# Device Management Policy

**Document Number:** ITS-0010 **Date Published(sys):** 7/8/2021

## General Description

### Purpose:

It is important that the personal and Trinity-owned devices that connect to the TUNetwork are maintained appropriately in order to protect Trinity IT resources. As a service to the University Community, Trinity provides services related to these devices. The Device Management Policy provides guidelines for the responsibilities of the University and the device users.

### Scope:

The Device Management Policy applies to all users of the TUNetwork. Use of the TUNetwork constitutes the user's acceptance of this policy.

## Policy Content

### Resident Computer Consultants

Resident Computer Consultants (RCCs) are students hired by Information Technology

Services to assist students with their network configuration and connection to the TUNetwork. A student with connectivity issues may contact the ITS HelpDesk x7409 or helpdesk@trinity.edu to receive assistance from an RCC. The following guidelines are provided for students administering and receiving computer and TUNetwork related services.

RCCs are required to:

- Conduct themselves in a professional manner when servicing student machines.
- Respect and protect the privacy of student data.
- Present, discuss, and have student sign a TUNetwork Service Invoice.
- Contact student through Trinity email when service has been completed.
- Avoid conflicts of interest with the University, e.g., by offering competing services to the students.

Students receiving computer assistance will:

- Pick up their computer within one class day of being notified that the service has been completed.
- Stay with the RCC in the residence hall room until the tasks are completed – leaving the RCC alone to service a computer will terminate the service in progress, requiring the student to seek assistance at a later date.
- Provide a smoke free working environment in the residence hall room without obstacles in and around the work area.

Services are governed by the Student Computing Service Center. Please note that hardware removal or installation is not supported.

## Reinstalling Operating Systems

May be necessary if damage to the existing operating system occurs through virus infection, intrusion by a hacker, or spyware related programs, to name a few. A student may either have a Residential Computer Consultant (RCC) or Information Technology Services (ITS) technician reinstall the operating system for the fee listed above, or may choose to reinstall the operating system him or herself. Whether an RCC or ITS technician reinstalls the operating system or the student reinstalls the operating system, the student is responsible for backing up the data he or she wishes to keep. RCCs will not be responsible for backing up data. If a student chooses to have his or her operating system reinstalled by an RCC or ITS technician, the software and license must be legitimately owned by the student or licensed through the university.

RCCs or ITS technicians who reinstall an operating system will ensure that drivers to any hardware that was determined to be compatible with the software are installed and functioning correctly. RCC or ITS technician will also ensure that Symantec Anti-Virus software is installed and configured appropriately on the Windows/Mac machine before the project will be considered completed. Only with reinstallations of operating systems performed by an RCC or ITS technician will a student not be charged for the installation of Symantec Anti-Virus software.

## Software installation

Refers to antivirus, Microsoft, or Mac software that is legitimately licensed to the student or licensed through Trinity University for student use. Examples include Microsoft Office products, BitDefender. Trinity University technicians or RCCs will not install other types of software such as games, AIM, or BitTorrent clients.

## Virus, spyware, and adware removal

Is required when malicious code and spyware is present in computers which can dramatically affect a computer's performance and compromise TUNetwork security. Such code includes viruses, worms, and spyware. For more, please read our Computer Security guide.

While some malicious code can be removed without also installing software, the removal of spyware will require software to be installed on the computer in question and configured properly for effective cleaning. Trinity cannot guarantee a student's machine will function normally after the computer has been cleaned and cannot be held liable for the loss of intellectual data or integrity of the computer's operating system. If the computer is experiencing residual effects after the malicious code has been removed, the computer's operating system may have to be reinstalled. If the student's operating system is functioning abnormally, the student will be encouraged to reinstall it or have an RCC or ITS technician reinstall it.

RCCs will attempt to resolve software related issues. However, depending on the degree of damage sustained to a computer's operating system by malicious code or a file corruption, there may be residual effects that inhibit application features or reduce system performance. RCCs and Trinity University cannot be held liable either for virus infections or how the operating system responds to the removal. Additionally, based on a student's Internet surfing and computing habits, there may be a propensity for the issues that have been resolved to re-occur. If an RCC has to remove a virus or spyware problem again, the situation will be treated as a separate work order with the appropriate fees charged to the student.

## Port deactivation and reactivation

Can occur for, but is not limited to, a violation of the Technology and Information Responsible Use policy. One of the main reasons that a port may be disabled would be if the Information Technology Services Department determines that a student's PC is infected with malicious code. The port to that machine will be turned off until that machine has been cleaned. The computer can be cleaned by an RCC, a technician from the University's ITS department, or by an outside source. If someone other than Trinity personnel cleaned the system, that computer must be inspected by a Trinity representative prior to accessing or connecting it to the TUNetwork. Port deactivation may also occur for violations of copyright as in the illegal downloading of music, games, movies and other such media.

## University-Provided Software

Trinity University provides all students with the software and instructions necessary to perform an installation of supported and university provided software. These materials can be found at the Circulation Desk located on the third floor, main entrance level, of the Elizabeth Huth Coates Library. Before installing such software, the person conducting the installation should:

- Verify that the computer meets the minimum hardware criteria.
- Select "Check System Compatibility" from the Welcome to Windows installation window.

- Instructions for checking system compatibility are included in the "Installing Windows –New Installation and Upgrading to Windows" instruction packets that can be acquired from the Circulation Desk located on the third level of Elizabeth Huth Coates Library.
- Assure that drivers for hardware devices are available for the Windows version being installed.
- In some cases, hardware drivers for specific devices will not be available for Windows or will be available only on the hardware manufacturer's Internet site.
- Similarly, the above applies to university provided software for the MacOS platform.

## University-Owned Devices

Security vulnerabilities are inherent in computing systems and applications. These flaws allow the development and propagation of malicious software which can disrupt normal business operations in addition to placing university data at risk. In order to effectively mitigate this risk, software "patches" are regularly made available to remove a given security vulnerability.

Given the large number of computer workstations and servers that comprise the TUNetwork, it is necessary to utilize a comprehensive patch management solution that can effectively distribute security patches automatically when they are made available. The patch management solution has the ability to evaluate individual computer workstations and servers for vulnerabilities. Patches may then be automatically installed and, when necessary, the affected machine rebooted.

Effective security is a team effort involving the participation and support of every Trinity University employee and affiliate who is a user of the TUNetwork. The "patches" involve software that may be applied to all equipment that is owned or leased by Trinity University such as all electronic devices, servers, application software, computers, peripherals, routers, and switches.

In the event that a critical or security patch cannot be centrally deployed by ITS, it must be installed in a timely manner using the best resources available. In the case of non- Microsoft desktop operating systems where a centralized deployment is not available, then installation should occur in a timely manner by a member of the ITS staff or the end user.

Failure to properly configure new workstations is a violation of this policy. Disabling, circumventing or tampering with patch management protections and/or software constitutes a violation of policy.

## Employee Cellphones

Employees may be given the opportunity to purchase a cell phone through a Trinity University account or with Trinity University funds. Cell phones purchased with a Trinity Account should be approved by ITS prior to purchase. ITS will be unable to support unapproved cell phones. (Any cell phone, including Android, Blackberry, and iPhone, supported by AT&T will likely be supported by ITS.)

The following guidelines outline the employee cellphone purchase process:

- AT&T Wireless (formerly Cingular) is the current provider for cellular services for Trinity University. Cell phones that are currently operating under a different service provider should be migrated to AT&T once the current contract expires.
- Cell phone rate and data plans should be coordinated with ITS.
- Each purchasing unit will be responsible for the payment of each cell phone belonging to their department, including change of plans and porting fees.
- For lost or stolen cell phones, the end user is responsible for notifying the department head and ITS. The end user is responsible for filing a lost or stolen property report with Trinity University campus safety.
- Purchases with University Funds must go through ITS.

The following guidelines detail how to switch from a current provider:

- Contact the Director of the Technology Operations Center in ITS (x7414). The following information will be required:
  - cell phone number
  - current provider
  - cell phone account number
  - expiration date of current contract
  - name on current account
  - current voice and data rate plan
  - new cell phone model selected from: http://www.att.com/shop/wireless.html
  - department account number to which the new service plan and equipment will be charged.

Cell phones and cell phone equipment purchased through Trinity University accounts or with Trinity University funds that have been replaced and or are no longer in use should be sent to Trinity Information Technology Services (ITS) for proper disposal. Before cell phones are turned over to ITS for disposal, a reasonable attempt should be made to delete and erase all information from the phone. ITS will then wipe clean the memory of the phone again before properly disposing of it.

## ITS Communications

TS will make every effort to inform the Trinity community of discretionary changes that substantially affect their devices and service well ahead of time. Examples include migration to a new email service or introduction of major new services. Occasionally, it may become necessary to interrupt TUNetwork or system services for routine maintenance, installation of software upgrades, repairs, etc. These events are planned in advance. ITS will work to alert members of the community to these impending events through multiple communication venues. Announcement of pending changes will be made through emails and via appropriate listservs. Training and documentation, as needed, will be available at or ahead of the time for the change.

Unfortunately, unexpected system outages do occur, in which one or more file servers, email services or some portion of the TUNetwork becomes unavailable without warning. ITS will provide timely information whenever possible when these instances occur through emails from its-announcement@trinity.edu.

## *Performance Evaluation*

### Consequences of Policy Violation:

**Enforcement**

Any behavior in violation of this policy is cause for disciplinary action. Violations will be adjudicated, as appropriate, by the CIO, the Office of the Dean of Students, the Office of Housing and Residential Life, and/or the Office of Human Resources. Sanctions as a result of violations of this policy may result in, but are not limited to, any or all of the following:

- Attending a class or meeting on device management issues, as well as successful completion of a follow up quiz;
- Loss of University computing, email and/or voice mail privileges;
- Disconnection from the residential hall internet network;
- University judicial sanctions as prescribed by the student Code of Conduct;
- Monetary reimbursement to the University or other appropriate sources;
- Reassignment or removal from University housing and/or suspension or expulsion from the University;
- Prosecution under applicable civil or criminal laws;
- Employees may be subject to disciplinary action.

**Violations**

Reports of non-compliance with this policy should be reported to: infosec@trinity.edu

## *Terms & Definitions*

### Terms and Definitions:

| Term: | Definition: |
|---|---|
| Patch | A patch is a piece of software designed to update a computer program or its supporting data, to fix or improve it. This includes fixing security vulnerabilities and other bugs, and improving the usability or performance. |
| Patch management | The process of using a strategy and plan of what patches should be applied to which systems at a specified time. |
| Port de-activation | A security function ensuring that no unwanted devices are connected to the TUNetwork. |

# *Revision Management*

### Revision History Log:

| Revision #: | Date: | Recorded By: |
|---|---|---|
| v1.0 | 8/14/2019 2:37 PM | Courtney Cunningham |

### Vice President Approval:

Enter Vice President(s) that are responsible for approving this document

| Name: | Title: |
|---|---|
| Gary Logan | Vice President for Finance & Administration |