



Network & Information Security Policy

Policy Version: 2.1

Approved: 02/20/2015

Effective: 03/02/2015

Table of Contents

I.	Purpose.	1
II.	Scope.	1
III.	Roles and Responsibilities	1
IV.	Risk Assessment	2
V.	Information Security Policy	3
VI.	Physical Security Policy	4
VII.	Information Systems Acquisition	4
VIII.	Information Security Incident Management	5
IX.	Business Continuity Management	5
X.	Compliance	6
XI.	Terms and Definitions.	7

I. Purpose

Utah Telehealth Network (UTN) connects unrelated health care facilities to improve access to health care services and resources through the innovative use of technology. It supports telehealth, the exchange of protected health information, and collaboration among unrelated organizations. The network is at risk from potential threats such as human error, accident, system failures, natural disasters, and criminal or malicious action.

The purpose of this policy is to secure the network to protect sensitive information and systems which may traverse or reside on the network.

II. Scope

This policy is applicable to all users and organizations that use UTN. It is limited to security policies; UTN procedures and recommendations for best practices can be found elsewhere.

III. Roles and Responsibilities

Information security is the preservation of confidentiality, integrity and availability of information. It is a shared responsibility between UTN, member organizations, and users. Together, we must take measures to protect private sensitive information. This section defines general areas of responsibility for information security.

A. Responsibilities of UTN

UTN secures network connections to all members. UTN's roles and responsibilities include, but are not limited to, the following:

1. Develop and maintain security policy, plans, procedures, strategies, architectures, best practices, and minimum requirements in cooperation with UTN members
2. Maintain all UTN network equipment up to the firewall or network switch
3. Monitor, log, and analyze network traffic information to ensure compliance with UTN security policies, and evaluate, identify, and resolve security vulnerabilities, breaches and threats to UTN resources
4. Inform the appropriate parties of traffic patterns or other anomalies which may indicate a problem
5. Apply security policy and procedures to UTN network devices
6. Conduct security audits as scheduled or requested
7. Run periodic vulnerability scans on each member's LAN to proactively identify potential attack trajectories and communicate results to member.
8. Direct the incident response activities as far as they relate to resolving security vulnerabilities, breaches and threats to UTN resources.
9. Assist auditors in the analysis of UTN resources to ensure policy compliance.

10. Build VPNs between member sites or third parties upon written request of the member site's senior management and the UTN network staff.
11. Prepare disaster recovery plans and procedures for UTN network connections and equipment.

B. Responsibilities of UTN members and other users of UTN resources

The member is responsible for all activities within its environment and past the UTN demarcation point. Its security roles and responsibilities as they relate to UTN include, but are not limited to, the following:

1. Understand UTN network and information security policy, and conduct activities accordingly.
2. Manage its own infrastructure, such as wireless networks, servers, applications or any system with PHI and IT security, up to the UTN demarcation point
3. Resolve security issues on their endpoint devices
4. Secure the data that is shared with other organizations
5. Prepare and implement its own IT security policy, business continuity, and disaster recovery plans in the event of a network outage
6. Train personnel on how to contact UTN during an outage.

IV. Risk Assessment

UTN conducts risk assessments for every system on its network periodically and/or upon request.

A. Proactive Vulnerability Detection

UTN runs vulnerability scans on UTN's and members' networks to proactively identify security weaknesses.

1. UTN reserves the right to run vulnerability scans on any IP address in the network at any time.
2. Vulnerability Remediation
 - a. Members by accepting this policy understand that vulnerabilities not mitigated in a timely fashion can pose a serious threat to member networks and the Univ. of Utah hospital. Therefore, sanctions up to or including denial of service to and from a specific device or network can be implemented in order to preserve the integrity of the network. UTN must notify the site of the denial of service. A UTN Vulnerability Compliance Procedure detailing the sanctions, process, timeline, and notifications will be followed.
 - b. The exception to denial of service is when the device is directly related to patient care. In this scenario, approval to deny is required from UTN management.
2. Service Degradation and/or Interruption.

- a. Network performance and/or availability may be affected by the vulnerability scanning. The member releases UTN of any and all liability for damages or missed Service Level Agreements caused by the network scanning, unless such damages are the result UTN's gross negligence.

V. Information Security Policy

This section provides rules for use of all UTN resources.

A. Acceptable Use

1. The resources of UTN are intended to support the missions of UTN and its members. Any unauthorized use that deviates from the missions, jeopardizes data, breaks the law or violates the security policy is considered unacceptable. It is therefore expected that users will conduct themselves in a responsible and ethical manner, adhere to the high standards of professional conduct, and abide by all local, state and federal laws.

B. Security and Proprietary Information

1. All electronic protected health information records that travel over UTN must be encrypted.
2. Data exchanges between members and third parties must be encrypted.
3. Requests to open access must contain the IP address of the vendor, the specific firewall ports to open, a list of IP addresses the vendor may access, and the written permission from the member's senior management (i.e. CEO or CFO) and approval of UTN.
4. All members are required to have an UTN approved and managed firewall in line.
5. Access rights to all network devices under UTN's direct control will be restricted to only those with approved permission.
6. Proprietary Information – All documentation regarding UTN, member networks, and third party networks is strictly confidential. Access to diagrams, maps, spreadsheets, databases, and other network information repositories should be kept on a secure drive location only accessible to those who have a business need to know.

C. Remote Access

UTN provides remote access to its network for business purposes with proper authorization.

1. All PHI and applications to be accessed remotely must be accessed through an UTN-approved VPN gateway.
2. Only UTN-approved remote access applications are permitted. UTN will block unapproved VPNs, applications, or unacceptable uses of the network.
3. Remote access is limited to authorized users for acceptable and necessary use only.

4. Remote access will only be granted after providing all information, forms, and proper authorization.

D. Access Control

Access to UTN-managed equipment is limited to those personnel with a business need to access such equipment.

1. Unauthorized access to equipment that is managed by UTN is strictly prohibited.
2. UTN may grant read-only permission to equipment that UTN manages to authorized personnel.
3. Passwords may not be shared.
4. All authorized users must use strong, encrypted passwords that automatically close connections if left unattended.
5. Access privileges must be revoked upon termination of anyone with access to UTN's environment. It is the responsibility of the member to notify UTN of the termination.

VI. Physical Security Policy

This section outlines requirements and responsibilities for the physical security of UTN equipment.

A. Secure Areas

1. The UTN member should keep UTN network equipment in a locked area with environmental controls, and a record of any physical access to the equipment.
2. Locked rooms or cabinets should be accessible only by those personnel with a business need to enter.

B. Equipment Security and Placement

1. Critical IT equipment and cabling must be protected against physical damage, fire, flood, theft, etc., both on- and off-site as appropriate. This includes placing equipment with a minimum distance to walls, doors, AC, and other electrical cabling as prescribed by building code.

C. Responsibility

1. UTN is not responsible for theft or destruction of its equipment located at a member facility.
2. The member is responsible for replacing the equipment in the event of destruction or loss.

VII. Information Systems Acquisition

New information systems or network security systems, such as VPNs, that interact with, or traverse, UTN or require the support of UTN require a security review by UTN.

A. Security requirements of network security systems

1. Devices must have UTN network engineer approval prior to implementation.
2. Devices that interact with the University of Utah must be evaluated and approved by the University of Utah network staff.
3. All new systems are required to be put through a risk assessment prior to implementation.

B. Implementation lead time

1. For systems to be supported by UTN, at least 30 days of lead time is required in order to evaluate and implement any new systems.
2. Exceptions may be made for emergencies, but requestors must understand that the process itself may take at least 30 days.

VIII. Information Security Incident Management

This section describes the response to information security incidents.

- A. All security events and risks must be reported to UTN.
- B. UTN is required to document and report security incidents and their remediations to affected parties. UTN may initiate or participate in security investigations.
- C. All machines involved in a security incident will undergo a risk assessment

IX. Business Continuity Management

This section addresses policies in the event that network operations fail and security of the network is compromised.

A. Written plan

1. UTN and members site must have a written plan in place for Business Continuity.

B. Communication

1. The member must provide UTN with a list of contacts for handling network outages.
2. UTN or the member will attempt to communicate with the appropriate parties when there is an incident.

C. Disaster Recovery Policy

In the event of a catastrophic outage or compromise, UTN will restore service according to the following priorities:

1. Network and security equipment at the UTN core
2. Network and security equipment for members that access patient care over the UTN
3. Network and security equipment for members that depend on UTN for other services
4. Videoconferencing bridge
5. Videoconferencing equipment

X. Compliance

- A. All violations of UTN Information Security Policies will be reported to UTN management and the member site's senior management.
- B. If a member becomes a threat to other UTN users, UTN reserves the right to restrict network access to an individual device or, if necessary, a member site until the incident is resolved.
- C. Requests for exceptions to the UTN policy must be made in writing and include the signature of the member's senior management (i.e. the CEO or CFO).

XI. Terms and Definitions

- A. Acceptable use – Anything that supports the missions of UTN and its members.
- B. Disaster Recovery Plan - A written plan including provisions for implementing and running critical information technology resources at an alternate site or provisions for equivalent alternate processing (possibly manual) in the event of a disaster.
- C. Information Security – preservation of confidentiality, integrity and availability of information
- D. Local Area Network (LAN) – Anything that is within the control of the UTN member and beyond UTN’s management
- E. Member - A health care organization that receives services from UTN
- F. Member site - A specific site within the UTN
- G. Network Security System – Any network device, such as a firewall or VPN, that deals with protecting information resources
- H. Patient Health Information (PHI) – Data that contains confidential patient and billing records
- I. Remote Access - Any access to a member's LAN when not physically located on the LAN
- J. Security - Measures taken to reduce the risk of 1) unauthorized access to IT Resources, via either logical, physical, managerial, or social engineering means; and 2) damage to or loss of IT Resources through any type of disaster, including cases where a violation of security or a disaster occurs despite preventive measures.
- K. Security Incident – The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with systems operation in an information system.
- L. Spam - Unauthorized and/or unsolicited electronic mass mailings.
- M. Strong Encryption - An algorithm that is public and approved by ASTA standards.
- N. Unacceptable use – Anything that breaches the confidentiality, integrity, or performance of an information resource or is not consistent with the mission of UTN or its members.
- O. UTN demarcation point – the last point of equipment that UTN manages before handing off to the UTN member
- P. UTN user – anyone who operates on a network inside UTN or traverses through the UTN WAN.
- Q. VPN - A virtual private network protects the transport of data. It does **not** protect source and destination from each other.
- R. Vulnerability Scan - An intensive security scan that looks for security problems. It may scan one or all machines in a network.
- S. Wide Area Network (WAN) – Geographically dispersed telecommunications network.