

# **St. Cloud Technical & Community College**

## **Policies and Procedures**

### **Chapter S5 – Administration**

#### **S5.2 Acceptable Use of Computers and Information Technology Resources Policy**

SCTCC follows MnSCU policy 5.22 Acceptable Use of Computers and Information Technology Resources <http://www.mnscu.edu/board/policy/522.html>, procedure 5.22.1 <http://www.mnscu.edu/board/procedure/522p1.html>, and procedure 5.22.2 Cellular and Other Mobile Computing Devices <http://www.mnscu.edu/board/procedure/522p2.html>

*Update Revision Responsibility: Vice President for Administration*

The computer facilities at St. Cloud Technical & Community College are provided for use by currently enrolled students, faculty and staff of the college, for college-related activities only. Access to the equipment and technology provided in these facilities is a privilege. All students, faculty and staff are responsible for seeing that these facilities are used in an effective, efficient, ethical and lawful manner.

Failure to abide by any portion of this entire policy is prohibited. Students, faculty and staff who violate this policy will be subject to disciplinary procedures of the college and/or immediate revocation of Network privileges.

I. Computer facilities and computer accounts: Computer facilities (equipment, software and related computer technology) and accounts are owned by the college and are to be used for college-related activities only and are not to be used for commercial purposes or non-college-related activities. The following items relate explicitly to use of computer facilities and use of computer accounts:

- A. All access to computer systems, including the issuing of passwords, must be approved by the Information Technology Services department. (Instructors wishing to add student accounts for instructional purposes should receive prior approval from the Information Technology Services department and that instructor agrees to take full responsibility for those accounts.) Users are required to take every precaution to secure their accounts, especially by keeping passwords private.

- B. Computer equipment and accounts are to be used for the purpose for which they are assigned and are not to be used for commercial purposes or non-college-related activities. State statute (Chapter 43 A.38, Subd. 4) specifically states that an employee shall not use or allow the use of state time, supplies, or state owned or leased property and equipment for the employee's private interests or any other use not in the interest of the state, except as provided by law.
- C. No one may use loopholes in computer security or knowledge of special passwords to damage computer systems, or obtain extra resources, to take resources from another user, or to use systems for which proper authorization has not been given. Any knowledge of these security issues for college networks should be reported to the Information Technology Services (hereafter referred to as IT) department immediately.
- D. Under special circumstances, faculty or staff may be allowed to take college-owned equipment off-site. Approval to do this must be obtained from the department or group responsible for the equipment. The checkout of this equipment must be formally documented with the department chair or the designated personnel. All portions of this policy apply to usage of this equipment as well.
- E. No one may deliberately attempt to degrade the performance of a computer system.
- F. No faculty, staff, or student may load software on college-owned equipment unless the software is owned by or licensed to the college and having received written prior approval from IT. Exceptions to this are:
  - 1. Evaluation software may be installed if prior written approval of the IT department. Staff or faculty requesting software installed to Network must be present at the time of installation.
  - 2. Students may load classroom software under the direction and supervision of the instructor only.
- G. No modification will be made to college-owned hardware without written approval of the instructor only.
- H. Web pages will not be permitted unless authorized by State of Minnesota, SCTCC Leadership Team or Designee for approved college curriculum.
- I. No one may violate copyright laws and license agreements.

- I. Any attempt to disguise the origin of a message by altering the user ID or domain name is prohibited.
- J. Peer-to-Peer file sharing (P2P) is prohibited on the campus network at St. Cloud Technical & Community College. In addition, it is a violation of policy to use technology designed to circumvent the blocking of peer-to-peer file sharing.

II. **Viruses:** All computers utilizing the St. Cloud Technical & Community College network must have at least the College approved, vendor-supported anti-virus software installed and scheduled to run at regular intervals.

Anti-virus software and the virus definition files must be kept up-to-date. Virus-infected computers will be removed from the network until they are verified as virus-free. Also, any computers found on the network without anti-virus software installed will be removed from the network until they have installed and updated the College approved, vendor-supported anti-virus software. Network administrators are responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified as virus-free. Any activities with the intention to create and/or distribute malicious programs into SCTCC 's networks (e.g., viruses, worms, Trojan horses, spam, etc.) are prohibited and anyone found to have violated this policy might be subject to disciplinary action, up to and including termination of employment or expulsion from SCTCC.

III. **Electronic communications:** Electronic communication facilities (i.e., E-mail, talk, network news and Internet Relay Chat) are for college related activities only. Harassing messages must not be transmitted over the Internet or any college-owned network, on or off-campus. Inappropriate messages include but are not limited to:

- A. Harassment message: Message that harasses an individual or group because of their sex, race, religious beliefs, national origin, disability or sexual orientation.
- B. Non-college related messages: Messages that contain such items as, but not limited to: chain letters, receipts, announce "garage sales" or to advertise items for sale or rent that result in personal gain or revenue for non-college departments or programs.

If an individual wishes to participate in a news group of a controversial nature, he/she is encouraged to include a disclaimer within the text of any document that states the author is speaking for his/herself and not as a representative of the college.

This policy should not be interpreted as prohibiting transmissions protected by existing collective bargaining agreement provisions dealing with mailing privileges nor shall it be used to deny access to recognized student organizations and related student service departments who wish to announce upcoming events that may be of interest to members

of the college community. Users are, however, asked to take caution in directing their messages to large audiences and to avoid sending repeats of the same message as “reminders”, to avoid causing unnecessary traffic on the network.

IV. Internet usage: The internet must be used as a learning and research tool for college-related activities only. The following items relate explicitly to the usage of the Internet.

- A. No one may participate in any activity that violates the spirit of cooperation that is the basis of the Internet.
- B. The individual user is responsible for his/her image on the Internet, as well as, the image of the college.
- C. No one may deliberately attempt to degrade the performance of a computer system on the Internet including the college network.
- D. No one may install any software or establish a TCP/IP resource on any campus network without the explicit consent of the CIO. All addresses are administered by the IT department. Users must adhere to the addressing conventions established by this department.
- E. All users must adhere to all applicable laws, including federal copyright laws in using information obtained on the Internet.

Any faculty, student, or staff person who has Internet access is expected to comply with this item in the policy and the generally accepted policies and practices of the Internet.

V. Confidentiality and/or Privacy: Users are advised that the data stored or sent on the system is **not private**. There are a number of circumstances in which data stored on the system will be accessed by authorized individuals. Those circumstances include, but are not limited, to the following:

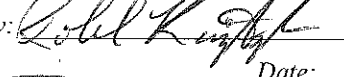

- A. Performing administrative tasks, and/or routine system maintenance and related computer systems.
- B. Monitoring use of the computer systems to determine whether the policies of the College, MnSCU, and/or state or federal law have been broken.
- C. Monitoring use of the E-mail and related computer systems when it is necessary so that the College can provide its services or protect the rights or property of the College.

St. Cloud Technical & Community College makes no warranties of any kind, expressed or implied, for the computer facilities and resources it is providing. St. Cloud Technical & Community College will not be responsible for any damages that users suffer. This

includes loss of data resulting from delays, non-deliveries, and miss-deliveries, or service interruptions caused by its own negligence or a user's error or omission. Use of any information obtained via the Internet is at your own risk. St. Cloud Technical & Community College takes no responsibility for the accuracy or quality of information obtained through the internet services.

SCTCC follows MnSCU policy 5.22 Acceptable Use of Computers and Information Technology Resources: <http://www.mnscu.edu/board/policy/>

---

Faculty Shared Governance President or AASC Chair Review:  Date: 8/31/12  
College President:  Date: 9/5/12  
Date of Adoption: \_\_\_\_\_  
Date of Implementation: \_\_\_\_\_  
Date repealed or replaced: \_\_\_\_\_

# **St. Cloud Technical & Community College**

## **Policies and Procedures**

### **Chapter S5 – Administration**

#### **S5.2.1 Sensitive Assets Tracking Procedure**

##### **Arrival/receipt of New Sensitive Assets – Process**

1. Items arrive at the main campus receiving area, the carrier tracking number is scanned and an email is automatically sent to the person who ordered the item with the piece counts. A copy of the purchase order is also scanned to the Information Technology Services Department (hereafter referred to as IT) to alert them of items being received.
2. All sensitive assets are delivered to IT and counts are reconciled between the packing list and the email sent by receiving.
3. Packing lists are sent to the administrative assistant in the area which the employee reports to, and a 3-way match with the purchase order and invoice(must be approved for payment) is done.
4. Asset tag is affixed.
5. Items are assigned to an employee or a program area and are entered into the SCTCC online inventory –Information must be entered accurately and timely to ensure the integrity of the system.
6. IT fills out the Equipment Maintenance Form and sends to the Business Office Purchasing Agent for entry into ISRS and also adds the item into the SCTCC online inventory system.
7. Employees who are assigned portable devices must come to IT to pick up their device.
8. Employees with portable devices, must sign an agreement form that is kept by the laptop manager in IT. A copy of the agreement is sent to the Administrative Assistant for that area.

##### **Transfer of Sensitive Assets to a new user or storage – Process**

1. Item is delivered to IT for re-imaging and location changed to IT(room 1-215)
2. If an item is going into storage, location must be changed to indicate.
3. When the information is changed in the online system, an email is sent to the purchasing agent so that the changes can be updated in ISRS.
4. Employees with portable devices, must sign an agreement form that is kept by the laptop manager in IT. A copy of the agreement is sent to the Administrative Assistant for the area where the employee works.

##### **Disposal of Sensitive Assets- Process**

1. Item is delivered to IT workroom (room 1-215) for disposal.
2. Hard drive is scrubbed.

3. Disposal forms are completed by IT staff. Asset Tag must be attached to the form.
4. Disposal forms are signed by CIO.
5. Disposal forms are delivered to Business Manager to review and sign off.
6. Purchasing agent enters disposal information into ISRS.
7. Scrubbed computers are made ready and palletized for shipment to a State of Minnesota authorized electronic recycler.

**Repairing Sensitive Assets-Process**

1. Item is delivered to the IT Department for repair.
2. The name of the individual requiring the repair must be written on the work order form.
3. When the repairs are completed, the room location is changed back to the location of the person receiving the item.
4. If item is going into storage it must be changed in the online inventory system. Storage items must be accurately recorded.

---

Faculty Shared Governance Council President or AASC Chair Review:  Date: 8/31/12

College President: \_\_\_\_\_ Date: 9/5/12

Date of Adoption: \_\_\_\_\_

Date of Implementation: \_\_\_\_\_

Date repealed or replaced: \_\_\_\_\_

**St. Cloud Technical & Community College  
Policies and Procedures  
Chapter S5 – Administration**

**S5.2.2 Steps to Improve Sensitive Asset Accountability  
Procedure**

- A web based software package was developed in house to track SCTCC sensitive assets inventory. This software is easily used with barcode scanners.
- The inventory software sends an email to the purchasing agent in the Business Office each time changes are made. The ISRS equipment module is updated with these changes by the purchasing agent. The goal is to have the changes automatically updated into ISRS via the LADE process.
- Adding an item and deleting an item in the sensitive assets system is restricted to the purchasing agent in the Business Office.
- IT Staff are able to run mismatch reports that show discrepancies between the ISRS inventory and the SCTCC sensitive assets inventory system.
- The SCTCC IT department participated in a roundtable at the MnSCU IT conference to discuss our newly developed software system for tracking assets. As a result we have gotten several inquiries from other campuses that are interested in using the system. It was also suggested that we do a presentation on our system at next years MnSCU IT conference to present it as a “best practice” for doing inventory on MnSCU campuses.
- The CIO wrote procedures for IT Department to streamline and perfect the inventory process in the IT area.
- The CIO wrote procedures for the inventory process for Deans and Departments.
- IT staff trained SCTCC staff in the use of the new web based inventory system.

---

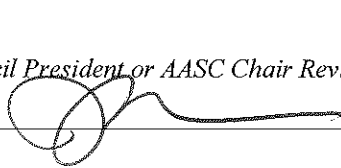
Faculty Shared Governance Council President or AASC Chair Review

College President: \_\_\_\_\_

Date of Adoption: \_\_\_\_\_

Date of Implementation: \_\_\_\_\_

Date repealed or replaced: \_\_\_\_\_



Date: 8/31/12

Date: 9/5/12



# St. Cloud Technical & Community College

## Policies and Procedures

### Chapter S5 – Administration

#### S5.2.3 Instructions for Deans/Administrative Assistant Procedure

##### Inventory of all laptops, iPads, netbooks and other sensitive portable assets

*Portable Sensitive Asset Definition: For the purposes of this document a portable sensitive asset is defined as a portable computing device capable of storing data such as a laptop, iPad or netbook.*

Each department must complete a thorough inventory of portable sensitive assets annually. Sensitive assets assigned to adjunct faculty need to be inventoried each semester. Sensitive assets assigned to full time faculty need to be inventoried once per year in the spring. Not completing this inventory successfully could result in serious consequences for the college.

The list completed by employees will be reconciled with the lists of assets assigned to the employee in the college inventory management system and in ISRS. The administrative assistants in each area will be entering this information into the College sensitive assets inventory database to be later synced with ISRS.

Only the Business Office purchasing agent is able to enter or delete assets from the SCTCC inventory system and the ISRS inventory.

##### **Every Semester:**

Each semester make sure to get back any laptops assigned to **adjuncts** if they will not be returning.

For portable sensitive assets being returned: Administrative Assistants should update the online inventory and give portable sensitive asset back to the IT department for processing.

Complete the HR checkout sheet with adjunct if they will not be returning or if they will not be reassigned.

##### **Each year in all departments:**

All portable sensitive assets must be inventoried using the form provided for this purpose. Sensitive items must be physically present to demonstrate to the administrative assistant that they are in employee's possession when submitting the inventory form.

All Sensitive Assets must be tagged with a state asset tag. If an employee discovers an untagged item, the item must be taken to IT immediately to research if it has an existing tag or if it was never issued a tag when purchased. IT will manage the process to update the inventory.

**Inventory Process done by IT and Business Office Staff:**

IT and the Business Office Staff will take care of inventorying all desktop computers and laptop carts on campus. Items that are locked up in closets or otherwise unavailable and out of plain view, must be inventoried by each department.

**Inventory of all laptops, iPads, netbooks and other sensitive portable assets**

Dear Faculty/Staff Member,

Each department must complete a thorough inventory of portable sensitive assets annually for full time faculty and staff, and each semester for adjuncts. Not completing this inventory successfully could result in serious consequences for the college. What is needed from you is a list of every portable sensitive asset that is assigned to you such as a laptop(s), iPad, or Netbook that has an asset tag affixed to it. If you are in possession of more than one laptop, please list all of the asset tag numbers. Also, if you are in possession of an untagged item please bring that to the attention of the administrative assistant assigned to your department. The list you provide will be reconciled with the list of assets assigned to you in the college inventory management system and in ISRS. The administrative assistants will be entering this information into the College sensitive assets inventory database to be later synced with ISRS. We cannot overstate the importance of supplying this information.

Sensitive items must be physically present to demonstrate to the administrative assistant that they are in your possession. Please bring them with you when submitting this form.

1. Complete form listing all portable sensitive assets in your possession such as laptops, netbooks and iPads or tablets. There is no need to list desktops.
2. Bring this form, along with the physical asset(s) to the administrative assistant for verification and signature.

State of MN Asset Tag	Serial No.	Department	Current Room	Current User	MFG (eg HP, Apple, Dell)	Model (eg Ipad, 6530B, D830)

Employee Signature \_\_\_\_\_ Date \_\_\_\_\_

Department Verified Inventory Present \_\_\_\_\_

*Signed by Dean, Supervisor or Admin Asst.*

Faculty Shared Governance Council President or AASC Chair Review: [Signature] Date: 9/31/12

College President: [Signature] Date: 9/5/12

Date of Adoption: \_\_\_\_\_

Date of Implementation: \_\_\_\_\_

Date repealed or replaced: \_\_\_\_\_