the control of the local department(s) and/or division(s).
- F. NAP – Network Access Point. The interconnection point for several major Internet service providers.
- G. Network Backbone – The physical and electronic network infrastructure, currently under the operational administration of the Network Communications Department (NetCom), allowing for inter-network communications between Local Area Networks (LANs) and virtual LANs (VLANs), including access to Internet and advanced research networks.
- H. Network flow – The unidirectional sequence of packets between given source and destination endpoints
- I. NOCC – Network Operations Control Center. Monitors the health of critical services, and provides the central coordination of data services for campus.
- J. Packet – Electronic unit of data that is routed between an origin and a destination on a network.
- K. Packet Data – The part of the packet containing user data and other data or information used by applications.
- L. Packet Header - The first part of the packet, which contains protocol, source address, destination address, and other controlling information.
- M. University College, Department, or Division – Any University of Utah organization requiring and or requesting direct backbone network connectivity.
- N. VLAN – Virtual Local Area Network. A LAN defined on a basis other than physical location.
- O. Sniffer – A program that monitors and analyzes network traffic. A sniffer can be used legitimately or illegitimately to capture data being transmitted on a network.
- P. Promiscuous Mode - Mode of operation in which every data packet transmitted is received and read by every network adapter. Promiscuous mode is often used to monitor network activity.

## V. SCOPE

This policy applies to all users of University of Utah information resources over networks that cause traffic to traverse the Campus Network Backbone. The policy extends from the Network Access Point (NAP) to the end-user machine.

## VI. POLICIES

- A. Monitoring network traffic at the University of Utah will involve only the collection of packet header information, not the packet data, unless required to check for viruses, to monitor the improper release of confidential patient, employee or student information, or for intruder detection.
- B. Two entities on campus are authorized to routinely monitor traffic on the network backbone. These are authorized personnel in the Department of Network Communications (NetCom) and the Institutional Security Office (ISO).
- C. Intranet traffic may be monitored by local college(s), department(s) and division(s) at the discretion of the cognizant Dean, Department Head, or Vice President. If a college, department or division intends to perform network monitoring for purposes other than routine network operations, diagnostics and

maintenance, the network administrator will notify the Institutional Security Office of such network monitoring activity.

- i. The use of sniffers or devices, which operate in promiscuous mode, are to be used only by the authorized local network administrator for diagnostic purposes of intranet traffic only.
- ii. Users must not intercept or attempt to intercept or access data communications not intended for that user, for example, by "promiscuous" network monitoring, running network sniffers, or otherwise tapping phone or network lines, and must respect users' rights to privacy as outlined in PPM 1-15, (5.B).

D. Personnel authorized to analyze network backbone flow as set forth in paragraph B above, will not disclose any information realized in the process without approval of the cognizant dean or department head. Departments may request flow information with Vice Presidential approval. The method to request this information is as follows:

- i. A memo from the cognizant dean or department head must be sent to the appropriate Vice President requesting network backbone flow information generated by a campus user's machine.
- ii. The Vice President must determine if the request merits the involvement of the ISO and/or NetCom, and authorize their involvement via the appropriate form.
- iii. The ISO and/or NetCom will analyze the backbone flow information to establish the security risk to the University of Utah. If there is a risk, the ISO will proceed to examine the flow of the packets, and will take the necessary action. If there is not a security risk, but other issues are identified, (e.g., acceptable use as defined in University PPM 1-15) the ISO will return the request to the Department Security Officer (DSO) in NetCom.
- iv. The DSO will then release the requested subset of data to the requesting dean or department head.

E. The Institutional Security Office will be the contact for resolution of anomalies or other suspicious activity noticed by the Campus Security representative at the Network Operations Control Center (NOCC).

F. Through the NOCC, the NetCom Department will monitor the Campus Backbone Network 24 hours a day, 7 days a week. All network failures and excessive utilization will be reported to the technical staff for problem resolution or design enhancement. The NOC will act as the Point of Contact for campus network backbone traffic problems

G. Employee Electronic Transmission Monitoring

This policy does not govern the monitoring of employee electronic transmissions for job performance evaluation. This activity is governed by University Policy PPM 1-15 Paragraphs B.3.a to c.

H. Internet Services Monitoring

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 the University of Utah 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 University's Internet links.

- I. 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 that are not destroyed may be subject to production if a relevant "GRAMA" request is received.

- J. Disconnect Authorization

NetCom has the authority to discontinue service to any network or network device that is in violation of this policy or has demonstrated a hindrance to network backbone performance. If the threat appears to be security-oriented, consensus by one authorized NetCom representative and one ISO representative will be required to discontinue service. NetCom and ISO representatives will inform the local network administrator and inform them of specific actions that must be taken to avoid disconnection. If the Network Administrator is not responsive, NetCom may discontinue service. NetCom and ISO representatives will inform local administrators of corrective actions that must be implemented to avoid disconnection. If corrective actions are not implemented within a reasonable time period, NetCom may discontinue service.

More information regarding authorization to disconnect can be found in ISO Minimum Security Requirements and Practices Guideline (in process).

- K. Enforcement

NetCom, ISO, and the Office of Public Safety will cooperatively utilize information about traffic flow on the University of Utah Network backbone and Domain Name System (DNS) data space to enforce provisions set forth in the Network Connection Policy, the Network Monitoring Policy, University Information Resources Policy, other University policies, and State and Federal laws.