Network Operations Manual

Contents

1. Purpose

The Network Operations Manual defines roles, responsibilities, minimum network standards, and operational requirements for all university networks as required by the University of Texas at Austin Information Resource Use and Security Policy, sections 16 and 17.

It is the responsibility of the University of Texas at Austin to:

- Operate reliable networks with appropriate redundancies in order to meet minimum standards.
- Designate operational responsibility for the university's networking infrastructure to Information Technology Services (ITS) Networking and Telecommunications (henceforth, ITS Networking).
- Assign Network Custodians to be accountable for Unit networks.
- Centrally maintain accurate records of all networked equipment and all network use by individuals or devices.
- Monitor network activities in accordance with Network Monitoring Guidelines.
- Approve all means of network access, connectivity, and configuration.
- Offer a process to allow Units to file requests for exceptions (see section 7. Exceptions/Adjudications).

2. Scope

This manual applies to all networks at The University of Texas at Austin, including the Main campus, Pickle Research Center (PRC), and remote sites.

3. Audience

The Network Operations Manual is primarily intended for Network Custodians and ITS Networking. It also provides guidance for all individuals who may be authorized to connect to any University of Texas at Austin network, such as, but not limited to, faculty, students, staff, contractors, and vendors. These users may be concerned with roles (section 4.3) and minimum network standards (section 5).

4. Roles and Responsibilities

4.1 ITS Networking

Pursuant to the Information Resource Use and Security Policy (IRUSP) sections 16 and 17, ITS Networking is charged with operations of all university networks. Responsibilities of ITS Networking:

4.1.1 Decisions that have a campus-wide impact shall be reviewed by ITS management and the Information Technology (IT) Architecture and Infrastructure Committee (AIC) and/or the Operational IT Committee (OIT), depending on scope and impact.

4.1.2 Is responsible for interpretation and intent of this manual, with oversight from the AIC.

4.1.3 Is generally responsible for funding common good network elements identified by the IT Governance Strategic Information Technology Accountability Board (SITAB).

4.1.4 Must approve the procurement by any Unit of all network equipment and service acquisitions, configurations, and operations, thereby ensuring compatibility with the campus network architecture, management platforms, operations, and security. Examples of procurements requiring approval include, but are not limited to, cabling, telecom spaces, switches, routers, wireless access points (WAPs), firewalls, load balancers, virtual private networks (VPNs), and domain name service (DNS) and DHCP (dynamic host configuration protocol) servers and proxies.

4.1.5 Must provide oversight for network usage.

4.1.6 Must provide Fault, Configuration, Accounting, Performance, and Security management (FCAPS) for all compliant networks.

4.1.7 Will solely operate all border, core, distribution, and wireless layers of university networks.

4.1.8 May delegate appropriate responsibilities for edge layer networks (henceforth Unit networks, excluding wireless) to qualified local Unit support staff, under its oversight and support. ITS Networking must provide operations support and develop systems, guidelines, procedures, knowledge bases, training and certifications to support delegates in this role.

4.1.9 Is responsible for establishing standards and management of all network naming and addressing. Examples include DNS and Internet Protocol (IP) addresses.

4.1.10 Is responsible for allocating all resources and directing recovery of network operations in event of disaster at behest of university disaster response teams.

4.1.11 Will ensure all applicable state and federal laws; university policies, rules and procedures; and applicable codes are followed; escalating to proper authorities as required. ITS Networking will work with university officials to interpret policies as applied to network operations and policies, and document them for campus. ITS Networking will respect and support unique Unit rules and policies as long as they do not conflict with this manual.

4.1.12 Will evaluate requests for exceptions to network standards, policies and operations, and maintain documentation of all exceptions granted. (see section 7)

4.1.13 Will adjudicate disputes and allocations of network resources and expenses between Units, and for campus-wide resources of common interest. (see section 7)

4.2 College, Schools, Departments or Units (henceforth Unit)

4.2.1 Unit

4.2.1.1 Must designate a "Network Custodian" in the university Organizational Hierarchy System (OHS Contacts), to be delegated appropriate responsibilities to operate portions of Unit networks. This individual is also known as the Network Manager. Designation must be reviewed annually to sustain the chain of authorizations.

4.2.1.2 Decisions shall be reviewed and approved by Unit management, ITS Networking, AIC and/or OIT, depending on the scope and impact.

4.2.1.3 Is generally responsible for funding network elements not identified by SITAB as common good.

4.2.1.4 Will generally operate edge network equipment (excluding wireless) under ITS Networking's oversight. Including end user device moves, adds, and changes.

4.2.1.5 Shall maintain their network to the Minimum Network Standards in this document (see section 5), and determine and fund any additional investments above the minimum standards.

4.2.1.6 Must comply with training and certification requirements. Unit managers who further delegate duties amongst their staff are responsible for ensuring those staff members' qualifications and immediately revoking network management access and privileges as positions change.

4.2.1.7 Will assign individual host addresses and host names locally based on allocations, rules, and procedures provided by ITS Networking.

4.2.1.8 Must follow all applicable state and federal laws; university policies, rules and procedures; and applicable codes; reporting violations to proper authorities when they are discovered and executing operational directives from the Information Security Office (ISO) and ITS Networking. Units may also create local rules and policies, as long as they do not conflict with established university rules and policies or this manual.

4.2.1.9 Must seek written exceptions to network standards, policies and operations as required. Units will evaluate requests for local exceptions to Unit network

standards, policies and operations that do not conflict with this manual, and will maintain documentation of all exceptions granted.

4.2.1.10 Will adjudicate disputes and allocations of network resources and expenses within their Units, and seek ITS Networking's assistance for issues that involve anyone outside their Unit, including, but not limited to, other Units, students, organizations, etc.

4.2.1.11 Must develop local disaster recovery plans when operating their own networks. Operation of networks without ITS Networking support is only allowed by exception (see section 7).

4.2.2 Network Manager

4.2.2.1 Is accountable for adherence to these procedures and the Units' general network operations as delegated by ITS Networking.

4.2.2.2 May designate Technical Support Coordinators (henceforth Network TSC) to carry out additional networking responsibilities.

4.2.3 Network Managers and Network TSCs

4.2.3.1 Must complete and acknowledge the position of special trust designation annually.

4.2.3.2 Must complete approved network tools training or have equivalent experience. ITS Networking will confirm qualifications.

4.2.3.3 Must maintain accurate and current contact information in tools provided by ITS Networking. This includes campus and off-campus/non-UT phone number and e-mail. Emergency cell phones should be included for urgent issues. This information will not be shared or used except for network escalation purposes (see 6.2.5).

4.2.3.4 Must subscribe to and actively monitor e-mail, lists, sites, and forums used to announce planned and unplanned maintenance and outages. Currently, this list consists of:

- IT-Updates@utlists.utexas.edu mailing list
- ITS Services Status Web site
- E-mail messages to e-mail address as listed in the tools provided by ITS Networking
- Tech Staff Portal

4.3 Faculty, Students, Staff, Official Visitors, Affiliates and others granted network access:

4.3.1 Must follow the Information Resource Use and Security Policy.

4.3.2 Must adhere to all network access rules.

4.3.3 Must not extend university networks by any means, including, but not limited to using routers/switches/hubs, physical or logical wireless mechanisms, tunnels, or other methods, without authorization from Unit network personnel or ITS Networking.

4.3.4 Must not engage in activities placing network operations in jeopardy.

4.3.5 Should quickly report and escalate network problems and security issues they encounter so that such problems may be quickly remediated, and should make themselves available for investigations to resolve the problems.

5. Minimum Network Standards

These minimum network standards establish goals to support the university's mission and to attract and retain the best faculty, students, and staff. All networks will be measured according to these standards and reported annually by ITS Networking to aid Units, IT governance and university leadership in the management of this critical resource. These standards are to be reviewed and updated every two years and as required.

5.1 Life-Safety Standards

Campus networks are not designed or operated to meet life safety standards. Life safety-class systems should utilize multiple modes of communication.

5.2 Building Networks

5.2.1 Access Layer–Wired

5.2.1.1 Upon request, each individually assigned workspace shall have available at least one wired Ethernet port. That Ethernet port shall be connected to an ITS Networking supported access-layer device properly installed in an MDF/IDF communication closet.

5.2.1.2 All wired network ports shall support a minimum of 10/100 Base-T switched Ethernet. Any new or upgraded wired network port shall support a minimum of 10/100/1000 Base-T switched Ethernet. 

5.2.1.3 The minimum performance characteristics for a wired Ethernet port on the main campuses shall be:

- Throughput: at least 90 megabits per second (Mbps)
- Packet Loss: less than 0.1%
- Round Trip Time: less than 5 milliseconds (ms)
- Jitter: less than 20 ms

5.2.1.4 Port Performance Verification

A port may achieve minimum performance requirements yet still provide poor service, especially for delay-sensitive protocols. As a rule of thumb, it is recommended that links (and supporting uplinks) should not exceed 35% of capacity at the 95th percentile in order to support delay-sensitive traffic. A recommended practice is to ensure all uplinks have more capacity than any single host can consume (for example, 1-Gigiabit uplink for 100 Mbps edge ports, 10-Gigabit uplink for 1-Gbps edge ports).

5.2.1.4.1 ITS Networking is the arbiter for measuring performance metrics.

5.2.1.4.2 All testing will be conducted by ITS Networking using their measurement services, located on the main campuses. Special testing software/equipment may be required by ITS Networking to verify port performance.

5.2.1.4.3 Testing will be conducted during busy hours for the port in question (typically business days between 13:00-15:00 hours).

5.2.1.5 All access-layer devices shall connect directly to the building point-of-presence (POP) device or to an appropriate aggregation device that connects to the POP device at gigabit speeds or higher.

5.2.2 Access Layer (Wireless)

IEEE 802.11g wireless networking (WiFi) is the minimum required standard. 802.11 a/n at the 5 GHz band, and 802.11ac is required for all new WiFi installations or upgrades.

5.2.2.1 Indoor WiFi

5.2.2.1.1 Ubiquitous indoor coverage of a density and capacity to meet performance metrics (5.2.2.1.3) during normal usage shall be provided.

5.2.2.1.1.1 As a general guide, one access point per 2,500 square feet provides sufficient coverage for typical university construction. High population areas will require a greater density. ITS Networking are necessary [forthcoming link to standard].

5.2.2.1.1.2 Typical exception scenarios envisioned include: large non-academic venues, tertiary mechanical spaces, un-occupied areas of warehouses and seldom occupied library stacks.

5.2.2.1.2 All classrooms shall have sufficient density to support all rated occupancy to conduct standard classroom activities, as defined by the Research and Educational Technology Committee (R&E), and resiliency to meet required SLAs by R&E..

5.2.2.1.3 The infrastructure shall provide end-device performance that meets or exceeds that of a typical residential broadband connection (currently 7 Mbps download and 384 kilobits per second (Kbps) upload to campus testing servers). Radio Frequency power levels shall be a minimum signal-to-noise ratio (SNR) of 25 decibels (dB).

5.2.2.1.3.1 High-density classroom environments may be exempted from meeting these performance metrics.

5.2.2.2 If 5GHz coverage is available in an area and meets these metrics, underperforming 2.4GHz coverage is acceptable.Outdoor WiFi

Outdoor WiFi shall be provided in areas adjacent to buildings. Full outdoor coverage is not a goal for the university at this time.

5.2.3 Distribution Layer

5.2.3.1 All university buildings and structures on the Main and PRC campuses shall be required to connect with a minimum of dual 1-gigabit routed Ethernet connections from the building POP device to the campus network backbone. The POP device shall be appropriate to the building size as recommended by ITS Networking. Buildings classified as “medium” or “large” shall be required to have dual 10-gigabit routed Ethernet connections.

5.2.3.2 Sites handling sensitive data shall consult with ISO and ITS Networking to determine if portions of their networks should utilize network layer security precautions, such as firewalls, access control lists (ACLs), or VPNs.

5.2.3.3 Campus emergency power is recommended for POP devices in existing installations. Emergency power is required for POP devices in new construction and renovations.

5.2.3.4 Connectivity needs for off-campus sites vary, and their connectivity requirements will be determined by ITS Networking based on available technology offerings and financial resources.

5.2.3.5 Uninterruptable power supply (UPS) units are recommended for POP devices, but are not required. If a UPS is utilized on a single power supplied device, an automatic transfer switch connected to both regular power and the UPS must be in-line between the device and UPS.

5.3 Building Network Cabling and Facilities

5.3.1 Inside building copper cabling for networking

5.3.1.1 Each individually assigned workspace shall have at least two copper cables available for the individual's use for Ethernet, telephone, etc. The presence of fiber ports does not discharge this requirement.

5.3.1.2 All copper cabling shall be Category 5 or better. All new installations shall be Category 5e or better, except for WiFi and 10Base-T installations which shall be Category 6a or better. Copper cabling for Ethernet shall meet or exceed the minimum requirements needed to deliver gigabit Ethernet within the distance specification (100 meters).

5.3.1.3 Copper cabling shall be terminated in 8-pin "RJ-45" patch panels or 110 blocks in approved MDF/IDF telecommunications closets, unless otherwise approved by ITS Networking. New installations must terminate on 8-pin "RJ-45" patch panels.

5.3.1.4 Access-layer network devices may connect to POP device or approved aggregation device over copper cables.

5.3.2 Inside Building Fiber

Access-layer network devices or end users connecting to the building POP device or approved aggregation device over fiber can use either single-mode or multi-mode fiber. In the event that multi-mode fiber (MMF) is used, the minimum standard is 50 micron (µ), 2000/500 megahertz per kilometer (MHz-Km) MMF. Existing installations of 62.5µ, 200/500 MHz-Km MMF will be grandfathered until they are no longer able to support the minimum connection requirements for access-layer or aggregation devices.

5.3.3 Outside Plant Fiber

All distribution-layer devices shall connect to the campus network over redundant fiber media.

5.3.3.1 Two single-mode fiber pairs (SMF-28) are required for all buildings on the main campuses.

5.3.3.2 Geographic diversity and dual entry for individual building fiber uplinks is recommended, and shall be installed for all new construction.

5.3.3.3 ITS Networking must maintain geographic diversity for single mode fiber plant for concentrations of buildings and major concentration feeds.

5.3.4 Telecommunications Closets (MDF/IDF)

5.3.4.1 Units shall furnish dedicated spaces to house telecommunications cabling and equipment in each building. These spaces consist of the Main Distribution Facility (MDF) and, as needed, Intermediate Distribution Facilities (IDF). The building manager and building occupant(s) will designate the space.

5.3.4.2 By default, MDF/IDF specifications shall adhere to UT Austin construction standard 27 11 00 Communication Rooms, to support current minimum network standards, which is inclusive of ANSI-J-STD-607-A, ANSI/NFPA 70, ANSI/TIA/EIA-606-A, NECA/BICSI-568, NECA/BICSI-607, and TIA-569-B. Deviations from the standard must be reviewed and approved by ITS Networking and the building manager prior to implementation. To reduce ongoing costs and IT footprint across campus, buildings must be designed with the fewest number of MDF/IDFs required to function according to minimum network standards.

5.3.4.3 Power and cooling capacity shall be planned to accommodate at least a 33% growth from initial deployment.

- Power load shall not exceed 75% of the maximum circuit capacity based on the initial deployment.
- Cooling capacity shall be designed to handle appropriate environmental conditions, as defined by the network equipment specifications, at maximum power load in the MDF/IDF.

5.3.4.4 All MDFs shall have a telephone line that is independent of the building's network.

5.4 Minimum Network Services

ITS Networking shall support the following network services on campus networks. Units shall support these services at the same level.

5.4.1 IPv4 (Internet Protocol version 4).

5.4.2 DNS shall be provided as reliably as the local network.

5.4.3 DHCP shall be provided as reliably as the local network.

5.4.4 NTP (Network Time Protocol Version 4) shall be provided as reliably as the local network with Stratum 2 accuracy.

5.5 Facilities Network

5.5.1 All Units shall provide Ethernet ports for Facilities Network (henceforth FacNet) connections (utilities monitoring, building security, etc.) upon request in fair proportion to their occupancy of the building.

5.5.2 A dedicated switch for facilities network connections is recommended, but not required. For all new building construction or major renovation projects, dedicated facilities

network switches are required for all MDF/IDF telecommunications closets to meet all facility network port needs. These switches should be placed on UPS and emergency power when available.

5.6 Network Lifecycle

Units shall plan for the replacement lifecycle of network equipment and infrastructure. The lifecycle is determined by its ability to provide adequate performance, vendor support levels, compatibility with the campus network, failure rates, and ability to meet minimum standards. Networking will report on the specific lifecycle status of equipment and infrastructure (6.12.3). For advanced planning purposes, the following guidelines may be used based on general campus experience:

5.6.1 Distribution layer devices typically have a useful life of seven years.

5.6.2 Application layer network devices, such as firewalls, VPNs, and load balancers, typically have a useful life of five years.

5.6.3 Access layer devices typically have a useful life of seven years for wired and five years for wireless.

5.6.4 Network cabling is expected to have a useful life of fifteen years. The useful life is determined by the capability of the cabling infrastructure to transport network traffic in accordance with the minimum network standards. For example, Category 3 cabling cannot transport 100Base-TX and shall be replaced.

5.7 Unit network response profile shall be:

Incident Type	Response / Resolution Time
Multiple switches or wide-spread non-functioning wireless area	Resolve or escalate to ITS Networking within two business hours.
Single switch	Resolve or escalate to ITS Networking within two business hours.
Malfunctioning wireless AP	Resolve or escalate to ITS Networking before the end of the next business day
Single end-user connection (wired/wireless)	Respond, escalate or resolve before the end of the next business day.

6. Operations

6.1 Protecting operations

6.1.1 ITS Networking and Unit must take all reasonable measures to physically and logically secure their network infrastructure to prevent unauthorized access which could contribute to an outage or compromise. This includes:

6.1.1.1 Ensuring that all telecommunication spaces remain locked at all times.

6.1.1.2 Limiting the ability to grant access to the MDF/IDF to ITS Networking.

6.1.1.3 Closely controlling access to the MDF/IDF, as granted by ITS Networking, from non-authorized personnel.

6.1.1.4 Limiting distribution of MDF/IDF keys and/or keycards to authorized personnel.

6.1.1.5 Protecting device passwords from distribution.

6.1.2 ITS Networking must take all necessary and legal actions to maintain network operations over all other IT concerns. While prior consultation is envisioned and recommended, this could include cessation of services to devices, individuals, buildings, Units and networks inside or outside of the university without prior notice. ITS Networking's actions are subject to post-action review by management (ITS and university executives), AIC and/or OIT.

6.1.3 ITS Networking may be directed to physically or logically reallocate Unit resources in the event of major incidents.

6.1.4 Wireless Spectrum

ITS Networking must track and approve allocation of all wireless spectrum to ensure non-interference of the university's wireless networks.

6.2 Service Level Agreements

6.2.1 Units and ITS Networking will maintain response and communication matrices for automated and manual alerts and escalations for network outages and communications as approved by AIC.

6.2.2 Unit must notify ITS Networking if they need assistance for edge network outages (see 5.7).

6.2.3 Urgent requests must be submitted via telephone (512-471-6387). Non-urgent requests must be submitted via the ticketing system (networking@its.utexas.edu). All requests will be entered in the ticket system.

6.2.4 Unit must communicate the scale of a problem to ensure the outage has been properly prioritized by ITS Networking, and must state its expectations of a reasonable resolution time.

6.2.5 ITS Networking is directed to immediately restore services to large populations (buildings and major MDFs/IDFs days, nights, weekends, and holidays) to avoid disruption of campus operations. Units must cooperate and assist ITS Networking as requested to restore service, including verification of restoration and ticket response, during and outside business hours. ITS Networking response times and service levels for campus networks will be:

Service	Initial Response, Business Hours	Initial Response, After Hours	SLA
Campus Network Backbone	Upon Detection	Upon Detection	99.98%
Commodity Internet	Upon Detection	Upon Detection	99.95%
Central DNS resolution services	Upon Detection	Upon Detection	99.98%
Central DHCP resolution services	Upon Detection	Upon Detection	99.95%
VPN Service	Upon Detection	Upon Detection	99.9%
Wireless Core	Upon Detection	Upon Detection	99.9%
Building Gateway Device	Upon Detection	<1 hour	99.9%
Building Aggregation Switch / MDF/IDF Closet (large)	Upon Notification	<1 hour	99.9%
Building Access-layer Switch	<2 hours Upon Notification	Next Business Day	99.5%
Building Wireless (multiple)	<2 hour Upon Notification	Next Business Day	99.5%
Building Wireless (single)	2 Business Days Upon Notification*	None	Best Effort
Single End-user Cable	2 Business Days Upon Notification*	None	99%
Resnet End-user	Before end of Next Business Day	Before end of Next Business Day	N/A

*Assuming any cable repair does not require construction or re-pulling.

6.3 Change Control and Incident Communications

6.3.1 Change Control

Change control processes must be followed for all network changes made by ITS Networking or Units. ITS Networking will establish and maintain change control procedures, mechanisms, and tools to be used outside of emergencies via its ticketing system (networking@its.utexas.edu).

6.3.1.1 Notification system

ITS Networking will provide a communication system for automatic or manual entry of contacts based on the affected sites or other criteria as defined by the change requester. Proper use of this system discharges communication responsibilities. All parties are required to maintain current contact information for this system to function (4.2.3.3), and to monitor and respond to these notifications in a timely manner (4.2.3.4).

6.3.1.2 Change Communications

All parties must notify each other using the notification system of network changes as specified in the change process. ITS Networking will inform Units of substantive changes it makes. Units will inform ITS Networking, other Units, and their end users of substantive changes they make.

6.3.1.2.1 For changes impacting campus as a whole, ITS Networking will use the current ITS notification process for campus changes.

6.3.1.2.2 Units are responsible for checking the notification system and ITS notification process (4.2.3.4).

6.3.1.2.3 Units are responsible for informing their end users via their own internal processes.

6.3.1.2.4 Authorization to proceed with a change will be assumed if not responded to prior to change request date, or reasonably specified response deadline.

6.3.1.2.5 ITS Networking and Units will use the notification system to communicate other activities they become aware of that could impact network operations, for example, building maintenance or unplanned events like an HVAC (Heating, Ventilation and Air Conditioning) outage.

6.3.1.2.6 Everyone with responsibility for the network (as defined in section 3) should set e-mail clients to provide out-of-office notifications when they are unavailable, or provide notification via ticket system to ITS Networking. Notifications should include whom to contact for assistance, or what other TSCs will be available.

6.3.2 Incident Communications

6.3.2.1 ITS Networking provides numerous tools that will automatically alert Unit to outages. Units will be notified at the account listed in the NetContacts tool for most networking issues that affect their customer base, and settings configured in other tools provided by ITS Networking. Phone calls may also be placed as appropriate, such as in the event of wide scale outage for a large building. (see 6.2 for incident response/SLA details)

6.3.2.2 For campus-wide incidents, ITS Networking will follow ITS Incident Communication Process. Additional notifications may be published to the IT-updates e-mail list as appropriate.

6.3.2.3 Units must keep their end users informed of incidents and estimated time of resolution.

6.3.2.4 End users should contact local support or ITS Help Desk for assistance with network outages.

6.4 Network Management via FCAPS (Fault, Configuration, Accounting, Performance, and Security)

6.4.1 All University network equipment must have full FCAPS management implemented. ITS Networking is responsible for defining FCAPS needs and implementing systems for Units.

6.4.2 Unit must work with ITS Networking to ensure full compliance with established FCAPS methods.

6.4.3 Units given exemptions to operate their own networks independently of ITS Networking must still implement FCAPS and submit every other year to reviews of their management model and systems by ITS Networking.

6.4.4 Fault Management

6.4.4.1 Processes will be implemented to detect, report, and escalate errors, alarms, and events; for example, monitoring ping responses from a device and notifying the responsible party when the device becomes unresponsive.

6.4.4.2 Processes will be implemented to prevent or provide early detection of faults based on anomaly detection and statistical logging; for example, establishing a baseline of "normal" behavior and triggering an alarm on significant deviation.

6.4.4.3 Procedures will be developed for responding to and handling faults to minimize their impact; for example, written response and escalation policies.

6.4.5 Configuration Management

6.4.5.1 Change control procedures (see 6.3.1) must be followed for all changes that can impact network operations.

6.4.5.2 All network equipment configurations shall be backed up daily, with the ability to restore current and archived configurations for the device.

6.4.5.3 The ability to change device configurations must be limited to only the appropriate parties within Unit and ITS Networking and accessible only via approved methods, such as remote command line interface (CLI) access only from protected management networks.

6.4.5.4 The level of access to make configuration changes must be limited to only permit changes within the individual's area of responsibility; for example, layer-2 versus layer-3 configurations.

6.4.5.5 Site logs that document devices, interconnections, and inventory data must be maintained for all facilities housing network equipment.

6.4.6 Accounting

6.4.6.1 AAA (Authentication, Authorization, and Accounting) services are required for all network equipment.

6.4.6.2 Only approved personnel within Unit and ITS Networking staff may have credentials to authenticate and access network equipment.

6.4.6.3 Authorization levels must be implemented to limit the extent of access that personnel have to appropriate levels.

6.4.6.4 Accounting records must be maintained for all network equipment to identify what users have accessed the devices and what actions were performed while on the devices.

6.4.6.5 Accounting records for resource utilization must be maintained for all network equipment; for example, CPU, memory, port utilization, and bandwidth consumption.

6.4.6.6 Accounting records allowing for the identification of users and their actions must be maintained securely and in accordance with 6.5.5.2, which follows the university and Texas State Department of Information Resources (DIR) records retention policies. Records shall include device addresses (IP and MAC addresses), location on the network (for example, switch/port or WAP), and identity of the user.

6.4.7 Performance

Resource utilization (CPU, memory, bandwidth, etc.), environmental conditions (power, temperature, and humidity), data and error rates (switch port traffic and errors, etc.) for all network equipment must be logged, and historical data must be kept in accordance with record retention policies. The data must be available for establishing baseline operating conditions, trending analysis, and capacity planning.

6.4.8 Security

6.4.8.1 All network equipment must be physically secured in controlled spaces (that is, MDF/IDF rooms) with access limited to authorized personnel (see 6.9.1).

6.4.8.2 Remote access to network equipment, such as VTY (terminal interface), SNMP (Simple Network Management Protocol), etc., must be restricted by isolating the management interface of the device from the general network and controlling access using appropriate AAA methods.

6.4.8.3 Remote access to network equipment must be logged. Logs must include the identity of the individual accessing the equipment, the remote IP address from which they accessed the equipment, and what actions they performed (command accounting).

6.4.8.4 Units and ITS Networking must compete annual audits to ensure that their staff have the minimum access to network infrastructure necessary to perform their job duties and access has been removed from staff whose roles have changed.

6.4.8.5 Appropriate encryption and access control methods for network infrastructure must be implemented, for example, ACLs, 802.1x authentication, secure shell (SSH), and encryption.

6.4.9 Network Management Tools Capabilities (TSC Tools)

6.4.9.1 ITS Networking must provide tools for the TSC community to implement FCAPS as defined in this document for all managed network infrastructure it supports. (see section 4.2.1.7 for Unit responsibilities)

6.4.9.2 Any application designed to programmatically interface with the TSC Tools must be approved by ITS Networking.

6.5 Network Access and Security

6.5.1 Network Access

6.5.1.1 Access to university networks by individuals is only permitted for university faculty, students, staff, designated official visitors and affiliates, and Unit-sponsored guests with business related to the mission of the university.

6.5.1.2 Access to university networks by non-university entities requires Unit sponsorship, ITS Networking's approval and may require a contract with the university. Written acceptance of the university's rules is required.

6.5.1.3 All entities using the university network must agree to and comply with the terms described in the IRUSP.

6.5.1.4 ITS Networking is responsible for mechanisms to authenticate and authorize users to the university network.

6.5.1.5 Units are responsible for ensuring network access is provided only to authorized individuals who follow approved network authentication procedures.

6.5.1.6 Units providing network access to minors must include proper indemnification for each minor (those notices may be combined with other indemnifications).

6.5.1.7 Approved third party networks, such as "attwifi", are operated by ITS Networking for non-university individuals. Sponsorship of non-university individuals (outside designated official visitors and affiliates) for use of university networks is discouraged.

6.5.2 Port/Access Security

6.5.2.1 Physical and/or logical access controls must be implemented for all network access.

6.5.2.2 Access control mechanisms and methodologies developed by ITS Networking must be reviewed and approved by AIC for campus-wide impact.

6.5.2.3 Private offices assigned to a single individual that are generally locked and secured are not required to implement additional end-user port security measures. The individual assigned to the space must be held responsible for network activity for all ports in their designated space.

6.5.2.4 Ports located in public spaces, such as labs, lounges, hallways, and unsecured conference rooms, must be secured via methods approved by ITS Networking and must report transaction logs to ITS Networking (e.g. ITS Networking operated 802.1x).

6.5.2.5 Shared offices shall be treated as public spaces due to the inability to track usage to a specific user of the space; and must be authenticated as directed by ISO or ITS Networking.

6.5.2.6 Access-layer network equipment must be compatible with ITS Networking's adopted mechanisms.

6.5.3 Public Networks

6.5.3.1 Appropriate use of public networks is described in the university's Acceptable Use Policy.

6.5.3.2 Only authentication methods operated by ITS Networking may be used to provide public network access.

6.5.3.3 Units may sponsor use of Public Networks provided:

- The use is related to the mission of the university
- Unit assumes responsibility and cost for that use for equipment or additional non-incidental bandwidth.
- Unit verifiably identifies people individually with AAA services provided by ITS Networking and assumes responsibility for the individual. Existing mechanisms include:

  6.5.3.3.1 Creating University Affiliates through the HR Management System (HRMS) with network privileges. This method is preferred.

  6.5.3.3.2 Creating Guest accounts through the ITS Network TSC Utilities. Intended to be brief and temporary. This method is discouraged, and third party network options, such as "attwifi" are more appropriate.

6.5.3.4 Faculty, students, staff, official visitors, and other affiliates must use the secured and encrypted "restricted.utexas.edu" wireless network unless their device is not supported, in which case they may file an exception.

6.5.3.5 ITS Networking will maintain the capability of creating open networks in response to campus emergencies.

6.5.3.6 Resnet is the residential network operated by ITS Networking for the Division of Housing and Food Services. Access is restricted to students living in the on-campus DHFS residences. Use is governed by the Resnet Acceptable Use Policy.

6.5.3.7 For network use that is unsponsored, external networks provided by ITS Networking, such as the third-party "attwifi" wireless network, shall be used.

6.5.4 Identity: Who, What, When, and Where

The identity of all users accessing the university networks, the time of their access, and the location (physical and network) must be recorded with ITS Networking's management systems.

6.5.4.1 Units and ITS Networking must not engage in activities to shield any user or device's identity from ITS Networking's tracking systems. For example, MAC address spoofing is not allowed.

6.5.4.2 Unit networks must interoperate with ITS Networking's tracking services.

6.5.4.3 Users, Unit, and ITS Networking must not host services, such as anonymous proxies or TOR tunnels, that anonymize or masquerade identity on the university networks.

6.5.4.4 ITS Networking shall work with Units to evaluate situations where devices, for example, firewalls, are necessary to secure or obfuscate network segments.

6.5.5 Network Activity, Logging, Tracking, and Monitoring

6.5.5.1 Units must have written approval from ITS Networking before recording user identifiable network activity and logs. See also the Network Monitoring

Guidelines, which restrict network monitoring of users' activities while on the network.

6.5.5.1.1 Network information that identifies users must not be used except for managing network and system resources.

6.5.5.1.2 Network information that identifies users must not be revealed to parties other than ITS Networking and the ISO.

6.5.5.1.3 Network information that identifies users must explicitly not be used for personnel management issues, such as attendance, performance, location, etc., unless part of an official investigation coordinated through the ISO with proper approval of Legal Affairs and Human Resource Services.

6.5.5.1.4 End users may request their identifying network information be revealed to other parties.

6.5.5.1.5 Network information that identifies systems may be used for inventory purposes.

6.5.5.2 Record retention for network activity and logs of infrastructure devices and users of the network must adhere to ITS Networking's record retention policy, which follows the university's and Texas State Department of Information Resources (DIR) records retention policies.

6.5.5.2.1 Transactional data includes items related to tracking a person's presence and use of the network, such as 802.1x logins. This data will be stored for six months.

6.5.5.2.2 Content data includes anything representative of person's activities while on the network, including URLs visited, servers accessed, content of those sessions, etc. This data may be stored a maximum of 14 days. Refer to the Network Monitoring Guidelines.

6.5.5.2.3 Statistical data regarding a person's consumption of network resources, such as bandwidth consumption, but which do not denote specific content data, may be stored for up to one year.

6.5.5.2.4 System log information that is not specific to users shall be stored only as long as needed to ensure system stability, investigate activities, track performance, and identify trends. This specifically includes staff activities on network devices. Records shall be stored a minimum of 90 days, depending on the volume of data required.

6.5.5.2.5 Aggregate statistical data, which does not identify individuals, may be stored indefinitely.

6.5.5.2.6 Data may be stored beyond the stated maximum retention lengths above if part of an official investigation or to investigate operational anomalies. For these cases, ITS Networking and the other party of the investigation must establish a date on which the data can be deleted.

6.5.6 Inventory and Device Tracking

6.5.6.1 NetContacts / TSC Tools

Units must maintain the following information in NetContacts for all systems (wired and wireless) that are owned by the Unit or are allowed to connect to the Unit's networks.

- MAC Address(es) – all MAC addresses assigned to device
- IP Address (if statically assigned)
- UT Inventory Tag (if assigned)
- System Serial Number (if exists)
- EID(s) of primary assigned user(s) (if assigned)
- Location (optional)

(Note: Concerns have been raised about the usability of the current NetContacts system. Further development will be needed to fix existing issues before this requirement takes effect. Including a new inventory role (so the person fulfilling inventory functions does not receive permissions or notifications). Extension to identify non-UT machines. Support multiple EIDs. Binding multiple MACs to one device.)

6.5.6.2 Personally owned devices connected to the Unit's networks must adhere to these identification requirements, with the exception of inventory information (UT Inventory Tag, Serial Number).

6.6 Bandwidth Management and Consumption

ITS Networking must implement bandwidth thresholds, allocation mechanisms, reporting measures, and enforcement mechanisms to ensure fair and efficient use of bandwidth as it relates to the university mission.

6.6.1 ITS Networking establishes bandwidth allocations for the Public Networks, to be reviewed by ITS management and R&E.

6.6.2 ITS Networking establishes bandwidth thresholds for Unit networks, to be reviewed by ITS management and R&E and/or OIT. (forthcoming link)

6.6.3 Units must:

6.6.3.1 Respond promptly to investigation requests, identifying individuals and actions, where known.

6.6.3.2 Review Unit consumption via available tools and work with Unit management to stay within thresholds or request additional bandwidth.

6.6.3.3 Report high usage and request clearance prior to extraordinary bandwidth consumption.

6.6.3.4 Educate Unit network users on appropriate use when users exceed thresholds.

6.6.4 Unit and ITS Networking must take all necessary actions to prevent network congestion, including traffic shaping or disconnecting users, hosts, Units, and buildings. Unit and ITS Networking are expected to exhaust normal management channels prior to impacting Units and buildings as long as it does not impact campus operations.

6.7 Naming and Addressing Services

6.7.1 DNS

6.7.1.1 All network names and addresses belong to the university as a whole and are administered by ITS Networking. ITS Networking must work with Units to minimize the impact of changes where possible.

6.7.1.2 Network names and addressing must follow the university's naming guidelines (forthcoming).

6.7.1.3 Naming and addressing must follow current ITS Networking practices including:

6.7.1.3.1 All addresses used must have current forward and reverse DNS mappings to the correct domain.

6.7.1.3.2 ITS Networking must provide the central DNS for authoritative name registrations and forward and reverse resolution services for clients.

6.7.1.3.3 ITS Networking must provide DNS delegation services for specific zones within the university's DNS namespace for Units as requested. This is not generally recommended.

6.7.1.4 Use of ITS Networking's DNS services is recommended for stability, reliability, and security.

6.7.1.5 Units operating their own authoritative DNS servers must update ITS Networking with current mappings of addresses to names at least daily.

6.7.1.6 Unit DNS servers and caches must use ITS Networking's recursive DNS servers.

6.7.1.7 Units providing Dynamic DNS Services must ensure security precautions are in place to prevent a client from advertising a name outside the Unit's assigned zone.

6.7.2 DHCP

6.7.2.1 ITS Networking must make available central DHCP services to all campus-routed networks. Users and Units will not be required to use the central DHCP service; however, it is recommended to achieve high levels of reliability.

6.7.2.2 Units operating their own DHCP services must keep and provide logs to ITS Networking and ISO upon request and follow retention policies.

6.7.3 NTP

Networking must provide accurate Network Time Protocol services. Users are not required to use this service; however, server administrators should understand the importance of time synchronization in clustered environments.

6.8 Protocols

ITS Networking will work with AIC to establish supported network protocols for the campus networks.

6.8.1 IPv4 is the only supported protocol on the campus backbones. Other protocols may be supported on Unit networks so long as they do not interfere with network operations. IPv4 multicast is experimental and may not function.

6.8.2 Protocol tunnels, such as those to support IPv6, must adhere to ITS Networking guidelines as developed.

6.9 Physical Infrastructure

6.9.1 Access

6.9.1.1 Entry to MDF/IDFs must be managed by ITS Networking.

6.9.1.2 The university's Building Access Control System (BACS) must be used to control access to MDF/IDFs. Existing data closets without BACS will be reported and plans for retrofitting them evaluated. All new construction and renovation projects must implement BACS on all MDF/IDFs in the building or renovated spaces. 

6.9.1.3 ITS Networking must grant access to MDF/IDFs to authorized and qualified Unit personnel, and those servicing or responsible for approved devices in MDF/IDFs, reporting to the Unit Network Manager when changes to access are made.

6.9.1.4 Unit requests for access to MDF/IDFs must be submitted by the Unit's network manager. ITS Networking must answer all requests for access by the close of the next business day from the time the request is submitted.

6.9.1.5 Unit network manager must review access granted to staff annually.

6.9.1.6 ITS Networking must be provided an unescorted path of ingress and egress to all network closets 24x7.

6.9.2 MDF/IDF Telecommunication Spaces

6.9.2.1 Devices installed in MDF/IDFs are restricted to network, telecom, cable TV (CATV), and building systems (fire/security/utilities) due to security sensitivity, heat/power load, and space constraints. Servers unrelated to operating these systems, for example, file servers, print servers, and multi-user systems, may not be placed in the MDF/IDFs.

6.9.2.2 Closets must be kept clean and free of all trash and debris.

6.9.2.3 Environmental monitoring for temperature, humidity, leaks, standing water, etc., are required for MDFs and recommended for IDFs. ITS Networking will operate the monitors and include them in automated escalation notifications.

6.9.2.4 A printed list of Unit and ITS Networking contacts responsible for the management and operations of all devices in the MDF/IDFs must be posted in the MDF/IDFs. Information must be kept current and reviewed annually. (contact ITS Networking for new forms).

6.9.3 Cabling / Cable Management

6.9.3.1 Outside Plant Fiber

All installation of Outside Plant (OSP) fiber and assignment of inter-building fiber circuits must be processed through ITS Networking. Only fibers explicitly assigned by ITS Networking may be used.

6.9.3.2 Building Cable Pathways

Media cabling through building pathways shall only be installed or modified by ITS Networking and approved contractors. Contractors must be vetted and approved by ITS Networking, follow university building codes and standards, and adhere to ITS

Networking's inspections. ITS Networking may approve Unit staff to install specialized media with proper training and post-installation inspections.

6.9.3.3 Building Cable Labeling

All cables through building pathways must be labeled at all termination points.

6.9.3.4 Cable Removal

Abandoned cables must be removed per university adoption of National Electrical Code (NEC/ NFPA). ITS Networking will act as the arbiter in any dispute over future reuse of cabling per 4.1.13.

6.9.3.5 Data Closet Patch Cable Management and Labeling

All patch cables in MDF/IDFs must be properly managed using cable management hardware and labeled with the port number to which the cable is connected. In data closets with multiple occupants, it is strongly recommended that each Unit use a unique color cable (and/or label) to distinguish ownership.

6.9.3.6 Patch Cables

Locally constructed patch cables (copper and fiber) are strongly discouraged due to high failure rates.

6.9.3.7 Patch Panel Connector Types

Patch panel connector types must adhere to the standards as established by ITS Networking in construction standards.

6.10 Voice Over IP (VoIP)

ITS Networking provides fee-based communication services to the university in collaboration with Units. Based on Session Initiation Protocol (SIP) standards the system: 6.10.9) replicates the traditional controlled telephone environment with dedicated and certified instruments, and 6.10.10) provides new flexible communication services across the network more familiar in software environments.

6.10.1 ITS Networking will fund all central operations and any distributed support through fees charged to Units. The core SIP system is operated by ITS Networking's Voice group.

6.10.2 Units will fund distributed equipment and support (including: phones, software, end user support, network equipment, cabling, data closet infrastructure).

6.10.3 ITS Networking defines services and establishes and enforces standards, rules, procedures for connecting to the system with IT Governance oversight.

6.10.4 ITS Networking may delegate some provisioning functions to Units to reduce fees and enhance service.

6.10.5 Units must act in good faith to ensure: correct provisioning and records, proper fee allocation for collection, that services are used as intended, and reporting of violations or irregularities to ITS Networking. [voice@its.utexas.edu]

6.10.6 Units and end users must not extend, share or interconnect the SIP communication services with other systems or parties in any manner. Any security violation must be immediately reported to ITS Networking and the ISO. [voice@its.utexas.edu]

6.10.7 Units will be responsible for all costs incurred as a result of end user actions or compromise of portions they manage.

6.10.8 Any Unit operated distributed voice systems require SITAB approval. Pre-existing systems registered with ITS Networking [as of 3/6/2012] are grandfathered at current version/scale until their next upgrade cycle or expansion, when they must convert to the ITS Networking provided system or seek SITAB approval for alternate proposals.

6.10.9 Traditional Telephone Environment

A controlled traditional telephone environment with dedicated and certified instruments has been replicated utilizing SIP/VoIP and analog technologies. It is operated to achieve a high degree of reliability and security for those instruments, along with E911 support.

6.10.9.1 Service Level Agreement (SLA) for Traditional Telephone Environment

Service	Initial Response, Business Hours	Initial Response, After Hours	SLA
Core SIP System	Upon Detection	Upon Detection	99.95%
Ancillary SIP Services **(Provisioning, Voicemail, Conferencing, Personal Agent, Licensing, etc.)**	Upon Detection	Upon Detection	99.9%
End-user telephone instrument **(Unit responsibility)**	Upon notification, 16 Business Hours*	None	99%

*Assuming any cable repair does not require construction or re-pulling.

6.10.9.2 ITS Networking will solely manage and operate analog telephone services.

6.10.9.2.1 Analog service availability will be limited to reduce university costs.

6.10.9.2.2 ITS Networking will evaluate and approve requests for analog service based on IT Governance guidelines. The intent of analog service is to provide extended run-time for code specified life-safety telephones that is not economically achievable using VoIP systems on the university's networks (e.g. elevators and areas of refuge).

6.10.9.2.3 All other analog devices utilizing the service should be converted to VoIP, unless exempted by ITS Networking.

6.10.9.3 Units will conduct all tasks related to VoIP moves, adds, changes and instrument/end user support; adhering to SLAs.

6.10.9.3.1 ITS Networking may provide enhanced fee-for-service offerings to perform distributed duties for Units (envisioned in the "Business Class" offering of the initial VoIP governance proposals). ITS Networking must coordinate any port allocations with the responsible Units.

6.10.9.4 ITS Networking will create and operate segregated voice networks to provide secure and reliable telephone services. Only compliant network equipment managed by ITS Networking may be utilized for voice networks.

6.10.9.5 Only certified telephone instruments may be connected to voice networks.

6.10.9.5.1 ITS Networking manages the software, security and configuration for the certified instruments. ITS may delegate support for certain end user configuration options to Units to reduce fees.

6.10.9.5.2 IT Governance and ITS Networking specify certified telephone instruments. Certified instruments must be purchased from ITS Networking, or registered with ITS Networking for its management via its approved mechanisms. (ITS Networking will maintain adequate supplies)

6.10.9.5.3 ITS Networking is responsible for maintaining NetContacts and assessments for ISORA for certified telephone instruments.

6.10.9.5.4 Uncertified devices found on voice networks may be removed from the network without warning.

6.10.9.6 Units must maintain cable number to switch port mappings in the TSC Networking tools for all certified telephone instruments and comply with 911 safety requirements (all network devices must be mapped per 6.11.1.1).

6.10.10 Other Communication Services

SIP enables services not possible with traditional telephone services such as mobile and software clients, web-mediated interactions, video, presence, etc. Its breadth of services and features creates a less controlled support environment leading to slightly lower service levels and no E911 support. This is an initial framework for responsibilities. Both 6.10.9 and 6.10.10 modalities could be utilized by a user.

6.10.10.1 Service Level Agreement

Service	Initial Response, Business Hours	Initial Response, After Hours	SLA
Core SIP System	Upon Detection	Upon Detection	99.9%
Ancillary SIP Services	Upon Detection	Upon Detection	99.5%
End-user interface **(Unit responsibility)**	TBD by Unit	None	Best Effort

6.10.10.2 Units are responsible for the management, configuration, security, operations and end user support for all non-certified telephone instruments, other devices and software used with the system. Best industry practices must be followed.

6.10.10.3 ITS Networking has certified communications software for some platforms to work with the system. Units should purchase and utilize these offerings to reduce support costs to the university.

6.10.10.4 Units should consult with ITS Networking prior to connecting non-certified instruments/devices or software to the system. [voice@its.utexas.edu]

6.10.10.4.1 ITS Networking may disapprove instruments/devices or software due to impact or risk to the system, or cost of central support. Those must be disconnected.

6.10.10.4.2 ITS Networking is not responsible for compatibility or researching support issues for devices/software it does not certify.

6.10.10.5 Unit must comply with notification and procedures related to 911. [TBD]

6.11 Network Equipment

6.11.1 Equipment Management

6.11.1.1 Units must maintain correct cable number to switch port mappings in the TSC Tools. These mappings should be audited every two years.

6.11.1.2 A description must be provided for all interface/port configurations for uplinks and devices providing major/critical services.

6.11.1.3 All equipment must be labeled with the device name and IP address. In data closets with multiple occupants with independent equipment, the equipment must be uniquely identifiable. Methods include painted brackets or other methods to match the assigned cable color for each Unit.

6.11.1.4 It is recommended to use console servers for out-of-band management of POP devices.

6.11.1.5 Installation of SOHO switches/hubs/routers outside of the MDF/IDF is not permitted or recommended. Unit Network Managers may grant an exception for networks they operate.

6.11.1.6 Emergency power circuits may be unreliable, therefore may only be used for network equipment in these situations:

- Dual power supplied equipment, where one supply is connected to regular power and either can support full operations.
- Single power supplied equipment, where the supply is connected to a UPS, which is connected to the emergency circuit. Note, however, 5.2.3.5 Minimum Network Standards states an automatic transfer switch is required between the UPS and network equipment, connected to regular power and emergency power.
- Single power supplied equipment, where the supply is connected to an automatic power transfer switch (local or building), which is in turn connected to both regular and emergency power. This is not recommended as it may result in brief outages.

6.11.2 Extending Networks

6.11.2.1 Only ITS Networking may interconnect with external networks.

6.11.2.2 Only ITS Networking may physically or logically extend networks beyond a building or between Units.

6.11.2.3 Only ITS Networking may operate routers that interact with access/distribution/core routers.

6.11.2.4 Only ITS Networking and Units may extend networks within Units, for example, through router/switch in offices, or logical tunnels.

6.11.3 Network-based Firewalls

6.11.3.1 All firewalls must be acquired and operated by ITS Networking and must be provided full FCAPS support. ITS Networking will grant exceptions until the next upgrade cycle for existing firewalls, if the exception request is submitted within six months of this manual's adoption.

6.11.3.2 ITS Networking must enable Units to manage, configure, and debug their rule sets.

6.11.3.3 ISO must provide default template recommendations.

6.11.3.4 Firewalls must operate in transparent mode to facilitate monitoring operations.

6.11.3.5 ITS Networking should evaluate performance and security needs with the Unit and ISO to arrive at appropriate recommendations for firewall use. For example, high performance data flows may require hardware-assisted ACLs as opposed to stateful firewalls.

6.11.3.6 Network-based content filtering is not permitted.

6.11.4 Port Configurations

6.11.4.1 Units must not use switches and ports that are not assigned to them without permission from the party responsible for the switch. ITS Networking must clear any patch assignments it makes with Unit.

6.11.4.2 Units must not configure ports to provide access to networks they do not operate, such as FacNet or another Unit's VLAN.

6.11.4.3 Only ITS Networking may configure or authorize access to FacNet ports and VLANs.

6.11.4.4 All unused ports must be assigned to a non-routed, unused VLAN and shut down to prevent unauthorized or unintentional access to the network.

6.11.4.5 All unused VLANs must be pruned from 802.1q ports. All 802.1q ports should be reviewed annually for compliance by ITS Networking (for switch and building uplinks) and Units (for end user trunked/encapsulated ports).

6.11.5 Vendor Software, Licensing and Support

6.11.5.1 Licensing and support contracts must be kept current and maintained according to licensing restrictions.

6.11.5.2 All core and distribution layer devices and systems must be actively supported by the vendor and have active support contracts (as required by vendor licensing) to operate the most recent software versions. For example, all Cisco routers must have active SmartNet contracts.

6.11.5.3 Any equipment determined to be a risk to operations based on software version must be removed from the network.

6.11.5.4 Wireless Access Points (WAPs) must be actively supported by ITS Networking. Units must remove unsupported WAPs and related infrastructure.

6.11.5.5 Any equipment determined to be a risk to operations based on software version must be removed from the network.

6.11.5.6 ITS Networking must maintain support contracts for items listed in section 6.10.5.2 and bill Units for the contracts. ITS Networking will notify Units of costs annually by February for planning in the next fiscal year.

6.11.6 Spares

6.11.6.1 For items on the approved equipment list (forthcoming), ITS Networking must maintain spare equipment of equivalent function to ensure fast return to service.

6.11.6.2 Unit must fund the purchase of a spare if it is deployed and remains at Unit.

6.11.6.3 Unit must fund the purchase of a spare if a deployed device is not on the approved equipment list and equivalent functionality is not available within the spares set.

6.12 Maintenance

6.12.1 Units should not conduct other IT related maintenance during scheduled campus-wide network maintenance events. See AIC IT Maintenance Blackout Operations Procedure.

6.12.2 ITS Networking will publish non-emergency blackout dates three months in advance.

6.13 Planning and Lifecycle

6.13.1 ITS Networking shall operate and maintain systems to provide Unit visibility into trending issues related to:

- Faults/Failure rates.
- Traffic utilization and growth rate expectations for wired and wireless networks.
- Other load-related issues, such as client load on the wireless network.

6.13.2 Life Cycle Management

6.13.2.1 ITS Networking shall maintain and provide lifecycle information on the equipment that it manages for Units. Reports for the following fiscal year will be provided by February 1 and will include:

- Current age of hardware by line item.
- Projected replacement date (year) by line item.
- Projected replacement cost by line item. Projected cost will be a best effort because of expected changes in models and associated costs.

6.13.2.2 Units shall consult with ITS Networking and budget for lifecycle replacements.

6.13.2.3 ITS Networking will maintain and provide lifecycle information on core network hardware and other centrally funded assets and make this information available annually to ITS management, IT Governance, and upon request to appropriate parties.

6.13.3 Building Infrastructure Assessment

ITS Networking will provide and maintain a system to assist Units in identifying networking needs for buildings. This “building report card” will be calculated and derived from multiple factors, including but not limited to:

- Building square footage and corresponding port and WAP density
- Age of infrastructure (derived from lifecycle data)
- Adherence to minimum network standards listed in section 5
- Utilization of existing infrastructure (available vs. consumed bandwidth, client loads on wireless)
- Physical facilities in data closets (HVAC, electrical capacity, overall suitability of environment)

7. Exceptions/Adjudications

7.1 Exceptions to these standards and operations may be granted by ITS Networking and Units based on delegation of responsibilities. Considerations include:

7.1.1 The underlying need for exception is closely aligned with the university's mission.

7.1.2 Exception is in alignment with the overall goals of this manual.

7.1.3 Exception does not conflict with rules, laws, or policies.

7.1.4 Exception does not compromise the integrity of the network or the ability to manage network resources. Specifically, it may not impact network stability, supportability, and maintainability.

7.1.5 Extraordinary costs (ordinary costs will not be considered).

7.1.6 Requestor assumes all responsibilities incurred if granted the exception.

7.2 When adjudicating disputes, additional considerations include consideration for fairness, consistency, and funding (who paid).

7.3 Exceptions must still comply with other requirements outlined in this document.

7.4 Unless specified, exceptions will be reviewed annually.

7.5 Exceptions will be recorded and maintained by the authorizing party.

7.6 Unit head approval may be required for exceptions.

8. Review and Updates

8.1 This manual will be updated as needed and reviewed at least every two years.

8.2 Minor updates will be ratified by the AIC.

8.3 Major modifications will be ratified through AIC to OIT, and possibly SITAB, depending on scope and impact.

8.4 Change logs will be maintained.

9. Glossary of Terms

802.11
IEEE standard set related to wireless (WiFi, WLAN) (a/ac/b/g/n) networking.

802.1d
IEEE standard which defines Spanning Tree Protocol behavior (used to prevent network loops).

802.1x
IEEE standard which provides for port based network authentication for users attempting to connect to a network.

AIC
Information Technology Architecture and Infrastructure Committee at the University of Texas at Austin.

ACL
Access Control List (a means of controlling access to on networks).

ANSI
American National Standards Institute. A private organization that oversees the development of voluntary consensus standards across a wide array of industries in the United States.

BACS
Building Access Control System at the University of Texas at Austin. A centrally managed and monitored system that uses card swipe/proximity card readers to allow/deny/audit individual access to external building doors and internally secured areas.

BICSI
Building Industry Consulting Service International. Organization responsible for developing design standards for building structured cabling systems.

Building Size
The building size classification is determined based on the number of unique devices seen connected to the building network over a determined length of time. The count will include both wired and wireless users (average peak).

- A “medium” size building hosts 350-600 devices.
- A “large” size building hosts over 600 devices.

Cat 5/5e/6a
Structured cabling standard which defines the physical design of a cable. Speed and capability usually increase with the higher the category number.

Core
A layer of the campus network, typically central, that other buildings/devices rely upon. Also see Distribution and Edge.

DHCP
Dynamic Host Configuration Protocol. A protocol for actively distributing network addresses to hosts configured to request them.

Distribution
A layer of the campus network, typically located in building MDFs. Provides layer 3 and other network services. Distribution networks serve as the communication path between the Edge and Core resources and are usually located in the building MDF. Also see Core and Edge.

DNS
Domain Name Services. System for resolving named network resources to actual numeric IP address.

EIA
Electronic Industries Alliance. Organization accredited by ANSI to help develop standards related to electronic components, consumer electronic products, telecommunications and internet security.

Edge
(Also known as Access) A layer of the campus network, typically where end devices obtain network access in buildings; for example, a switch or wireless access point. Also see Distribution and Core.

FacNet
Facilities Network. Operated by ITS Networking, access is restricted.

FCAPS
Term used to describe the overall functionality of an enterprise network management system. It represents (F)ault Management, (C)onfiguration Management, (A)ccounting Management, (P)erformance Management, and (S)ecurity Management.

IDF
Intermediate Distribution Facility. Typically a communications closet which houses customer network access equipment (Edge).

IEEE
Institute of Electrical and Electronics Engineers. Responsible for defining key networking standards.

IPv4
Internet Protocol version 4. Connectionless protocol that operates as a best effort delivery model, used worldwide for network routing purposes – the Internet. Also see IPv6.

IPv6
Internet Protocol version 6. Successor to IPv4.

IRUSP
Information Resource and Use Policy for The University of Texas at Austin.

ISO
Information Security Office at The University of Texas at Austin. The UT entity that monitors and addresses a wide variety of information security issues.

ISP
Internet Service Provider.

ITS
Information Technology Services.

LAN
Local Area Network.

MAC
Media Access Control. Layer 2 addressing mechanism which provides for a unique 48 bit identifier for each device connected to a network.

MDF
Main Distribution Facility. Typically a communications closet which houses entire building network access equipment which connects back to the Core. Also see Distribution.

MMF
Multi-Mode Fiber. Fiber optic cable type typically used for in-building (short range) applications.

Network Equipment
Any device involved in transport of data across the network, such as switches, routers, firewalls, load balancers, VPNs, WAPs. While a computer is typically an origination and termination point for data, it can become network equipment if software is run to convert it to equipment that data passes through, such as a proxy, cache, or tunneling server. A computer configured to transport data must comply with all requirements (including those about monitoring, acquisition, and FCAPs).

NEC/NFPA
National Electrical Code, National Fire Protection Association

NIC
Network Interface Card. A physical card/connector typically located in a host which provides network connectivity to the device.

NTP
Network Time Protocol. A protocol used to synchronize clocking over networks, particularly networks subject to jitter/latency.

POP
Point of Presence. Typically the point where an Internet Service Provider interconnects with local facilities. At UT, the gateway/router device connecting a building network to the campus network.

Port
Typically refers to the physical connection on a network switch. May also refer to a logical port accessed by network applications and controlled by a virtual or physical firewall.

PNA
Public Network Authentication at The University of Texas at Austin. Methodology used to control access to the campus networks.

Resnet
Set of networks dedicated to the students occupying the campus residence halls.

RJ-45
Network cable connector standard that defines an 8-pin male/female connector/jack, used in network switch connectors, patch panels, wall jacks, and NIC cards.

SIP
Session Initiation Protocol refers to a collection of IETF standards for establishing communication sessions (voice, video, text, other) utilizing Internet Protocol across the network.

SITAB
Strategic Information Technology Advisory Board at The University of Texas at Austin.

SLA
Service Level Agreement. A minimum service level, typically an availability metric, that a service provider guarantees to a customer. In the context of this manual, it is reporting availability for factors under direct control of those parties (e.g. for networking, general assumptions are made that the facility, media and pathways, power and cooling, are available – more information is available in their SLA documents).

SMF
Single-mode fiber. Fiber optic cable typically used for inter-building or inter-site (long range) applications.

STP
Spanning Tree Protocol. Protocol that operates at Layer 2 and is designed to prevent bridge loops in a network. Also see 802.1d.

TIA
Telecommunications Industry Association. Global trade association responsible for defining networking standards related to voice/video/data cabling.

Tools
Generic term that refers to the collection of network management and monitoring tools used by ITS Networking and the TSC community to monitor and manage network resources assigned to them.

TOR
Originally derived from The Onion Routing Project, is also commonly referred to as Tor. This is a system that attempts to provide total anonymity for a network user by obfuscating user identity, location, and routing information.

TSC
Technical Support Coordinator. Typically a member of a Unit who is assigned the duties of managing Unit network resources and working with ITS Networking to resolve any issues.

UPS
Uninterruptable Power Supply.

VoIP
Voice over Internet Protocol. Usually associated with network based telephone services.

VLAN
Virtual Local Area Network. A virtual network that allows hosts to operate as if they are connected to the same physical network even though they may be located on different physical segments of a network.

VPN
Virtual Private Network. A communications model that allows for the encapsulation of data across a public network to provide remote users or sites with secure access to their organization's main network.

WAP
Wireless Access Point. May also be referred to as an AP. Contain the radio(s) that connects the wireless clients (computers) back to the network via either a physical network cable or another wireless access point (Mesh configuration).

WiFi
Generic term to describe wireless networks as defined by the IEEE 802.11 standards set.

WLAN
Wireless Local Area Network (Also see 802.11a/ac/b/g/n).

10. Document Conventions

The Construction symbol  identifies requirements for new construction or space renovations.

"Shall" indicates a future requirement. These are items that may not be completed in the near-term. It is expected that they will be completed as soon as technology/ resource/ budget can be allocated. There should be a plan and intent to accomplish the task.

"Will" and "Must" indicate required items.

"Should" indicates a recommendation.

11. Revision History

Version	Date	New	Original
NetOpsMan v1-2.pdf	April 12, 2013	Numerous changes, the major ones: 5.2.2 Wireless and related sections: changes to ubiquitous coverage and increase in response stance. 5.6 Lifecycle –distribution 7 years 6.5.1 Network Access Clarifying requirements. Discouraging sponsored non-university use. 6.10 Voice Over IP	 Unit determined coverage level. 5 years None
NetOpsMan v1.pdf	June 15, 2011	5.6 Network Lifecycle: criteria for replacement clarified	Typical lifecycle could be interpreted as literal requirement.
NetOps Man Mv16 4-22-2011.pdf	April 22, 2011	Submitted for SITAB appproval	
NetOps Man Mv15 2-15-2011.pdf	February 15, 2011	Submitted for OIT approval	
NetOps Man Mv14 2-8-2011.pdf	February 8, 2011	Submitted for AIC endorsement	
NetOps Man Mv7 12-7-2010.pdf	December 23, 2010	Submitted for campus community review	

12. Approvals

Name	Role	Members	Date
AIC Subcommittee	Authoring	Charles Soto, College of Communications Gabriel Hernandez, Department of Electrical and Computer Engineering Ryan Baldwin, College of Education Chris Carter, General Libraries Cam Beasley, Information Security Office Ty Lehman, Jackson School of Geosciences James Lewis, College of Liberal Arts Ryan Moore, ITS Edge Networking William Green, ITS Networking and Telecommunications (chair)	April 5, 2012
IT Architecture and Infrastructure Committee	Approval	See governance	April 12, 2012

Name	Role	Members	Date
Operational IT Committee	Approval	Alex Albright, School of Law Brad Englert, Chief Information Officer Fred Friedrich, Business Services Committee Bryan Harold, College of Natural Sciences Mike Harvey, IT Architecture & Infrastructure Committee Fred Heath, University of Texas Libraries John McCall, Associate Vice President for Development Emily McTavish, Graduate student representative Kevin Ramos, Undergraduate student representative Clark Penrod, Applied Research Laboratories Chris Plonsky, Athletics Director Soncia Reagins-Lilly, Senior Associate Vice President and Dean of Students Charles Roeckle, Deputy to the President Dan Slesnick, Representative, Provost's Office Dan Stanzione, Research & Educational Technology Committee	April 27, 2011

Name	Role	Members	Date
Strategic IT Accountability Board	Approval	Alex Albright Chair, Operational IT Committee Jay Boisseau Director, Texas Advanced Computing Center Pat Clubb Vice President for University Operations Andrew Dillon Dean, School of Information Greg Fenves Dean, Cockrell School of Engineering Rod Hart Dean, College of Communication Kevin Hegarty Vice President and Chief Financial Officer Steve Leslie Executive Vice President and Provost David Neubert Chairman, Faculty Council IT Committee William Powers, Jr. President, Committee Chair Brad Englert Chief Information Officer (ex-officio)	June 15, 2011