

DRAFT

Policy on the Use of the Campus Network

Office of the CIO
The Ohio State University

January 25, 2004

General Statement

The Ohio State University and university community members rely on reliable and ubiquitous access to network-based electronic information and communications resources to support the university's teaching, research, and outreach missions. To provide for this access, the university maintains and operates the OSUNet (formerly SONNET) campus-wide data network. This network connects all campus facilities through a high-speed backbone and also provides worldwide Internet and Intenet2 connectivity. It is basic tool for community information exchange and collaboration on campus, throughout the greater regional community, and with national and international communities.

OSUNet is composed of the fiber optic and copper cables, routers, bridges, servers, repeaters, monitoring equipment, software, and other devices which enable the interconnection of building networks on the campuses. OSUNet facilities generally extend to the academic or administrative unit connection or demarcation point on a building entry network switch.

To ensure the optimal and reliable operation of this critical university resource the university Chief Information Officer (CIO) is responsible for the provision of OSUNet and for the development of policies regarding its operation and use.

Applicability

This policy applies to all university academic and administrative units using OSUNet facilities. The Office of Information Technology (OIT) is responsible for operating OSUNet and enforcing this policy.

Policy

Use of OSUNet facilities and deployment of devices connected through academic and administrative unit facilities to OSUNet is subject to compliance with the following:

- All use of OSUNet must be consistent with the university's *<Policy on Responsible Use of University Computing Resources>*.

DRAFT

- Use of OSUNet should be consistent with the tripartite mission of the university and with the strategies, directions, and initiatives of the university's *<Academic Plan>* and PlanIT Strategic Information Technology Plan.
- OIT will develop and continuously update technical guidelines and standards for devices connected directly to or through unit facilities to OSUNet, communications protocols supported on OSUNet, and both operational and security requirements for use of OSUNet in collaboration with the campus technical user community. The community will be represented by the PlanIT Stakeholders Group *<Need new name>* and the Ohio State University Network Working Group (OSUNETWOG).
- OSUNet technical operational and security guidelines and standards are available at *<Technical Standards and Operational Requirements for OSUNet>*. Academic and administrative units and individuals using OSUNet as well as devices connected directly or indirectly to OSUNet and must comply with these guidelines and standards.
- University academic and administrative units are responsible for OSUNet traffic originating in their facilities and areas they administer. To help meet this responsibility university units may implement additional policies, guidelines, and standards in their physical or administrative areas of responsibility. Such policies, guidelines, and standards should be made available on unit web sites, should refer to this policy, and may not contradict this policy.
- To help the university responsibly administer Ohio State Internet traffic all OSUNet access must be authenticated and logged in accordance with the *<Technical Standards and Operational Requirements for OSUNet>*.
- Academic and administrative units, as well as community members, should be aware that the normal operation and maintenance of OSUNet requires OIT to routinely engage in backup and caching of data and communications, logging of activity, monitoring of general usage patterns, and security activities. However, OIT's use of information gathered in this manner is subject to the privacy constraints of the university's *<Policy on Responsible Use of University Computing Resources>*.
- OIT Enterprise Networking will work with academic and administrative units to help ensure use and compliance with this policy and with the *<Technical Standards and Operational Requirements for OSUNet>*. In the event of a conflict, OIT Enterprise Networking will work to negotiate acceptable compromise arrangements. If a compromise cannot be reached, the OIT Director of Enterprise Networking will specify a resolution.

Enforcement

A university unit using OSUNet in a manner that does not appear to be compliant with this policy or operating an apparently non-compliant device or service will be notified by

DRAFT

OIT so that the use, device or service may be brought into compliance. A use, device or service remaining noncompliant may be denied OSUNet access. To avoid disrupting university services, OIT will notify the unit prior to denying access except in perceived emergency situations. Noncompliant use of OSUNet may also be reported to university executive management with recommendations for corrective measures.

Individual use of OSUNet in violation of the university's *<Policy on Responsible Use of University Computing Resources>* may result in disciplinary action in accordance with the provisions of that policy.

In a perceived emergency situation OIT may take immediate steps, including fully or partially blocking OSUNet access, to ensure the integrity of the university data network and systems, safeguard the health and safety of university community members and property, or protect the university from liability.

All decisions, notifications, or measures taken under this policy may be appealed to the CIO through the CIO Office Director of Information Technology Policy and Services. Appeals should be submitted by email to ITPolicy@osu.edu.