



## Information Technology Security & Usage Policy

Latest Revision: June 30, 2009

Original: July 28, 2006

### Introduction

Information and its availability are essential to the operation of TSU programs. Expanded use of telecommunications and computing facilities has actualized precise, consistent and rapid information processing and has allowed information to be more readily accessible to administration, students, faculty and staff than ever before. TSU has experienced increases in productivity, the quality and quantity of services delivered, and enhanced administrative capabilities, as a direct result of the use of information technology.

Many program 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 TSU'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
- Application software programs
- Electronic data
- Personal computers, PDA's, Smartphones, networking equipment, and gaming systems

### Roles and Responsibilities

#### Policy Administration

This policy has been approved by the President's Cabinet and administered by the Information Technology (IT) department. Policy violations are reported to the Chief Information Officer (CIO), the employee supervisor, or Dean of Students.

#### Data Ownership

The data "owner" is the department with primary responsibility for creation and maintenance of the data content.



### **Data Owner Responsibilities**

The data owner is responsible for determining how the data may be used within existing policies, and authorizing who may access the data.

### **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.

### **Policy Purpose**

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

### **Policy Applicability**

The Computer Security Policy applies to all TSU faculty, staff, students and others (e.g. vendors, grant or independent contractors, etc.) accessing or attaching to computers operated by TSU. Persons violating the Computer Security Policy will be subject to appropriate University, administrative, civil and/or criminal sanctions.

It is the policy of Trine University that:

1. Access to the Trine University network will be granted to those that meet the University hardware and software configuration standards.
2. Persons using or attaching to Trine University computer resources will acknowledge compliance with the Computer Security Policy. All computer systems will provide a notice before logon stating that the computer is protected by a computer security system; that unauthorized access is not permitted; and that usage may be monitored
3. 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

# TRINE

---

## UNIVERSITY

Computer Security Policy that may be violations of laws will be reported to the Appropriate Law Enforcement Office.

4. Computer software donated to Trine University or purchased using University funds is Trine University property.
5. 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 Dean of Students.
6. 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.
7. 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.
8. User ID's and passwords must control access to all computer resources except for those specific resources identified as having public access.
9. 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. Users are responsible for managing their passwords according to the guidelines specified in Appendix B, Password management.
  - a. Adjunct Faculty Password Handling
    - i. Main Campus – Department Chairs must contact the IT Helpdesk and request a password reset.
    - ii. Branch Campuses – Branch Campus Managers must contact the IT Helpdesk and request a password reset.
10. Data, which is essential to critical functions, must be protected from loss, contamination, or destruction. 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.

# TRINE

---

## UNIVERSITY

11. When an employee terminates employment and a future contract has not been issued, their access to computer resources will be terminated immediately. If an employee wishes to retrieve personal data from their account they should contact Human Resources immediately. Similarly, students who are graduating will have their access to computer resources terminated 3 months after the semester ends.
12. All end-user workstations must have virus protection software installed and current and maintain current operating system security patches.
13. All information processing areas used to house computer resources supporting mission critical applications must be protected by physical controls appropriate for the size and complexity of the operations and the criticality or sensitivity of the systems operated at those locations. Authorized personnel shall be determined by the area supervisor and the Policy Administrator.
14. 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 Dean of Students.
15. Individuals who have reason to believe that their personal information has been compromised or computer intrusion/tampering have occurred with respect to their accounts should contact the IT Help Desk.
16. Guest access to the Trine University Network will be evaluated on a case-by-case basis.
17. 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.
18. 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 mail 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

20. All Trine University owned employee computers located offices or classrooms 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.
21. Trine University owned portable computers (laptops, tablets, etc) will need to be physically locked down when in an office. Employees will be held responsible if their portable computer is stolen while not physically locked down.
22. Trine University will not support personally-owned wireless access points, switches, hubs or routers. It is the policy of Trine University that wired access be limited to one device per hard-wired port.
23. End users will not download or share copyrighted materials via any method. This included peer-to-peer (P2P) networking via services such as: LimeWire, Kazaa, BitTorrent, BearShare, or any service providing free access to copyrighted materials. P2P sharing of files from device to device via shared drives is allowed only for non copyrighted materials. The preferred method for sharing such files is via Windows Live Skydrive, which is included with student email accounts.
24. 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.

### **User Rights Management**

Three levels of user rights are possible under Trine University’s current Microsoft operating system: Normal Users, Power Users, and Administrators. To minimize the possibility of a security breach (viruses, stolen data, identify theft, etc.), best practice is to have an employee operate as a Normal User to reduce the "attack surface" of his or her computer by eliminating unnecessary privileges that can result in network exploits and computer compromises. As a Normal User, software is installed on an employee’s computer by an IT Help Desk staff member.

The Administrator level (administrative rights) allows a user to install software that modifies the operating system, and these rights are reserved for IT staff in the interest of maintaining the integrity of the network. Power User rights allow a

# TRINE

---

## UNIVERSITY

user to install and run applications that do not affect the operating system. This level of rights was designed to accommodate software written for execution under older operating systems. In the case of a valid business reason, Power User rights may be granted to those approved by the VP for Academic Affairs and Chief Information Officer. To minimize the “attack surface” of the network, Power User rights may be approved for a limited number of users either to address a one-time need or on a permanent basis.

If software which modifies the Trine University core image (list can be obtained from the IT Help Desk) is required, it must be used on a lab or test machine in order to preserve the users’ production PC environment. IT must be contacted to assist with any software that requires a network to execute or that includes a multi-user, shared database. These requests are typically projects requiring approval of the IT Academic Sub-Committee.

### **Power User Responsibilities**

- Document business reason for additional rights
- Do not modify software in the Trine University core image (list can be obtained from the IT Help Desk)
- Install software used for business purposes only
- Report all software installed to IT with proof of licensing (It is recommend that the license be registered to Trine University.)
- Only login as Power User when necessary to install or run software. Login as normal user otherwise
- Provide self-support of PC, excluding network connectivity and hardware break/fix service
- Store data in “My Documents”, on a network server, or an external storage device

### **Information Technology Responsibilities**

- Maintain software inventory using licenses provided by Power Users
- If, after reasonable effort, a Power Users PC problem cannot be solved by the IT Help Desk, the corrective method will be a PC re-image. In this case, IT will reinstall the core image, copy personal user settings, .pst files, and the contents of My Documents folder.

To request Power User rights, complete the form in appendix D on page 11

# TRINE

---

UNIVERSITY



## ***Appendix A – Security Access Warning Message***

Successful prosecution of unauthorized access to Trine University computerized systems requires that users are notified prior to their entry into the systems that the data is owned by Trine University and that activities on the system are subject to monitoring. All multi-user computer systems will display the following warning message when a user attempts to access the system and prior to actually logging into a system:

This system is to be used only by authorized personnel and all others will be prosecuted. Activities on this system are automatically logged and subject to review. Trine University reserves the right to intercept, record, read or disclose all data on this system at the sole discretion of authorized personnel. Specifically system administrators may disclose any information on or about this system to law enforcement or other appropriate individuals. Users should not expect privacy from system review for any data whether business or personal even if encrypted or password-protected. Trine University abides by the Family Educational Rights Act of 1974 and takes precautions to prevent the disclosure of confidential information.

-  
Use of this system constitutes consent to these terms.

Each system must require 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.

What are popular passwords that could be easily guessed?

- Your name
- Your spouse's name
- Your parents' names
- 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:

- Use both uppercase and lowercase letters if the computer system considers an uppercase letter to be different from a lowercase letter when the password is entered.
- Include digits and punctuation characters as well as letters.
- 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
10	3,656,158,440,062,9
11	131,621,703,842,267



### ***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.



***Appendix D – Power User Request Form***

***Request for PC Power User Rights***

You are requesting power user rights to the workstation in your area. In order for the rights to be considered, a statement of business need which explicitly details the justification for this level of access must be documented below. If the IT Help Desk can provide the services on your workstation that you require to perform your job, power user rights will not be approved. The IT department will determine the method and timing for granting approved power user rights.

By signing this form, you acknowledge understanding the associated responsibilities as documented in the Information Technology Security Policy.

**Business Reason for Request (suggested format: who, what, when, why):**

---

---

---

---

Requestor Name (Printed)	Requestor Department
Requestor Signature	Date
Requestor Supervisor(s) Approval	Date
VPAA Approval	Date
CIO Approval	Date