TRINE UNIVERSITY

Information Technology Security and Usage Policy

Latest Revision: April 19, 2012
Original: July 28, 2006

TABLE OF CONTENTS

Introduction **1**
Policy Purpose **1**
Policy Administration **1**
Persons Subject to Policy **1**
Data **1**
Data Ownership 1
Data User Responsibilities 2
Confidential Data 2
Encryption 2
Backups 2
Cloud storage 2
Passwords 2
Network Access **3**
Appropriate Use **4**
Inventory 4
Employee Termination or Transfer 5
Student Access Termination 5
Guest Access 5
Internet 5
Software **6**
Copyright 6
Home Computers 6
Acquisition of Technology **6**
Software 6
Personal Computers 7
Secondary Device 7
Wireless and Mobile Computing **8**
Device Support 9
Incident Reporting **9**
User Rights Management **9**
Appendix A – Security Access Warning Message **11**
Appendix B – Password Management **12**
Appendix C – Confidential Information **13**

Introduction

Information and its availability are essential to the operation of Trine University. Expanded use of technology has actualized precise, consistent and rapid information processing which has allowed information to be more readily accessible to administration, students, faculty and staff than ever before.

Many operations that traditionally were manual or partially automated are today fully dependent upon the availability of automated information services to perform and support their daily functions. The interruptions, disruption, or loss of an information support service may adversely affect Trine University's ability to administer programs and provide services. The effects of such risks must be eliminated or minimized.

The scope of this Security Policy covers the following.

- Data center processing facilities and equipment
- Telecommunications networks
- Electronic data
- Application software programs
- Personal computers including desktops, laptops and convertible laptop/tablets
- Mobile hardware such as Smartphones, tablets, and gaming systems

Policy Purpose

The purpose of the Trine University Computer Security Policy is to ensure the safety and integrity of information maintained on Trine University computerized information systems. This policy is not intended to address the proprietary interests of intellectual property.

Policy Administration

This policy has been approved by the President's Cabinet and is administered by the Information Technology department. Policy violations are reported to the Chief Information Officer (CIO) and the employee supervisor or VP of Student Life.

Persons Subject to Policy

The Security Policy applies to all Trine University employees, students and others (e.g. vendors, contractors, guests, etc.) accessing or attaching to computers and networks operated by Trine University. Persons violating the Security Policy will be subject to appropriate University, administrative, civil and/or criminal sanctions.

Data

Data Ownership - The data "owner" is the department with primary responsibility for creation and maintenance of the data content. The data owner is responsible for determining how

the data may be used within existing policies, and authorizing who may access the data. The Jenzabar software module managers, along with their respective Vice President's, are data owners for information associated with this enterprise administrative software.

Data User Responsibilities - The data user is the person who has been granted explicit authorization to access the data by the owner. The user must use the data only for purposes specified by the owner, comply with security measures specified by the owner, and not disclose information about the data nor the access controls over the data unless specifically authorized by the owner.

Confidential Data - Information, which by law is confidential, must be protected from unauthorized access or modification. Confidential information shall be accessible only by personnel who are authorized by the owner on a basis of strict "need to know" in the performance of their duties. Data containing any confidential information shall be readily identifiable and treated as confidential in its entirety. Confidential information is not to be extracted, downloaded or printed and taken off of university property. Confidential data is defined in Appendix C. Reference the University Identity Theft / Red Flag Policy for further information about appropriate handling of confidential data.

Encryption – Data processed and stored in University owned systems is not encrypted. PCI compliance for credit card processing is maintained by using secure third party services for all transactions. All communications between University employees and outside parties that transmit confidential or sensitive data must use an Information Technology approved secure and encrypted service.

Backups –Backup policy intent is to cover all production server-based applications and data, facilitating business resumption after the loss of server hardware. Only servers managed by Information Technology are covered by this policy. Backup of material stored locally on end-user workstations is the responsibility of the user. For this reason, all users are strongly recommended to store copies of critical documents/files on network shares, and not on local PC drives, portable devices, or cloud based services.

Cloud storage – Confidential, sensitive, or critical data should not be stored outside of the University network unless approved by the data owner and Information Technology. Cloud storage provider contracts should be evaluated for data ownership and privacy policies before such services are utilized. Students are encouraged to use their Microsoft Live@edu provided Sky Drive as an approved method to store and share documents.

Passwords - User ID's and passwords are used to control access to all computer systems except for those specific resources identified as having public access.

Student passwords are assigned upon registration at Trine University and can be changed by the students. There is no forced password change procedure required for students. Student active

directory passwords can be reset by visiting the Help Desk in person and providing your student ID and birth date. Requests made via telephone will require the student to provide additional information that is validated against the students administrative record before a password is reset. Password resets for other student systems, such as email, myPORTAL, and Moodle, are initiated by the student within the individual software systems.

Employee passwords must be changed periodically by the user. Computer resources will require passwords to be changed at least every 90 days and be unique, up to or exceeding six previous passwords. Employees are responsible for managing their passwords according to the guidelines specified in Appendix B, Password Management. For security purposes, prior to resetting a password, the Help Desk requires that the requestor validate personal information.

Network Access

Access to the Trine University network and its resources is provided for University owned hardware and other devices that meet Information Technology hardware and software configuration standards. Persons using or attaching to Trine University computer resources will acknowledge compliance with the Computer Security Policy upon login to University owned PC's, Bradford Campus Manager, and Moodle.

All Trine University owned computers, except those deemed public or special purpose by Information Technology, will "lock" after a ten (or thirty for faculty) minute period of inactivity and display a screensaver. The user that was logged in to the computer before it became locked, or a network administrator, will need to enter their password to access the computer.

Personal Devices: Employees - Personally owned employee devices may attach to the wired network after successful login and registration, but will have limited access to University resources. See Wireless and Mobile Computing section of this policy for more information about wireless access.

Personal Devices: Students – Resident students wishing to connect entertainment devices such as gaming consoles (ie: Nintendo, PlayStation, Xbox) or Internet ready devices (ie: televisions, DVD/Blu-ray players, Roku, Boxee Box) to the wired or wireless network will need to register that device. Registration can be completed one of two ways. Through the University's registration site or by contacting the Help Desk. The physical (MAC) address is required for registration in order the device to be authorized to be used on the University's network.

Network Devices – Any device that may cause interference with the University's wired and/or wireless network is prohibited. Employees and students are not authorized to connect any networking device to the University's wired or wireless network. This includes but is not limited, to; routers, switches or hubs, access points, and printers. These types of devices can negatively impact the performance of University provided computer services. Printers with wireless connectivity must have that feature disabled. Wired access is limited to one device per hard-wired port.

Appropriate Use

Unauthorized use, alteration, destruction, or disclosure of computer assets is a computer-related crime, punishable under Indiana statutes and federal laws, as well as through administrative and/or civil sanctions. Willful violations of the Security Policy that may be violations of laws will be reported to the Appropriate Law Enforcement Office.

Use of Trine University systems to attack Trine University or other computer systems, internal or external to Trine University, is a violation of this policy. Attempting to circumvent security or administrative access controls for computer resources is a violation of this policy, as is assisting someone else or requesting someone else to circumvent security or administrative access controls.

To reduce the risk of attacks and security threats, Information Technology maintains a network based spam filtering device, anti-virus and anti-spam software on personal computers, and Microsoft Windows updates and patches on all University owned computers. Users must exercise caution when opening email and text message attachments or clicking on links. If an email is suspicious, contact the Help Desk for assistance.

Employees may not use Trine University computer resources to set up services or accounts the purpose of which is not in accordance with the non-profit, educational mission of the University.

Trine University reserves the right to monitor the contents of electronic mail messages or the internet browsing habits of its students and employees. Information in electronic files or logs which contain a history of electronic communications may be subject to disclosure under certain circumstances; for example, during audit or legal investigations.

Trine University equipment is intended for work related use only. Personal use of equipment for activities such as messaging, Internet browsing, and gaming, is discouraged and should be performed during non-work hours.

Inventory – University owned computers will be inventoried on a periodic basis and users are expected to provide timely access to equipment for these purposes. Unauthorized or unlicensed software will be removed. When a new computer is delivered to an employee as a replacement, only licensed software will be installed regardless of what was installed on the old computer.

As a financial practice Trine University leases personal computers and all components and peripherals, including monitor, keyboard and mouse must be kept intact as one unit and provided for return at end of lease. Users are not permitted to disassemble hardware or deface any University equipment and must leave all labels and asset tags intact. Once a computer is assigned to a user, it is the user's responsibility to retain the inventoried equipment until such time as Information Technology replaces it. Relocation of all equipment, in offices or computer labs, must be requested by contacting the Help Desk. Missing equipment may be charged to the department responsible.

Trine University owned portable laptop and convertible laptop/tablet computers must be physically locked down when in an office. Smaller hand held devices such as smartphones, netbooks, and iPads must be secured within a locked office or desk at all times when not in use. Departments will be held responsible if their portable computers are stolen due to lack of physical security.

Unplugging a PC from its wired network connection in a computer lab and using the network connection for other devices is not permitted.

Employee Termination or Transfer – When an employee terminates employment and a future contract has not been issued, their access to computer resources will be terminated immediately. Managers and supervisors are responsible for notifying Human Resources when (or before) an employee leaves the University or transfers to another department so that access can be revoked. Terminations are reported to Information Technology by Human Resources immediately upon learning of the termination and Information Technology will retrieve the equipment for refresh and redeployment. If an employee wishes to retrieve personal data from their account they should contact Human Resources immediately.

Trine University provides equipment and software to meet the needs of the job function that an employee fulfills. When an employee termination occurs or an employee moves to another position within the University, the computing assets will stay with the original position. Exceptions will be made on a case by case basis as approved by the Vice President and CIO.

Student Access Termination - Students who are graduating will retain access to their Trine University email for life. Network access is removed for students who graduate, withdraw, or transfer. Access to course specific computing resources is removed at the end of the semester/term.

Guest Access – Access to the Trine University network is available for guests for a predetermined length of time upon the request of a University employee. Guest access is administered by Information Technology and the guest computers are subject to the University standard network registration process. Registration requires that appropriate anti-virus software be installed and up to date and that operating system security patches are installed.

Internet - Internet users must be aware that as they access Internet resources, they will be associated with the University through the mechanisms of the TCP/IP protocols. Therefore, users should access resources in accordance with their job description. Users shall remember that email and internet transmissions are not private information. Anything sent could possibly be read by individuals other than the intended recipient. Users shall not transmit any information that may be damaging to the organization or themselves. Confidential and private information, as covered in other university policies, shall not be transmitted without proper precautions. Users should exercise similar care when transmitting personal data.

Software

All end-user workstations must have virus protection software installed and current and maintain current operating system security patches

Copyright - Unauthorized/unlicensed use of software (software piracy) is illegal and such software will be removed by the appropriate administrators and reported to the CIO and VP of Student Life. End users will not download or share copyrighted materials via any method. This includes peer-to-peer (P2P) networking or any service providing free access to copyrighted materials. Sharing of files from device to device via shared drives is allowed only for non-copyrighted materials. The student preferred method for sharing such files is the Windows Live Skydrive, which is included with student email accounts. Employee file sharing can be accomplished using network folders.

Home Computers - Generally, Trine University-owned software cannot be taken home and loaded on a user's home computer if it also resides on a Trine University computer. However, some software packages such as Microsoft Office allow home use under special circumstances. Users should reference the Information Technology web site or contact the Help Desk to obtain additional information.

Acquisition of Technology

Software - All software acquired by the University for installation on, or access from, personal computers must be purchased through Information Technology (or Information Technology approved method), where a central budget is maintained. Additions to the approved budget are funded by the requesting department.

Once requested, to the best of their ability Information Technology will test to ensure that the software is compatible with the Trine University infrastructure and will not incur a security risk to the University before purchasing. Software acquisition channels are restricted to ensure that Information Technology has a complete inventory of all software that has been purchased for University computers to ensure legal software licensing, lowest cost, and that adequate support and upgrades can be performed as needed. This includes software that may be downloaded and/or purchased from the Internet. After the acquisition requirements have been met, the software shall be installed by a member of the Information Technology staff, or an Information Technology authorized installer.

Computer software donated to Trine University or purchased using University funds is Trine University property.

Discounted and "work at home" software for personal use can be purchased directly by employees through the Information Technology web site. Users are not permitted to bring software from home and load it onto Trine University computers.

Mobile application software, such as iPhone and iPad Apps, can be purchased and installed by the device user. It is the responsibility of the user or their department to fund these purchases. University credit cards are not to be linked to iTunes accounts. The primary user of the device will be required to link a personal credit card to the iTunes account managing the device.

This ensures that:

- all purchases remain the property of the individual
- no unapproved purchases are charged to a University Credit Card
- the University is not charged sales tax for purchases

On an as needed basis, Information Technology will recommend common apps/software to perform specific functions. Information Technology does not support mobile device software application functionality unless such software is developed by Information Technology or provided as part of administrative or academic Information Technology supported software systems such as Jenzabar or Moodle.

Personal Computers – Information Technology selects manufacturers and identifies models and configurations to meet the needs of the University departments. In most cases the computers are leased and replaced on three to four year cycles. All components of the computer configuration, including carrying case and peripherals are to be kept together as one unit unless split by an authorized Information Technology representative.

Secondary Device – A secondary device, such as a smartphone or tablet (iPad), is not a substitute for a personal computer but may be requested for either of the following scenarios.

- Device requested for individual employees whose job function is such that the use of the device significantly enhances the performance of the employee. The business purpose for the device must demonstrate that tasks are difficult, cumbersome, or impossible to complete with existing campus technology / personal computer.
- Device requested for departmental use wherein multiple employees responsible for performing a shared set of job functions are such that the use of the device significantly enhances the performance of the employees in the department.

Information Technology will determine which devices are approved University standards and will only purchase and support such devices. The approved list will be updated as needs and devices change.

Acquisition of secondary devices requires Vice President approval and will be on a case-by-case basis. It is the responsibility of the requestor to secure appropriate department funding for the device and to justify the purchase. All requests must first come through the Help Desk with documentation confirming reason for purchase per the above requirements, along with Vice President approval and identification of the funding source. All devices purchased with

university funds will be inventoried and considered University property.

Devices are assigned to the person and position held and must be returned upon an employee's separation from the University or transfer to a new position within the University. Devices no longer found useful by a department or individual must be returned to Information Technology. In most cases, applications installed on the device are the property of the individual and will be removed as the device is wiped and returned to its native state prior to redeployment.

Secondary device hardware will not be maintained by Information Technology and once determined unusable or obsolete, must be turned in to Information Technology for recycling. No additional apps will be purchased once the current release of the operating system does not support the device - at that point the device will be considered End of Life. The device will not be supported and continued use by a department or individual is at their own risk. Replacement devices will not be planned for or funded by Information Technology.

Printers are leased through a University preferred vendor. Reference the Trine University Print Policy issued by the Business Office and Information Technology Department for more information.

Wireless and Mobile Computing

This portion of the Security and Usage Policy applies to any mobile computing device connected to Trine University Information Technology resources, used to process or store University data, or conduct University business. Mobile devices include various types of equipment such as SmartPhones, notebooks, tablets, or netbook computers and may be owned by either the University or the employee.

Wireless networks are inherently insecure. In any wireless network, the transmission over public airspace always poses a risk of interception and capture, regardless of the methods of encryption or security. Because of the inherent security risks when using a wireless system, users assume responsibility for any data transmitted via this connection. All users are expected to exercise caution when using a wireless network.

Tablet or netbook computers are devices designed and marketed as a platform for consuming audio-visual media including books, periodicals, movies, music, games and web content. Tablets, much like smartphones, can be configured to connect to an email system to synchronize email, calendar, and contacts. Tablets in the terms of this policy, are small, thin, portable computers having an LCD screen onto which data can be input with a stylus or the fingertips (one example being the Apple iPad).

The University allows all students, staff and faculty with active user accounts to connect to the wireless network using a University owned or personally owned mobile device. To connect to the Trine University wireless network, the mobile device must be able to connect to a wireless network using 802.11g, (or earlier) wireless standards. The University does not allow employee

owned “hacked” devices, or devices that have been altered from the manufacturer’s original configuration by someone other than the devices original owner, to connect to its network.

It is highly likely that mobile devices used for university business contain sensitive information in the form of email correspondence, documents, or other files. It is the responsibility of the user to ensure that information stored on the mobile device is protected as required by applicable state and federal laws such as FERPA and HIPAA. Users must meet the following security provisions before a device is used to process or store University data, or connect to Trine University information resources.

1. Password Policy: All employee mobile devices must be secured using a logon or power-on password.
2. Avoid using auto-complete feature that remember user names or passwords.
3. Enable auto-lock features when available.
4. Disable Wi-Fi and set Bluetooth to non-discoverable when not in use.
5. Virus Protection: Information Technology approved virus protection must be installed and up-to-date on any device where such utility is commonly available.
6. Required system patches and updates: Mobile device users must ensure that devices are up-to-date with required software patches and updates. Enable automatic update functions when available.
7. Data: Users must be aware that all information synched from the Trine University network is the property of the University and not the individual. Do not store data files on personally owned mobile devices. Delete all information / wipe device prior to disposal.

Device Support - The extent to which Trine University will support a personally owned device’s connection is limited to authorizing the devices MAC or Ethernet Address onto the wireless network. Questions or problems concerning the actual mobile device and its settings need to be addressed to the service provider and/or manufacturer of the mobile device.

Incident Reporting

Individuals who have reason to believe that their personal information has been compromised, computer intrusion/tampering has occurred with respect to their accounts, or theft of equipment has occurred should contact the Help Desk (and Campus Safety in the event of a theft).

Employees who believe they have experienced computer generated harassment or discrimination should contact the Human Resources department. Students who believe they have experienced computer generated harassment or discrimination should contact the VP of Student Life.

User Rights Management

With the deployment of Windows 7, all PC’s will be installed with normal user rights.

Exceptions to this policy will be considered only if they are the result of a required software configuration, and the software in question is not available in an updated format for Windows 7.

Appendix A – Security Access Warning Message

"By logging onto the Trine University network, you agree to abide by the terms and conditions set forth in the Trine University Information Technology Security and Usage Policy and the Intellectual Property Policy."

Each system requires an active response from the user to move past this screen at the time of sign-on (i.e. user must press the Enter/Return key to continue).

Appendix B – Password Management

Password Selection

Passwords are used to authenticate a user's identity and to establish accountability. A password that is easily guessed is a bad password which compromises security and accountability of actions taken by the user ID's which represents the user's identity.

Beginning with the deployment of Windows 7, the Trine University standard password length is 8 characters and it must be complex. A complex password requires that the password cannot be your name or login user name and must contain the following components: a capital letter, a lowercase letter, and a number or a special character.

What are popular passwords that could be easily guessed?

- Your name
- Your parents' names
- Your pet's name
- Your spouse's name
- Your children's names
- Birthdates

Other bad passwords are these names spelled backwards or followed by a single digit. Short passwords are also bad, because there are fewer of them; they are more easily guessed. Especially bad are "magic words" from computer games, such a XYZZY. Other bad choices include phone numbers, characters from favorite movies or books, local landmark names, favorite drinks, or famous people.

Some rules for choosing a good password are:

- Choose something easily remembered so it doesn't have to be written down.
- It should be easy to type quickly so someone cannot follow what was typed by watching the keyboard.
- Use two short words and combine them with a special character or a number, such as ROBOT4ME or EYE-CON.

Number of Characters	Possible
3	46,656
4	1,679,616
5	60,466,176
6	2,176,782,336
7	78,364,164,096
8	2,821,109,907,456
9	101,559,956,668,416

Appendix C – Confidential Information

According to Indiana Code 24-4.9 “personal information” means:

- Social Security number that is not encrypted or redacted, or
- Individual’s first and last name or first initial and last name and one or more of the following:
- Driver’s license number,
- State ID card number,
- Credit card number, or
- Financial account number/debit card number and security code/password, or access code.