Network Connection Policy

Category: Operations; Students and Teaching

Approval: September 12, 2016

Responsibility: AVP-Information Technology

Date: October 11, 2016

Definitions:

"User(s)" are defined as operators of computing devices. Every computing device connected to the network has an associated owner (e.g. a student who has a personal computer) or caretaker (e.g. a staff member who has a computer in her office). For the sake of this policy, owners and caretakers are both referred to as Users.

"Computing Devices" or simply "Devices" is a term inclusive of any technology that connects to our network (whether personally owned or owned by the university), including, but not limited to, desktop computers, laptops, servers, wireless computers, mobile devices, smartphones, specialized equipment, cameras, environmental control systems, wearable devices and telephone system components.

"Appropriate Connectivity Points" is defined as the methods by which a user, through their device(s), can connect to the network. For the purposes of this policy, this includes Trent voice/data jacks, Trent's wireless network access points (Eduroam and ResNet), or via remote access technologies (e.g. VPN or SSH tunnel as approved by the IT department).

Purpose/Reason for Policy:

This policy is designed to protect the campus network and the ability of members of the Trent community to use it. The purpose of this policy is to define the standards for connecting computing devices to the University's network. The standards are designed to minimize the potential exposure to Trent University and our community from damages (including financial, loss of work, and loss of data) that could result from computing devices that are not configured or maintained properly and to ensure that computing devices or users on the network are not taking actions that could adversely affect network performance.

Trent University must provide a secure network for our educational, research, instructional and administrative needs and services. An unsecured computing device on the network could allow denial of service attacks, viruses, Trojans, and other compromises to enter the university's campus network, thereby affecting many computing devices, as well as the network's integrity. Damages from these exploits could include the loss of sensitive and confidential data, interruption of network services and damage to critical Trent University internal systems.

Universities that have experienced severe compromises have also experienced damage to their public image. Therefore, individuals who connect computing devices to the Trent network must follow specific standards and take specific actions as required by this policy.

Scope of this Policy:

This policy applies to all members of the Trent University community or visitors who have any computing devices connected to the Trent University network. The policy also applies to users who have computing devices outside the campus network that remotely access the campus network and resources. The policy applies to university-owned computing devices (including those purchased with grant funds), and personally owned or leased computing devices that connect to the Trent network. The policy does not apply to devices connected solely to university resources that are publicly available through the World Wide Web.

Policy Statement:

Appropriate Connection Methods

Users may connect devices to the campus network at appropriate connectivity points.

Modifications or extensions to the network can cause undesired effects, including loss of connectivity. These effects are not always immediate, nor are they always located at the site of modifications. Therefore, extending or modifying the Trent network (e.g. through the addition of switching equipment or routers) must only be done by, or with the guidance of, the IT department.

Network Registration

Users of the university network may be required to register a device before connecting it. Users may also be required to install a software agent on their device before they are allowed on the network. The role of such an agent would be to ensure that the device complies with current standards.

Responsibility for Security

Users are responsible for ensuring that their computing devices meet all relevant security standards (see below) and for managing the security of the equipment and the services that run on it. Some departments may assign the responsibility for computer security and maintenance to dedicated departmental staff. Therefore, it is possible that one user manages multiple departmental devices plus his or her own computing devices. Every user should know who is responsible for maintaining his or her computing device(s).

Security Standards

Users must ensure that all computing devices capable of running anti-virus/anti-malware software have licensed anti-virus software (or other appropriate virus protection products) installed and running. Owners should update definition files at least once per week. See Information Technology's Service Catalogue for more information.

Users must install the most recent security patches on the system as soon as practical or as directed by Information Technology. Where computing devices cannot be patched, other actions may need to be taken to secure the computing devices appropriately.

Users must ensure that they have password, pin code, or biometric access enabled on their devices. Additionally, users who regularly handle research data or sensitive data such as student biographic and registration information must encrypt their devices. See Information Technology's Service Catalogue for more information.

Centrally-Provided Network-Based Services

Information Technology is responsible for providing reliable network services for the entire university community. As such, users or departments may not run any service which disrupts or interferes with IT-provided services. These services include, but are not limited to, email, DNS, DHCP, and Domain Registration. Exceptions may be made by Information Technology for approved personnel in departments who can demonstrate competence with managing such services. Also, users or departments may not run any service or server which requests TrentNet credentials.

Protection of the Network

Information Technology uses multiple methods to protect the Trent network, including:

- monitoring for external intrusion
- scanning hosts on the network for suspicious anomalies
- blocking harmful traffic, both inbound and outbound

Traffic of computing devices connected to our network may be scanned for signs of compromise.

Information Technology routinely scans the Trent network, looking for vulnerabilities. At times, more extensive scans may be necessary to detect and confirm the existence of vulnerabilities. Computing devices connected to our network may be scanned for possible vulnerabilities.

Information Technology reserves the right to take necessary steps to contain security exposures to the University. Information Technology will take action to contain devices that exhibit the behaviours indicated below, and allow normal traffic and central services to resume**:**

- imposing an exceptional load on a campus service
- exhibiting a pattern of network traffic that disrupts centrally provided services
- exhibiting a pattern of malicious network traffic associated with scanning or attacking others
- exhibiting behaviour consistent with a host compromise

While the above list is not exhaustive, it is comprehensive. Information Technology reserves the right to take the necessary steps to contain security exposures to the University for any other reason.

Information Technology reserves the right to restrict certain types of traffic coming into and across the Trent network. Information Technology restricts traffic that is known to cause damage to the network or hosts on it. Information Technology may also control other types of traffic that consume too much network capacity, such as file-sharing traffic.

Computing devices exhibiting any of the behaviours listed above are in violation of this policy and will be removed from the network until they meet compliancy standards.

Contact Officer:

Tariq Al-Idrissi, Associate Vice-President-IT

Date for Next Review:

Sept. 12, 2018

Related Policies, Procedures and Guidelines

- Computing Resources Acceptable Use Policy
- User Electronic Information Access Policy
- Computing Privileges Policy

Policies Superseded by this Policy:

- Guidelines for Use of Information Technology