

# Procedure: 3.5.1p1.

## Acceptable Computer and Internet Use

**Revised:** January 16, 2018; May 17, 2016; and February 2, 2012.

**Last Reviewed:** May 29, 2024; September 14, 2022; and January 16, 2018.

**Adopted:** October 2, 2003.



### I. PURPOSE:

In making decisions regarding access to the Internet and use of its computers, the System considers its stated educational mission, goals, and objectives. Electronic information research skills are now fundamental to preparing citizens and future employees. Therefore, the System expects faculty to blend thoughtful use of the Internet throughout the curriculum and provide guidance and instruction to students in its use. As much as possible, access from Technical Colleges to Internet resources should be structured to point students to those resources that have been evaluated before use. While students shall be able to move beyond those resources to others that have not been reviewed by staff, they shall be provided with guidelines and lists of resources suited to learning objectives. Students and employees utilizing Technical College-provided Internet access are responsible for good behavior online, just as they are in a classroom or other areas of the college.

Using a computer without permission is theft of services and is illegal under state and federal laws. Federal law prohibits misuse of computer resources. In addition, computer crimes are prohibited by state law in Georgia (O.C.G.A. § 16-9-90 et seq.).

- a) Computer Theft
- b) Computer Trespass
- c) Computer Invasion of Privacy
- d) Computer Forgery

### II. RELATED AUTHORITY:

O.C.G.A. § 20-4-11 – Powers of Board

O.C.G.A. § 20-4-14 – TCSG Established; Powers and Duties

### III. APPLICABILITY:

All work units and Technical Colleges are associated with the Technical College System of Georgia.

### IV. DEFINITIONS:

**Computer Theft:** (including theft of computer services, intellectual property such as copyrighted material, and any other property).

**Computer Trespass:** unauthorized use of computers to delete or alter data or interfere with others' usage.

**Computer Invasion of Privacy:** unauthorized access to financial or personal data or the like.

**Computer Forgery:** forgery as defined by other laws but committed on a computer rather than paper.

**Computer Password Disclosure:** unauthorized disclosure of a password resulting in damages exceeding \$500 - in practice, this includes any disclosure that requires a system security audit afterward.

**Misleading Transmittal of Names or Trademarks:** falsely identifying yourself or falsely claiming to speak for a person or organization by using their name, trademark, logo, or seal.

**Malware:** malicious software programs and applications designed to damage or cause other unwanted actions on a computer system.

## **V. ATTACHMENTS:**

Attachment: 3.5.1p1.a1 TCSG Information Security Standards

## **VI. PROCEDURE:**

The purpose of Technical College-provided computers, computer systems, and Internet access is to facilitate skills development and enhance communication in support of research, education, and workforce development. To remain eligible as users, employees' and students' use must support and be consistent with the System's objectives. Access is a privilege, not a right. Access entails responsibility.

Users should not expect files stored on System or Technical College-based computers or hosted services to be private. Electronic messages and files stored on Technical College-based computers shall be treated like other Technical College premises that are temporarily assigned for individual use. Administrators may review files and messages to maintain system integrity and ensure that users act responsibly. Moreover, System and Technical College officials are expected to cooperate with law enforcement officials authorized to search System and Technical College computers and computer systems.

All information created, stored, or transmitted by System or Technical College computers or networks is subject to monitoring for compliance with applicable laws and policies.

In addition to the computer crimes delineated in O.C.G.A. 16-9-93, the following uses of System or Technical College-provided computers, networks, and Internet access are not permitted:

- a. To create, access, or transmit sexually explicit, obscene, or pornographic material.
- b. To create, access, or transmit material that could be considered unlawful conduct based on race, color, creed, national or ethnic origin, gender, religion, disability, age, genetic information, political affirmation or belief, disabled veteran, a veteran of the Vietnam Era or citizenship status addressed directly to any individual or group that has the purpose or effect of unreasonably and

objectively interfering with that individual or group's: (1) performance, (2) work or educational environment, or (3) ability to participate in an educational program or activity

c. To violate any local, state, or federal statute.

d. To vandalize, damage, or disable the property of another individual or organization.

e. Access another individual's password, materials, information, or files without permission.

f. To violate copyright or otherwise use the intellectual property of another individual or organization violates the law, including software piracy.

g. To conduct private or personal for-profit activities. This includes use for private purposes such as business transactions, private advertising of products or services, and any activity meant to foster personal gain.

h. To knowingly endanger the security of any System or Technical College computer or network.

i. To willfully interfere with another's authorized computer usage.

j. To knowingly connect any computer to any of the System or Technical College networks unless it meets technical and security standards set by the System.

k. To create, install, or knowingly distribute a computer virus, rootkit, keystroke logger, "Trojan horse," "Malware," or other surreptitiously destructive programs on any System or Technical College computer or network facility, regardless of whether any demonstrable harm results.

l. To modify or reconfigure the software or hardware of any Agency computer or Network without proper authorization.

m. To conduct unauthorized not-for-profit business activities.

n. To conduct any activity or solicitation for political or religious causes.

o. To perform any activity that could cause the loss, corruption of, prevention of rightful access to, or unauthorized distribution of Agency data and information.

p. To create, access, or participate in online gambling. Occasional access to information or websites of the Georgia Lottery Corporation shall not constitute nor be considered inappropriate use.

q. To capture and/or record network traffic without authorization.

r. To knowingly transmit copyrighted material using peer-to-peer file sharing technology.

s. To knowingly evade Internet content filtering or other traffic monitoring tools using VPN, Proxy Services, Tor, or similar technologies.

Occasional personal use of Internet connectivity and e-mail that does not involve inappropriate use as described above may occur if the college permits. However, any such use

should be brief and infrequent and shall not interfere with the User's performance, duties, and responsibilities.

Users of System and Technical College computers and computer systems are subject to the System's policy on the development of Intellectual Property.

Users of System and Technical College computers and computer systems or hosted services are subject to the System's Information Security Standards. The System and Technical Colleges make no warranties, express or implied, for the computers, computer systems, and Internet access. The System and Technical Colleges shall not be responsible for any damages users suffer, including but not limited to data loss resulting from delays or interruptions in service. The System and Technical Colleges shall not be responsible for the accuracy, nature, or quality of information gathered through System or Technical College-based computer hard drives or servers; nor for the accuracy, nature, or quality of information gathered through System or Technical College-provided Internet access. The System and Technical Colleges shall not be responsible for personal property used to access its computers or networks or provided Internet access. The System and Technical Colleges shall not be responsible for unauthorized financial obligations resulting from providing access to the Internet.

The preceding standards are equally applicable to employees of the System, wherever housed, and to employees and students at the Technical Colleges.

### **Penalties**

Violations of these policies incur the same disciplinary measures as violations of other System or Technical College policies or state or federal laws, including criminal prosecution.

### **VII. RECORD RETENTION:**

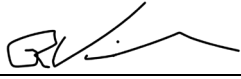
All related documents generated or collected according to this procedure shall be maintained in a manner consistent with the Georgia Archives' Retention Schedule for State Government Paper and Electronic Records

TCSG Information Security Standards  
May 29, 2023

**Approvals**

Last Modified Date: May 29, 2024

Last Modified By: Darrell Carter

Approved By:   
Robbie Vickers, CIO

Technical College System of Georgia Information Security Standards Contents

Table of Contents

I. **PURPOSE:**.....1

II. **RELATED AUTHORITY:**.....1

III. **APPLICABILITY:** .....1

IV. **DEFINITIONS:**.....1

V. **ATTACHMENTS:** .....2

VI. **PROCEDURE:** .....2

**Penalties** .....1

**TCSG Information Security Standards May 29, 2023**.....2

**Information Security Administrator Standards (ISS-00)**.....5

**Publicly Accessible Server Standards (ISS-01)** .....6

**User ID and Password Standards (ISS-03)**.....10

    d. **Level 1: System Level User** .....11

    e. **Level 2: Secure Application User** .....11

    f. **Level 3: User**.....11

    g. **Level 4: Student User**.....11

    h. **Level 5: Temporary User**.....11

**Student Records Server Standards (ISS-04)**.....13

**Definition of Student Records RDBMS Server(s): The host(s) that house(s) the Non-Encrypted Banner RDBMS Data.** .....13

**All Student Records RDBMS Servers are subject to the Publicly Accessible Server Standards (ISS-01) and User ID and Password Standards (ISS-03) as well as the following:**.....13

**Internet Access Filtering / Email Filtering Standards (ISS-05)**.....14

**Minimum Web Filter Category Blocking Standards for all TCSG sites per TCSG Procedure 3.3.4p – Acceptable Computer and Internet Use Excerpt from TCSG Procedure 3.3.4p Acceptable Computer and Internet Use (ISS-05a)**.....16

**Portable Storage and Transmittal of Confidential Information Standards (ISS-06)** .....19

**Use of Personal Mobile Devices (PMD) for Business Communications Standards (ISS-06a)** .....20

**Personal Mobile Device for Business Communications Terms of Use (ISS-06a.1)**.....22

**External Network Connection Standards (ISS-07)** .....23

**Secure Internal Network Design Standards (ISS-08)** .....24

**Secure Remote Access Standards (ISS-09)**.....25

**Computer Security Event and Incident Handling Steps for College IT Personnel (ISS-10a)** .....26

**Examples of Computer Security Events\*** .....26

**Examples of Computer Security Incidents\*** .....26

**Computer Security Event and Incident Handling Steps for College IT Personnel**.....27

**Purpose of the Computer Security Event and Incident Handling Steps for College IT Personnel: To provide TCSG IT personnel with a list of the steps that must be taken in the event of a suspected or confirmed computer security event or incident.** .....27

**Computer Security Event and Incident Handling Steps for College Personnel (ISS-10b)**.....28

**Examples of Computer Security Events\*** .....28

**Examples of Computer Security Incidents\*** .....28

**Computer Security Event and Incident Handling Steps for College Personnel** .....29

**Purpose of the Computer Security Event and Incident Handling Steps for College Personnel: To provide TCSG personnel with a list of the steps that must be taken in the event of a suspected or confirmed computer security event or incident.** .....29

**Computer Security Event and Incident Handling Steps for System Office Personnel** .....30

**Purpose of the Computer Security Event and Incident Handling Steps for System Office Personnel: To provide TCSG personnel with a list of the steps that must be taken in the event**

of a suspected or confirmed computer security event or incident.....	30
<b>Business (Non-Student) Email Archiving, Retention and Investigation Standards (ISS-11)</b> .....	<b>31</b>
I. <b>PURPOSE:</b> .....	31
II. <b>RELATED AUTHORITY:</b> .....	31
III. <b>APPLICABILITY:</b> .....	31
V. <b>ATTACHMENTS: N/A</b> .....	31
VII. <b>RECORD RETENTION:</b> .....	33
<b>HEOA P2P Unauthorized File Sharing Prevention Compliance Standards (ISS-12)</b> .....	<b>34</b>
I. <b>PURPOSE:</b> .....	34
II. <b>RELATED AUTHORITY:</b> .....	34
III. <b>APPLICABILITY:</b> .....	34
IV. <b>DEFINITIONS:</b> .....	34
V. <b>ATTACHMENTS:</b> .....	34
VI. <b>PROCEDURE:</b> .....	34
VII. <b>RECORD RETENTION:</b> .....	35
<b>Unauthorized Distribution of Copyrighted Materials is Against Federal Law</b> .....	35
<b>Summary of Civil and Criminal Penalties for Violation of Federal Copyright Laws</b> .....	35
<b>Unauthorized Distribution of Copyrighted Materials is Prohibited by TCSG Policy</b> .....	36
<b>PCI Compliance Standards (ISS-13)</b> .....	<b>37</b>
<b>Definition of PCI Compliance: All systems and networks that touch or store cardholder data must meet the security criteria set forth by the Payment Card Industry Data Security Standard (PCI DSS)</b> .....	<b>37</b>
<b>Protection of Personally Identifiable Information (PII) (ISS-14)</b> .....	<b>39</b>
<b>Definition of Personally Identifiable Information (PII): Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. Examples include direct references such as name, address, social security number, and e-mail address. PII also includes any information that could be used to reference other data elements that are used for identification, such as gender, race, and date of birth.</b> .....	<b>39</b>
<b>2. Social Security Numbers (SSNs), including truncated SSNs that include only the last four digits, are sensitive regardless of whether they are associated with an individual. If it is determined that such transmission is required, then secure methods must be employed.</b> .....	<b>39</b>
<b>Red Flags Rule (RFR) (ISS-15)</b> .....	<b>41</b>
<b>Red Flags Rule (RFR) Examples (ISS-15a)</b> .....	<b>42</b>
<b>RED FLAGS RULE – Examples of things that should raise 'RED FLAGS' Suspicious Documents Sometimes paperwork has the telltale signs of identity theft.</b> .....	<b>42</b>
<b>Suspicious Personally Identifying Information</b> .....	<b>42</b>
<b>Suspicious Account Activity</b> .....	<b>42</b>
<b>Personal Electronic Devices (PED) (ISS-16)</b> .....	<b>43</b>
<b>HIPAA Compliance (ISS-17)</b> .....	<b>44</b>
<b>Publicly Accessible Server Vulnerability Assessment Standard (ISS-18)</b> .....	<b>45</b>
<b>Cyber Security Awareness Training Standard (ISS-19)</b> .....	<b>46</b>
<b>Cyber Security Risk Management Framework Standard (ISS-20)</b> .....	<b>47</b>
<b>IT System Maintenance Standards (ISS-21)</b> .....	<b>49</b>
<b>Malicious Code Detection and Prevention Standard (ISS-22)</b> .....	<b>50</b>
<b>Physical Security and Access Control Standards (ISS-23)</b> .....	<b>51</b>

**Information Security Administrator Standards (ISS-00)**

**Definition of Information Security Administrator (ISA):** The person responsible for implementation and enforcement of TCSG and College Information Security Policies, Standards and Best Practices. This person is the single point of contact for the College for issues involving Information Security.

**Purpose of these Standards:** The purpose of these Standards is to outline the requirements for and responsibilities of the College Information Security Administrator.

1. The College ISA must be a full-time employee of TCSG or its affiliate College.
2. The College ISA must be approved by the TCSG Information Security Officer (ISO).
3. The College ISA must attend all mandatory meetings and training sessions as defined by the TCSG ISO.
4. The College ISA is the single point of contact for all issues involving Information Security and is accountable to the TCSG ISO for Information Security for the College.
5. To facilitate rapid response to security events, the College ISA is required to provide 24-hour emergency contact information to the TCSG ISO.
6. The College ISA has the responsibility and the authority to implement and enforce Federal, State, TCSG and College Information Security Policies, Standards and Best Practices.
7. The College ISA is ultimately responsible for the security of Campus information assets and has the authority to define and control access to all College Information Systems.
8. These Standards will be revised based on changing Information Security requirements.



**Publicly Accessible Server Standards (ISS-01)**

**Definition of Publicly Accessible Server:** Any server that is accessible via any network external to the Campus' local area network or that resides in a subscribed cloud environment.

**Definition of Critical Server:** Any server that is essential to the business operation and communication. Examples include but are not limited to web, email, and intranet servers.

**Purpose of these Standards:** The purpose of these Standards is to ensure a high level of security for publicly accessible servers housed at TCSG sites or subscribed cloud platforms by providing a mechanism for control and accountability for the security of these resources.

1. Servers must be physically located in a secure, climate-controlled data center.
2. Physical access to the data center must be limited to authorized personnel and logged, either electronically or manually.
3. Adequate backup power systems must be provided to assure continued operation, or at least a graceful shutdown of equipment in case of power failure.
4. Critical servers must be backed up on a daily basis and backups maintained for at least five weeks. For DR/COB purposes weekly backups must be stored or securely copied to an off-site facility.
5. Server operating systems and application software must be TCSG approved, properly licensed, and kept at current update/patch levels.
6. Server must be protected from external networks by a stateful firewall device managed by TCSG and the TCSG approved and trained College Information Security Administrator.
7. Only approved and necessary service ports will be allowed access to /from the public network. A deny all except explicitly allowed policy will be enforced for traffic both inbound and outbound from the public network to and from the server.
8. To the greatest extent possible granularity of services must be enforced. A publicly accessible web server, for example, should never house shares for internal user data. Publicly accessible servers should never be domain controllers for internal domains or house sensitive data that is not required for the public-access purpose of the server.
9. Only required services should be enabled on the server. All services not required for the specified purpose of the server should be disabled.
10. Server must be protected by an anti-malware product with current signatures.
11. Campus Information Security Administrators are responsible for implementing TCSG mandated security policies and Standards.
12. TCSG approved and trained Information Security Administrator for College is ultimately responsible for security of every server accessible from off campus to include those in a

subscribed cloud environment. TCSG and the College ISA have authority over all security related aspects for servers. College ISA will be granted administrative rights to all publicly accessible servers for audit purposes.

13. If a publicly accessible system and/or content is managed by a person outside of the College IT Staff, they may be designated as the *Responsible Party* for this system. The *Responsible Party* is responsible for the day-to-day maintenance of security patches, anti-malware updates, and other ongoing security-related operations for the server. The *Responsible Party* must maintain compliance with all TCSG and College security policies and will work with the College Information Security Administrator to assure compliance.
14. Periodic security audits will be performed by College ISA and TCSG personnel to assure compliance with stated information security policies and Standards.
15. These Standards will be revised based on changing information security requirements.

## Public Network Connection / Firewall Standards (ISS-02)

**Definition of Public Network Connection:** A network connection that allows traffic to flow between any Campus LAN and the Internet Service Provider network.

**Definition of Necessary Service Ports:** Communication endpoints required by the host system to support the functions of the end user network processes and services it is intended to support.

**Purpose of these Standards:** The purpose of these Standards is to ensure a high level of security for local area networks serving TCSG sites by providing a mechanism for control and accountability for the flow of network traffic between TCSG sites and the public network (Internet).

1. Any connection to/from the public network will be protected by a stateful firewall device.
2. Only approved and necessary service ports will be allowed access to/from the public network. A deny all except explicitly allowed policy will be enforced for traffic both inbound and outbound from the public network.
  - a. Example of a necessary service port: Web Application should have TCP/80 and TCP/443 available to access the end user application from a public network connection. However, management ports for this same server should not be accessible from a public network connection.
3. Current firewall configurations must be backed up to a separate media whenever updates are performed to provide for recovery in case of device failure.
4. Firewall configurations and rule sets are confidential and may not be shared with those not directly involved in the management of the firewall.
5. Firewalls will be managed by TCSG and the TCSG approved and trained College Information Security Administrator. Access to any perimeter security device by anyone other than the TCSG or College employee approved by the TCSG ISO is prohibited.
6. Remote management passwords must not contain dictionary words and must include upper- and lower-case letters, numbers, and special characters. Minimum length is 16 characters.
7. Remote management on the public network interface of the firewall must be via encrypted session such as SSH. SSH connections to the public interface may only originate from TCSG subnets (72.162.0.0 255.255.0.0).
8. Debug level logging to a separate syslog server must be enabled on the firewall. Logs must be retained for a minimum of 90 days. One-year retention is desirable if feasible.
9. Firewall Operating Systems must be kept at the approved release level in keeping with TCSG update notifications and schedules.

10. Rule sets should be documented as to purpose for each permission granted for inbound or outbound traffic. All changes to rule sets should be documented and retained for problem resolution purposes.
11. Campus Information Security Administrators are responsible for implementing TCSG mandated security policies and Standards.
12. TCSG approved and trained Information Security Administrator for College is ultimately responsible for types of traffic allowed in and out of the campus network. TCSG and the College ISA have authority to permit or deny any traffic to or from the campus network.
13. The “standard” firewall devices to be used by TCSG sites is the Cisco Firepower Appliance, Cisco ASA, and Palo Alto platforms. TCSG support for non-standard devices may be limited. In cases where TCSG Information Security deems the device in use is inappropriate, TCSG retains the right to require replacement of the device with an approved device.
14. Periodic security audits will be performed by College ISA and TCSG personnel using appropriate tool sets to assure compliance with stated information security policies.
15. These Standards will be revised based on changing information security requirements.

**Definition of User ID/Password:** The unique combination of login credentials that identifies a specific piece of equipment or individual user.

**Definition of Two-step Verification or Two-step Authentication:** The method of requiring the users to confirm their identity by utilizing something they know, like a password, and then utilizing some sort of out-of-band mechanism like a one-time-password generator, Authenticator App on their phone, phone call, SMS message, or Campus location.

**Definition of Passphrase:** Passphrases are defined as being a phrase, sentence or other group of words used in place of a standard password.

Purpose of these Standards: The purpose of these Standards is to ensure a high level of security for local area networks and subscribed cloud environments serving TCSG sites by providing a mechanism for control and accountability for access to the local area network, attached resources, cloud services, and the internet via user authentication with a unique user ID and password.

1. Any device which allows a user to connect to the campus network is defined as a point of network access. All points of network access must be protected by a user ID and password to prevent unauthorized network access.
2. Use of generic logins (multiple users using same user ID/password) is prohibited except for specific approved situations approved by the College ISA as defined in ISS-00 or the TCSG Information Security Officer, as accountability and audit ability are severely compromised. Generic logins may only be used for specific, limited time applications, and distribution of the login credentials will be limited to persons authorized for specific applications. Passwords for generic logins should rotate on a periodic basis as set by the College ISA.
3. The combination of Passwords and User IDs are confidential and must be protected. Sharing of login credentials or logging on using another user's login credentials is prohibited and may result in disciplinary action.
4. Maximum password life for TCSG employees is 42 days unless some other technical control is in place. If an additional technical control, like Two-Step Verification, is in place, then the password life can be extended to a maximum of 120 days.
5. Previously used passwords cannot be re-used.
6. Passwords may be assigned to users by the College ISA or his/her designee.
7. Initial passwords or password changes by the College ISA or his/her designee should require a password change on first login except for Level 5 Temporary User accounts. If there is a technical option that will perform this operation it is preferred over relying on the user to change the password.

8. All passwords are required to adhere to the following rules, subject to operating system/application limitations:
- a. Complexity requirements for passwords are based on five levels of user access. Level 1 is the most stringent, and level 5 is the least stringent. If you are unsure as to what level password requirements you must meet, please check with the College ISA for clarification. TCSG Central Office/QuickStart office users will follow Level 2 requirements.
  - b. Level 1, 2, and 3 users should have Two-Step or Multi-factor Authentication enabled.
  - c. It is recommended that Level 4 users have Two-Step or Multi-factor Authentication enabled.
  - d. **Level 1: System Level User**
    - i. All network devices, local machine administrator, and service accounts require Level 1 passwords.
    - ii. 16-character minimum and must include:
      1. Upper case: A-Z
      2. Lower case: a-z
      3. Numbers: 0-9
      4. Special characters: ~!@#\$\$%^&\*()\_+={}|?><.,;
  - e. **Level 2: Secure Application User**
    - i. Secure Applications consist of applications that access sensitive protected data as defined in ISS-14
    - ii. 14-character minimum and must include 3 of the 4:
      1. Upper case: A-Z
      2. Lower case: a-z
      3. Numbers: 0-9
      4. Special characters: ~!@#\$\$%^&\*()\_+={}|?><.,;
  - f. **Level 3: User**
    - i. All other users not listed in this Standard.
    - ii. 8-character minimum and must include 3 of the 4 following items:
      1. Upper case: A-Z
      2. Lower case: a-z
      3. Numbers: 0-9
      4. Special characters: ~!@#\$\$%^&\*()\_+={}|?><.,;
  - g. **Level 4: Student User**
    - i. For colleges using Single Sign On for Student Users.
    - ii. These users can be for students in any departments at the colleges.
    - iii. 8-character minimum and must include 3 of the 4 following items:
      1. Upper case: A-Z
      2. Lower case: a-z
      3. Numbers: 0-9
      4. Special chars: ~!@#\$\$%^&\*()\_+={}|?><.,;
      5. Initial password must be unique and not contain the college name.
  - h. **Level 5: Temporary User**
    - i. Accounts should be removed once user access is no longer needed.
    - ii. 8-character minimum

9. The use of passwords is exempt where SSH public key authentication is an option.
  - a. The minimum requirements to qualify for the exception would be the following:
    - i. SSH password authentication for that user would have to be disabled.
    - ii. The private key type and length would have to be a minimum of an RSA key with a 4096-bit length or a ECDSA key with a 256-bit length.
    - iii. The key pair would need to be rotated every 12 months.
10. Upon the termination, separation or re-assignment of an administrative user with access to non-expiring privileged system account passwords, those passwords must be changed within 5 business days of the termination/separation. Only the passwords known by the terminated/separated administrative user must be changed.
  - a. The affected privileged system accounts are:
    - i. Linux - root
    - ii. Oracle & Banner - Any user account assigned the DBA role that also has a non-expiring password.
    - iii. Active Directory – Any Administrator accounts known to the user.
    - iv. Cisco Equipment – Firewall and Switch login passwords.
11. The College Information Security Administrators shall develop a procedure to remove accounts that are no longer required.
12. College Information Security Administrators are responsible for implementing TCSG-mandated security policies and standards.
13. The College Information Security Administrator as defined in ISS-00 is ultimately responsible for implementing password standards. TCSG and the College ISA have authority to permit or deny any user access to network and network-attached resources.
14. These standards represent minimum requirements. Users are encouraged to use more complex passwords and passphrases and to change passwords more frequently. Use of passphrases or the first characters of words in phrases are encouraged. Substitution of special characters for letters in the body of the password is encouraged. When possible, use of non-ASCII standard characters is encouraged.
15. Periodic security audits will be performed by College ISA and TCSG personnel to assure compliance with stated information security policies. User accounts found not to be in compliance may be disabled until proper passwords are implemented or assigned.
16. These standards will be reviewed annually and revised as necessary based on changing information security requirements.

## Student Records Server Standards (ISS-04)

Definition of Student Records RDBMS Server(s): The host(s) that house(s) the Non-Encrypted Banner RDBMS Data.

**Purpose of these Standards:** The purpose of these Standards is to ensure a high level of security for Student Records servers housed at TCSG sites by providing a mechanism for control and accountability for the security of these resources.

All Student Records RDBMS Servers are subject to the Publicly Accessible Server Standards (ISS-01) and User ID and Password Standards (ISS-03) as well as the following:

1. Student Records RDBMS servers will be connected to a secure, access-controlled network segment which is accessible only by the Banner Application Servers and specified administrative personnel. Direct access to this network segment from outside the college LAN is prohibited except via on-demand VPN for TCSG ES, TCSG MS, and TCSG DC access.
2. The RDBMS host may not provide any auxiliary services that require connections originating from hosts other than hosts listed in part 1.
3. Banner databases not housed on the current production RDBMS (ex: on or off-site backup) must be encrypted by the method specified by the TCSG DBA.
4. SSH is required for all remote terminal sessions, including those initiated on the local campus network. Clear text telnet will be disabled on all Student Records (RDBMS) servers.
5. Logging of all login and file access must be enabled with logs stored on separate logging hosts. Minimum storage period is 90 days
6. Direct root login from non-console sessions is not allowed. Intermediate initial login with non-privileged account is required for remote sessions.
7. All browser-based access to Student Records (Banner) server services must utilize encrypted (SSL) communications.
8. All data gathered from Student Records (Banner) databases must be treated with the appropriate level of confidentiality. Information not intended for public dissemination will not be stored in areas accessible by non-authorized personnel.
9. Access to Banner Data by third party (non-Banner) processes or tools must use unique, documented, auditable accounts created for that purpose. Banner or Oracle internal users (ex: saisusr, saturn, system, etc.) may NOT be used.
10. Third-party tools such as Cold Fusion may NOT be used to modify production databases on Student Records (Banner) Servers.
11. These Standards will be revised based on changing information security requirements.



**Definition of Web Access Filtering:** The use of a product that provides a mechanism for the enforcement of Agency policy regarding web usage from Agency Sites.

**Definition of Email Filtering:** The use of a product that provides a mechanism or the enforcement of Agency policy regarding the appropriate use of email.

**Purpose of these Standards:** The purpose of these Standards is to ensure compliance with Agency policies pertaining to the acceptable use of Agency resources for World Wide Web and email access.

1. All access to the World Wide Web from Agency sites will be filtered through an approved web\URL filtering system.
2. Access to sites prohibited by the TCSG Procedure 3.3.4p Acceptable Computer and Internet Use will be blocked. The minimum blocking standards for Policy adherence are defined by the Minimum Web Filter Category Blocking Standards, ISS-05a. Colleges may, at their discretion, enforce additional filtering rules.
3. All non-student email to and from college email systems will be filtered through an approved email filtering service.
4. Keyword-based filtering of email will be utilized to ensure compliance with TCSG Procedure 3.3.4p Acceptable Computer and Internet Use. Colleges may, at their discretion, enforce additional filtering rules.
5. The College ISA is responsible for the proper operation and maintenance of WWW and email filtering devices. Access to any perimeter security device by anyone other than the TCSG or College employee approved by the TCSG ISO is prohibited.
6. College Information Security Administrators are responsible for implementing TCSG mandated security policies and Standards.
7. TCSG approved and trained Information Security Administrator for the college is ultimately responsible for types of traffic allowed in and out of the campus network. TCSG and the College ISA have authority to permit or deny any traffic to or from the campus network.
8. Periodic security audits will be performed by College ISA and TCSG personnel using appropriate tool sets to assure compliance with stated information security policies and Standards.
9. These Standards will be revised based on changing information security requirements.
10. The "standard" web filtering system device to be used by TCSG sites is the Cisco Firepower platform. TCSG's support for non-standard systems may be limited. In cases where TCSG Information Security deems the system in use inappropriate, TCSG retains the right to require replacement of the system with an approved system.
11. The "standard" email filtering systems to be used by TCSG sites is Cisco Email Security and the Office 365 spam filtering platform. TCSG support for non-standard systems may be limited. In cases where TCSG Information Security deems the system in use

inappropriate, TCSG retains the right to require replacement of the system with an approved system.

Technical College System of Georgia

Minimum Web Filter Category Blocking Standards for all TCSG sites per TCSG Procedure 3.3.4p – Acceptable Computer and Internet Use Excerpt from TCSG Procedure 3.3.4p Acceptable Computer and Internet Use (ISS-05a)

[Procedure: 3.3.4p Acceptable Computer and Internet Use](#)

...

The following uses of System or technical college-provided computers, networks and Internet access are not permitted:

- a. To create, access or transmit sexually explicit, obscene, or pornographic material;
- b. To create, access or transmit material that could be considered unlawful conduct based on race, color, creed, national or ethnic origin, gender, religion, disability, age, genetic information, political affirmation or belief, disabled veteran, veteran of the Vietnam Era or citizenship status addressed directly to any individual or group that has the purpose or effect of unreasonably and objectively interfering with that individual or group's: (1) performance, (2) work or educational environment or (3) ability to participate in an educational program or activity;
- c. To violate any local, state or federal statute;
- d. To vandalize, damage, or disable the property of another individual or organization;
- e. To access another individual's password, materials, information, or files without permission;
- f. To violate copyright or otherwise use the intellectual property of another individual or organization in violation of the law, including software piracy;
- g. To conduct private or personal for-profit activities. This includes use for private purposes such as business transactions, private advertising of products or services, and any activity meant to foster personal gain;
- h. To knowingly endanger the security of any System or technical college computer or network;
- i. To willfully interfere with another's authorized computer usage;
- j. To connect any computer to any of the System or technical college networks unless it meets technical and security standards set by the System;
- k. To create, install, or knowingly distribute a computer virus, rootkit, keystroke logger, "Trojan horse," "Malware", or other surreptitiously destructive program on any System or Technical College computer or network facility, regardless of whether any demonstrable harm results;
- l. To modify or reconfigure the software or hardware of any Agency computer or Network without proper authorization;
- m. To conduct unauthorized not-for-profit business activities;
- n. To conduct any activity or solicitation for political or religious causes;

- o. To perform any activity that could cause the loss, corruption of, prevention of rightful access to, or unauthorized distribution of Agency data and information;
- p. To create, access, or participate in online gambling. Occasional access to information or websites of the Georgia Lottery Corporation shall not constitute nor be considered inappropriate use;
- q. To capture and/or record network traffic without authorization;
- r. To knowingly transmit copyrighted material using peer to peer file sharing technology;
- s. To knowingly evade Internet content filtering or other traffic monitoring tools using VPN, Proxy Services, Tor or similar technologies;

The foregoing standards are equally applicable to employees of the department, wherever housed, and to employees and students of the Technical College.

1. In compliance with prohibited activities under subsections a and b of TCSG Procedure 3.3.4p the access to sites in the following Web Filter categories will be blocked at all TCSG locations:
  - a. Adult Material
  - b. Adult Content - Sites featuring full or partial nudity reflecting or establishing a sexually oriented context, but not sexual activity
  - c. Adult and Pornography
2. Sex – Sites depicting or graphically describing sexual acts or activity, including exhibitionism in compliance with prohibited activities under subsection of c of TCSG Procedure 3.3.4p the access to sites in the following Web Filter category will be blocked at all TCSG locations:
  - a. Gambling – Sites that provide information about or promote gambling or that support online gambling. Risk of losing money possible. The State of Georgia does not consider occasional visits to the Georgia Lottery site to be gambling. [www.galottery.com](http://www.galottery.com) should be allowed.
3. To maintain compliance with all actives under the subsections of TCSG Procedure 3.3.4p the access to sites in the following Web Filter categories will be blocked at all TCSG locations:
  - a. Bot Nets
  - b. Confirmed SPAM Sources
  - c. Malware Sites
  - d. Proxy Avoid and Anonymizers
  - e. SPAM URLS
  - f. Spyware and Adware
4. In compliance with prohibited activities under subsection of s of TCSG Procedure 3.3.4p the access to sites and services in the following Web Filter and Application categories will be blocked at all TCSG Locations:
  - a. High Risk VPN/tunnel
  - b. TOR Services

c. Proxy Avoid and Anonymizers

5. Due to the potential for copyright infringement the following protocols will be blocked at all TCSG locations:
  - a. Peer to Peer File Sharing
  - b. It is permissible to allow (whitelist) P2P to/from specific sites required for instructional purposes
6. These requirements are MINIMUM requirements. Additional filtering based on locally determined criteria may be invoked at the Colleges' discretion.
7. All web access is logged and is subject to review.
8. All internet activity is logged, monitored, and subject to review and publication
9. These Standards will be revised based on changing information security requirements

## **Portable Storage and Transmittal of Confidential Information Standards (ISS-06)**

**Definition of Portable Storage and Transmittal:** Portable storage is defined as any storage medium that is not a fixed internal hard disk drive mounted inside a non-portable computer system. Transmittal is the electronic transfer of information beyond the College's local area network or subscribed cloud environment by any means other than portable storage devices.

**Purpose of these Standards:** The purpose of these Standards is to ensure that information not meant for public dissemination is protected when it is transmitted to/from or stored on any portable media storage or other electronic device.

1. Information not intended for public dissemination that is stored on any type of portable media or device must be encrypted. This includes information stored on, but not limited to, portable computers, PDAs, Blackberry devices, smartphones, CDs, DVDs, Flash Memory Devices (thumb drives), Zip discs, and diskettes. Information not intended for public dissemination that exists in any electronic form stored anywhere other than on a non-portable computer located at a TCSG site must be encrypted. Backup media approved by the College ISA is exempt from the encryption requirement if it is stored in a secure location approved by the College ISA. If unencrypted backup media is transported off-site, it must be secured both in transit and storage in a manner approved by the College ISA.
2. Information not intended for public dissemination which is electronically transmitted outside the local campus LAN by any electronic means must be encrypted. This includes, but is not limited to, email, FTP, HTTP/HTTPS, and any other electronic data transfer method.
3. All transmission of email to portable devices such as smartphone devices must be encrypted. No clear text transmission of email to any portable device is permitted. Non-encrypted text messaging of information not intended for public dissemination is prohibited.
4. Users of portable communication devices are responsible for not using these devices for the transmission of information not intended for public dissemination.
5. These Standards will be revised based on changing information security requirements.

## Use of Personal Mobile Devices (PMD) for Business Communications Standards (ISS-06a)

**Definition of Personal Mobile Devices (PMD):** Any portable electronic device capable of sending and receiving email and/or accessing business data via wireless or cellular connection that is owned by a user or by the College.

**Definition of Business Communications:** Any email, data or other communications transmitted to or from TCSG systems or subscribed cloud services. Also includes any other business-related communications regardless of source, destination or technology.

1. TCSG strongly encourages all affiliates to use access management applications to encrypt and manage remote device email and data services for all PMD users. This product meets all TCSG security requirements while keeping corporate mail separate from the user's personal data and allows selective application of security policy to business applications and data only.
2. Business email, data and other communications are the property of TCSG and its affiliates regardless of where they are stored.
3. Any personal mobile device used for business communications is subject to search and/or seizure in the event of a legal requirement for such.
4. There is no guarantee or expectation of privacy for any communications or data (personal or otherwise) stored on a PMD used for business communications.
5. Any personal mobile device used for business communications is subject to remote wipe of all device contents in case of loss, theft, or if the business data contained therein is considered at risk.
6. TCSG personnel are responsible for securing their devices to prevent non-public data from being lost or compromised. Unencrypted sensitive PII should never be transmitted via PMD.
7. Any personal mobile device used for business communications must be password, pattern or PIN protected at all times when not in use.
8. If supported by the device, when the password, pattern or PIN is incorrectly entered ten times the device must reset to factory defaults (all data erased).
9. If supported by the device, encryption must be enabled.
10. TCSG personnel must abide by all municipal, state and federal laws pertaining to the use of personal mobile devices.
11. Loss or theft of a PMD used for business communications must immediately be reported to your Information Security Officer or Administrator. The ISO/ISA or their designee will assist the user

in remotely wiping their device using appropriate software or management applications. If the device cannot be remotely wiped the user must immediately notify their carrier and request that the device be wiped clean and disabled.

12. All TCSG employees that use PMDs for business communications must agree to and sign the PMD for Business Communications Terms of Use document (ISS-06a.1), which will be kept in the employee's personnel file.

13. These Standards will be revised based on changing information security requirements.



Technical College System of Georgia

Personal Mobile Device for Business Communications Terms of Use (ISS-06a.1)

Business email, data and other communications are the property of TCSG and its affiliates regardless of where they are stored.

Any personal mobile device used for business communications is subject to search and/or seizure in the event of a legal requirement for such.

There is no guarantee or expectation of privacy for any communications or data (personal or otherwise) stored on a PMD used for business communications.

Any personal mobile device used for business communications is subject to remote wipe of all device contents in case of loss, theft, or if the business data contained therein is considered at risk.

TCSG personnel are responsible for securing their devices to prevent non-public data from being lost or compromised. Unencrypted sensitive PII should never be transmitted via PMD.

Any personal mobile device used for business communications must be password, pattern or PIN protected at all times when not in use.

If supported by the device, when the password, pattern or PIN is incorrectly entered ten times the device must reset to factory defaults (all data erased).

If supported by the device, encryption must be enabled.

TCSG personnel must abide by all municipal, state and federal laws pertaining to the use of personal mobile devices.

Loss or theft of a PMD used for business communications must immediately be reported to your Information Security Officer or Administrator. The ISO/ISA or their designee will assist the user in remotely wiping their device using OWA tools or a third-party application such as Android Lost. If the device cannot be remotely wiped the user must immediately notify their carrier and request that the device be wiped clean and disabled.

I understand and agree to the above. I also understand that refusal to abide by the above rules can result in disciplinary action and a revocation of user privileges.

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Technical College System of Georgia

**External Network Connection Standards (ISS-07)**

**Definition of External Network Connection:** Any connection to a network outside the College's local area network is defined as an External Network Connection

**Purpose of these Standards:** To ensure the security and availability of strategic TCSG network infrastructure components by prohibiting 'back door' connections into sites connected to the TCSG local area networks and interconnected sites.

1. External TCSG College sites shall have a single internet connection point which is managed by the College IT department. Separate departmental or other internet connections are prohibited unless approved in writing by the TCSG ISO. Redundant internet connection points managed by the College IT department are allowed if approved by TCSG.
2. These Standards will be revised based on changing information security requirements.

**Secure Internal Network Design Standards (ISS-08)**

**Definition of Secure Internal Network Design:** A local area network that is segmented (VLAN sub-netted) and ACL limited in such a way as to control and minimize traffic flow between subnets and only allow authorized access to subnets housing non-public information is a Secure Internal Network Design.

**Purpose of these Standards:** To protect critical non-public information assets from unauthorized access through network segmentation and flow control.

1. Each SIS RDBMS Server will reside as the only host on an access-controlled subnet.
  - a. Connections to the RDBMS subnet will be ACL limited to the following:
    - i. Banner Application Servers via TCP port 1525.
    - ii. Designated on-campus users who require direct access to the RDBMS to perform their job functions via TCP port 22 utilizing the SSH protocol.
    - iii. The TCSG Data Center via on-demand VPN for report generation.
    - iv. The TCSG Enterprise Support group (Banner) via on-demand VPN from specified hosts.
    - v. Other required systems approved in writing by the TCSG ISO.
    - vi. During system upgrades and maintenance temporary access from specific TCSG subnets via TCP port 22 using the SSH protocol is permitted.
2. Traffic between campus LAN subnets will be ACL limited to the minimum required as determined by the College Information Security Officer
3. These Standards will be revised based on changing information security requirements.

**Secure Remote Access Standards (ISS-09)**

**Definition of Secure Remote Access:** Access from outside the College LAN to internal networks or hosts via encrypted VPN tunnel or other approved tunneling method.

**Purpose of these Standards:** To protect internal networks and hosts from unauthorized access from outside the College LAN while providing a secure method for authorized network or host access.

1. VPN connections from outside the Campus LAN will utilize VPN to the designated Cisco or Palo Alto device or other approved tunneling device as the Campus LAN termination point.
2. VPN Users will be authenticated via the appropriate Campus authentication point, normally the Microsoft Active Directory.
3. IT Support personnel may be granted access to networks and/or hosts determined necessary by the College ISA.
4. For DR/BC purposes, each College must have a plan in place for providing Secure Remote Access for key operational personnel.
5. All VPN access to the Campus LAN must be logged.
6. These Standards will be revised based on changing information security requirements.

## Computer Security Event and Incident Handling Steps for College IT Personnel (ISS-10a)

**Definition of a Computer Security Event:** A computer security event is any observable occurrence which may violate or attempt to circumvent computer security policies, security standards, acceptable use policies or standard computer security practices. Computer security events occur across our system every day. TCSG's layered security model is designed to detect security events and prevent them from becoming computer security Incidents.

### Examples of Computer Security Events\*

A virus or worm is detected and neutralized by anti-virus software. An unauthorized connection attempt is stopped by a firewall.

An unauthorized individual unsuccessfully attempts to log into a secured server. An unsuccessful attempt at unauthorized access to deface a web site.

A USB key, CD-ROM, other portable media or device containing information not intended for public dissemination left in the open in an office is discovered by a coworker and properly secured.

**Definition of Computer Security Incident:** A computer security incident is a computer security event that has been verified to be a violation of computer security policies and/or standards, acceptable use policies or standard computer security practices resulting in significant compromise of the confidentiality, integrity, or availability of TCSG information system(s) and / or data.

### Examples of Computer Security Incidents\*

A verified virus or worm is not detected and spreads across numerous systems on a campus resulting in severely degraded network performance.

A verified unauthorized connection is allowed through a firewall.

An unauthorized login is made to an administrative or student records server resulting in the verified viewing, capture, modification and/or dissemination of information not intended for public dissemination.

A verified successful web site defacement.

A USB key, CD-ROM, other portable media or device containing information not intended for public dissemination is verified to be lost or missing.

\*No event is considered an incident until it is verified as such by College and TCSG information security personnel\*.

## Computer Security Event and Incident Handling Steps for College IT Personnel

Purpose of the Computer Security Event and Incident Handling Steps for College IT Personnel: To provide TCSG IT personnel with a list of the steps that must be taken in the event of a suspected or confirmed computer security event or incident.

1. **Exercise discretion.** Only two terms should be used to define a suspicious occurrence: “event” and “incident”. An event is any observable occurrence, suspicious or not. An event becomes an “incident” only upon validation as such by College and TCSG Information Security personnel. No other terms should be used.

Until an event is researched and validated as an actual incident by the appropriate College and TCSG personnel, discussion of the event should be limited to personnel associated with the investigation of the event.

2. **Immediately notify your College Information Security Administrator.** The College Information Security Administrator will evaluate the event. If upon initial investigation the event is determined or suspected to be an incident, the College ISA will contact the TCSG Information Security Officer to validate the determination of the incident. If the event is validated as an incident the TCSG ISO will notify the TCSG Chief Information Officer and if the event involves Banner or any Student Information Systems (SIS) the TCSG DBA. TCSG personnel will determine if and when it is appropriate to contact outside entities such as law enforcement or local media to prevent inappropriate release of sensitive information.
3. **Document everything.** Every action that is performed, every piece of evidence, every conversation regarding the incident. Record times, dates, methodologies and who was present and/or participating.
4. **Stop the incident** if it is still occurring. For instance, if a system is being compromised it should be removed from the network.
5. **Analyze the evidence** to confirm whether or not an incident has occurred. In conjunction with TCSG personnel the College ISA will perform additional research to determine if the event was a bona fide Computer Security Incident requiring corrective action.
6. **Preserve evidence** from the incident. Make backups (preferably disk image backups, not file system backups) of affected systems. Make copies of all log files and burn to write once optical media.
7. **Reverse effects** of the incident. Restore known good backups or rebuild systems from scratch.
8. **Identify and mitigate** all vulnerabilities that were exploited so that a similar event does not occur again.
9. **Restore systems** to service and check for proper operation, being especially vigilant for any remaining indication of compromise.

## Computer Security Event and Incident Handling Steps for College Personnel (ISS-10b)

**Definition of a Computer Security Event:** A computer security event is any observable occurrence which may violate or attempt to circumvent computer security policies, security standards, acceptable use policies or standard computer security practices. Computer security events occur across our system every day. TCSG's layered security model is designed to detect security Events and prevent them from becoming computer security Incidents.

### Examples of Computer Security Events\*

A virus or worm is detected and neutralized by anti-virus software. An unauthorized connection attempt is stopped by a firewall.

An unauthorized individual unsuccessfully attempts to log into a secured server. An unsuccessful attempt at unauthorized access to deface a web site.

A USB key, CD-ROM, other portable media or device containing information not intended for public dissemination left in the open in an office is discovered by a coworker and properly secured.

**Definition of Computer Security Incident:** A computer security incident is a computer security event that has been verified to be a violation of computer security policies and/or Standards, acceptable use policies or standard computer security practices resulting in significant compromise of the confidentiality, integrity, or availability of TCSG information system(s) and / or data.

### Examples of Computer Security Incidents\*

A verified virus or worm is not detected and spreads across numerous systems on a campus resulting in severely degraded network performance.

A verified unauthorized connection is allowed through a firewall.

An unauthorized login is made to an administrative or student records server resulting in the verified viewing, capture, modification and/or dissemination of information not intended for public dissemination.

A verified successful web site defacement.

A USB key, CD-ROM, other portable media or device containing information not intended for public dissemination is verified to be lost or missing.

\*No event is considered an incident until it is verified as such by College and TCSG information security personnel\*.

## Technical College System of Georgia

### Computer Security Event and Incident Handling Steps for College Personnel

Purpose of the Computer Security Event and Incident Handling Steps for College Personnel: To provide TCSG personnel with a list of the steps that must be taken in the event of a suspected or confirmed computer security event or incident.

1. **Exercise discretion.** Only two terms should be used to define a suspicious occurrence, “event” and “incident”. An event is any observable occurrence, suspicious or not. An event becomes an “incident” only upon validation as such by College and TCSG Information Security personnel. No other terms should be used.
2. Until an event is researched and validated as an actual incident by the appropriate College and TCSG personnel, discussion of the event should be limited to personnel associated with the investigation of the event or incident.
3. **Immediately notify your College Information Security Administrator.** The College Information Security Administrator will evaluate the event. If upon initial investigation the event is determined or suspected to be an incident, the College ISA will contact the TCSG Information Security Officer to validate the determination of the incident. If the event is validated as an incident the TCSG ISO will notify the TCSG Chief Information Officer and if the event involves Banner or any Student Information Systems (SIS) the TCSG DBA. TCSG personnel will determine if and when it is appropriate to contact outside entities such as law enforcement or local media to prevent inappropriate release of sensitive information.
4. **Document the event.** Make note of the time and date, symptoms or indications (what made you aware that something was going on), what applications were running and what specific operations were being performed at the time. Do not turn off systems or perform any operations unless instructed to do so by your College Information Security Administrator.



## Computer Security Event and Incident Handling Steps for System Office Personnel

Purpose of the Computer Security Event and Incident Handling Steps for System Office Personnel: To provide TCSG personnel with a list of the steps that must be taken in the event of a suspected or confirmed computer security event or incident.

1. **Exercise discretion.** Only two terms should be used to define a suspicious occurrence, “event” and “incident”. An event is any observable occurrence, suspicious or not. An event becomes an “incident” only upon validation as such by TCSG Information Security personnel. No other terms should be used.
2. Until an event is researched and validated as an actual incident by the appropriate TCSG personnel, discussion of the event should be limited to personnel associated with the investigation of the event or incident.
3. **Immediately notify your Information Security Administrator.** The Information Security Administrator will evaluate the event. If upon initial investigation the event is determined or suspected to be an incident, the ISA will contact the TCSG Information Security Officer to validate the determination of the incident. If the event is validated as an incident the TCSG ISO will notify the TCSG Chief Information Officer and if the event involves Banner or any Student Information Systems (SIS) the TCSG DBA. TCSG Information security personnel will work with the appropriate executive personnel to determine if and when it is appropriate to contact outside entities such as law enforcement or local media to prevent inappropriate release of sensitive information.
4. **Document the event.** Make note of the time and date, symptoms or indications (what made you aware that something was going on), what applications were running and what specific operations were being performed at the time. Do not turn off systems or perform any operations unless instructed to do so by your College Information Security Administrator.

TCSG System Office order of contact for suspected information security events:

Information Security Administrator:	Jessica Johnson
Information Security Administrator:	Anatoly Rapozo
Information Security Officer:	Darrell Carter
Chief Information Officer:	Robbie Vickers

**Business (Non-Student) Email Archiving, Retention and Investigation Standards (ISS-11)**  
**Procedure 3.3.13p Business Email Archiving, Retention, and Investigation Procedure**

I. **PURPOSE:**

Business email archiving and retention involves storing in an unalterable format for a specified amount of time all electronic messages processed by any TCSG or college email system used for employee business email communications. This procedure sets a standardized searchable storage system for retention and retrieval of all electronic correspondence to, from, or within TCSG/college business email systems in a manner that is consistent with federal requirements.

II. **RELATED AUTHORITY:**

- O.C.G.A. § 20-4-11 – Powers of the Board
- O.C.G.A. § 20-4-14 – TCSG Powers and Duties

III. **APPLICABILITY:**

All work units and technical colleges associated with the Technical College System of Georgia.

IV. **DEFINITIONS:** N/A

V. **ATTACHMENTS:** N/A

VI. **PROCEDURE:**

A. Retention and retrieval system:

1. To meet retention Standards and comply with e-Discovery requirements, every TCSG entity which operates a business email system will implement a TCSG- approved searchable email retention and retrieval system which stores unalterable copies of all email correspondence processed by their business email systems.
2. All employee business email correspondence must utilize the TCSG, Quick Start or college Microsoft O365 email system. This includes all correspondence with students with the exception of broadcast messages to classes sent via an online classroom format.
3. Archived messages will be transported and stored in an encrypted format readable only by TCSG, the college or their designees.
4. The archiving system will allow selected mailboxes to be marked for legal holds providing for storage for an indefinite period of time during legal proceedings (see VI.C. below).
5. The retention period for all email messages not subject to legal holds will be 60 months.

6. All archived messages will be accessible for retrieval for the full retention period, after which they will be purged from the archive.
7. PST file storage and POP3 mail access will be disabled.

#### B. Investigations involving archived messages:

1. Access to messages of other employees for investigative purposes will be achieved by the following:
  - a. Request must be submitted via email to the appropriate Information Security Administrator by a member of the college's senior management team or the System office executive committee. The request must contain the name of the requesting party, the subject and purpose of the investigation.
  - b. If the requesting party is not the Commissioner or College President the ISA will obtain approval via email from the Commissioner/President or his/ her designee prior to providing the information.
  - c. The ISA will notify the local HR Director and the TCSG Information Security Officer that an investigation is underway, the name of the mailbox being investigated, the name of the requestor and the reason for the investigation. The TCSG ISO will notify the TCSG Director of Human Resources.
  - d. The HR Director at the college or TCSG will notify the subject of the investigation that the contents of his/her email account will be investigated.
  - e. A temporary access account will be created with access to the mailbox under investigation. The temporary access account will be deleted once the investigation is completed.

#### C. Litigation holds:

1. Where TCSG or the college is the subject of litigation, there are special requirements related to electronic document retention (including emails).
2. Upon receipt of an ante litem notice, summons, complaint or other notice that TCSG or the college may be the subject of litigation, the receiving party is to contact the TCSG Legal Office.
3. The TCSG Legal Office will then issue a Litigation Hold Notice to the party of the lawsuit instructing the college to retain all documents which might be relevant to the lawsuit in their original state. Printing out and retaining only paper documents is not sufficient.

4. The archiving system discussed herein allows certain mailboxes to be marked for legal holds.
5. At the completion of litigation, the TCSG Legal Office will issue a letter indicating that the Litigation Hold on these documents has been lifted and the documents will return to their ordinary retention schedule.

VII. **RECORD RETENTION:**

Litigation Hold Notice – retained for 2 years after the completion of the litigation.

Technical College System of Georgia

**HEOA P2P Unauthorized File Sharing Prevention Compliance Standards (ISS-12)**  
**Procedure 3.2.3p HEOA P2P Unauthorized File Sharing Prevention Compliance**

**I. PURPOSE:**

To define a baseline for actions to combat the unauthorized distribution of copyrighted materials that is consistent with Federal requirements.

**II. RELATED AUTHORITY:**

O.C.G.A. § 20-4-11 – Powers of the Board

O.C.G.A. § 20-4-14 – TCSG Powers and Duties

**III. APPLICABILITY:**

All work units and technical colleges associated with the Technical College System of Georgia.

**IV. DEFINITIONS:**

**P2P Unauthorized File Sharing:** Unapproved distribution of copyrighted materials utilizing Peer to Peer or other technologies by users of TCSG networks and internet connected systems.

**V. ATTACHMENTS:**

N/A

**VI. PROCEDURE:**

1. To meet federal HEOA (Higher Education Opportunity Act) requirements a disclosure describing copyright law and TCSG policies and penalties must be provided to students annually. This statement must include the following:
  - a. A statement that explicitly informs its students that unauthorized distribution of copyrighted material, including unauthorized peer-to-peer file sharing, may subject the students to civil and criminal liabilities;
  - b. A summary of the penalties for violation of Federal copyright laws.
  - c. A description of the institution's policies with respect to unauthorized peer-to-peer file sharing, including disciplinary actions that are taken against students who engage in illegal downloading or unauthorized distribution of copyrighted materials using the institution's information technology system.
  - d. A link to legal alternatives for downloading or acquiring copyrighted materials.

2. To meet federal HEOA requirements each TCSG college will utilize one or more of the following technologies to identify and/or block P2P file sharing activities.
  - a. Bandwidth or traffic shaping
  - b. Traffic monitoring to identify abnormally high bandwidth users
  - c. Internet content filtering to block or reduce illegal file sharing
  - d. Other commercial products designed to reduce or block illegal file sharing
3. TCSG will respond to all Digital Millennium Copyright Act (DMCA) notices, notify the College ISA (Information Security Administrator) and work with the college to determine the sources of suspect traffic.
4. TCSG will periodically review the effectiveness of HEOAP2PUFSPCG compliance and make suggestions for improvement where needed.

## VII. **RECORD RETENTION:**

### Unauthorized Distribution of Copyrighted Materials is Against Federal Law

The unauthorized copying and distributing of copyrighted materials, including, but not limited to peer-to-peer (P2P) file sharing, is a violation of United States copyright law and may result in civil and criminal liability and prosecution.

### Summary of Civil and Criminal Penalties for Violation of Federal Copyright Laws

Copyright infringement is the act of exercising, without permission or legal authority, one or more of the exclusive rights granted to the copyright owner under section 106 of the Copyright Act (Title 17 of the United States Code). These rights include the right to reproduce or distribute a copyrighted work. In the file-sharing context, downloading or uploading substantial parts of a copyrighted work without authority constitutes an infringement.

Penalties for copyright infringement include civil and criminal penalties. In general, anyone found liable for civil copyright infringement may be ordered to pay either actual damages or "statutory" damages affixed at not less than \$750 and not more than \$30,000 per work infringed. For "willful" infringement, a court may award up to \$150,000 per work infringed. A court can, in its discretion, also assess costs and attorneys' fees. For details, see Title 17, United States Code, Sections 504, 505.

Willful copyright infringement can also result in criminal penalties, including imprisonment of up to five years and fines of up to \$250,000 per offense.

For more information, please see the Web site of the U.S. Copyright Office at [www.copyright.gov](http://www.copyright.gov), especially their FAQ's at [www.copyright.gov/help/faq](http://www.copyright.gov/help/faq).

## Unauthorized Distribution of Copyrighted Materials is Prohibited by TCSG Policy

TCSG Procedure 3.3.4p. prohibits the unauthorized distribution of copyrighted materials via TCSG systems or networks. Maximum penalties under Georgia Law are a \$50,000 fine and 15 years of imprisonment, plus civil liability in addition to the potential federal penalties listed above.

### **Legal Alternatives for Downloading or Otherwise Acquiring Copyrighted Materials**

For a list legal alternative sites for downloading copyrighted materials please visit:

<http://www.educause.edu/legalcontent>

**PCI Compliance Standards (ISS-13)**

**Definition of PCI Compliance:** All systems and networks that touch or store cardholder data must meet the security criteria set forth by the Payment Card Industry Data Security Standard (PCI DSS)

**Purpose of these Standards:** The purpose of these Standards is to assure that TCSG Colleges and affiliates that process credit/debit cards for payments of any kind comply with PCI DSS.

1. All TCSG Colleges and affiliates that process credit/debit card information by any means other than stand-alone direct dial-up card terminals that do not connect to any TCSG network, must meet the PCI DSS requirements and submit the appropriate periodic self-assessment questionnaire (SAQ) and Attestation of Compliance to their banking institution.
2. All TCSG Colleges and affiliates that process credit/debit card information by stand-alone, direct dial-up card terminals must retain a current Attestation of Compliance (AOC) from their payment processing company. This letter is the vendor's certification that they are PCI DSS Compliant and will serve as the College or affiliates compliance document.
3. 3<sup>rd</sup> Party Vendors such as bookstores, food service, etc. that are not owned and operated by TCSG are responsible for their own PCI DSS compliance. However, if they use a TCSG network to connect to their payment processing company the College or affiliate may be asked to provide the 3<sup>rd</sup> Party Vendor with an Attestation of Compliance (AOC) each year.
4. All TCSG Colleges and affiliates must maintain a current list of all 'in-scope' systems and networks under their control. Any TCSG system or network that the card approval process 'touches' is in-scope for PCI-DSS. For example, if there are four computers in the business office that are used for processing card data those four computers plus the College's network are in scope and must meet PCI DSS requirements which include quarterly vulnerability scans performed by qualified personnel.
5. In addition to the internal vulnerability scan requirements noted above, any in-scope system that is accessible from the public internet is also subject to quarterly external vulnerability scans and 3<sup>rd</sup> party certification requirements. An example would be a system that processes student credit/debit payments they enter via the web.
6. Any medium or higher threat level system vulnerability discovered must be remediated before the system will meet PCI DSS compliance requirements.
7. Payment information should pass through our systems and networks securely for processing only. If at all possible, cardholder data should \*never\* be stored in hard copy or electronic form.
8. If you must temporarily store cardholder data it must be protected at all times. Hard copy storage must be locked in a secure location and any electronic storage must be encrypted and secured. This information must be destroyed as soon as possible after use to assure protection from unauthorized access.
9. TCSG will assist College or affiliate Information Security Administrators in meeting PCI DSS requirements for all in-scope systems and networks.



PCI SAQs: [https://www.pcisecuritystandards.org/security\\_standards/documents.php?category=sags](https://www.pcisecuritystandards.org/security_standards/documents.php?category=sags)

## Protection of Personally Identifiable Information (PII) (ISS-14)

Definition of Personally Identifiable Information (PII): Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. Examples include direct references such as name, address, social security number, and e-mail address. PII also includes any information that could be used to reference other data elements that are used for identification, such as gender, race, and date of birth.

**Purpose of these Standards:** The purpose of these Standards is to assure that TCSG Colleges and affiliates protect Personally Identifiable Information from unauthorized access or dissemination.

1. The combination of an individual's name or other PII with other PII data many times results in the creation of 'Sensitive PII'. Sensitive PII is data that could be used to defraud, impersonate or otherwise harm an individual.

The following types of PII are considered sensitive when they are associated with an individual. Secure methods must be employed when transmitting or transporting this information\*:

- Social security number
- Student identification number
- Place of birth
- Date of birth
- Student address or address of student's family
- Student transcripts and related records, test results
- Mother's maiden name
- Biometric identification information including finger and voice prints
- Medical information, except brief references to absences from class or work
- Personal financial information
- Financial aid information
- Credit card or purchase card account numbers
- Passport numbers
- Potentially sensitive employment information, e.g., personnel ratings, disciplinary actions, and result of background investigations
- Criminal history
- Full face or equivalent photographs
- Vehicle information such as license plate number
- Any information that may stigmatize or adversely affect an individual.

\*This list is not exhaustive and other data may be sensitive depending on specific circumstances.

Social Security Numbers (SSNs), including truncated SSNs that include only the last four digits, are sensitive regardless of whether they are associated with an individual. If it is determined that such transmission is required, then secure methods must be employed.

3. Approved secure methods of transmission are: TLS for web-based applications, file, directory or full disk encryption for storage and physical transport (including storage on any portable device), and document encryption for email as long as keys or passwords are not transmitted in the same message as the data.

4. Student directory information may be published as long as students are notified in advance and have sufficient time to request that their information not be published.

Technical College System of Georgia  
**Red Flags Rule (RFR) (ISS-15)**

**Definition of Red Flags Rule:** The Red Flags Rule requires organizations to implement a written Identity Theft Prevention Program designed to detect the warning signs – or red flags – of identity theft and take steps to prevent it and mitigate its effects. Due to rapidly changing environment the program will be periodically reviewed and updated.

**Purpose of these Standards:** These Standards are designed to assist TCSG personnel to identify, detect and respond to common identity theft red-flags.

1. Always be aware and be on the lookout for any suspicious documents or behavior that may indicate attempted identity theft.
2. Review the attached examples of potential Red Flags (ISS-15a).
3. Add additional examples based on experience in your local College environment.
4. If you have credible information that an applicant for Federal Student Aid may have engaged in fraud or other misconduct in connection with their application you must contact the Office of Inspector General at DoE at 1-800-MISUSED or email them at [oig.hotline@ed.gov](mailto:oig.hotline@ed.gov)

If you suspect identity theft or other fraudulent activity on non-FASFAA documents contact your supervisor or Campus Police department.

Technical College System of Georgia

## Red Flags Rule (RFR) Examples (ISS-15a)

**RED FLAGS RULE – Examples of things that should raise ‘RED FLAGS’ Suspicious Documents Sometimes paperwork has the telltale signs of identity theft.**

- Identification that looks altered or forged
- The person presenting the identification doesn't look like the photo or match the physical description
- Information on the identification that differs from what the person presenting the identification is telling you
- Information on one document doesn't match with other information, like a signature card or recent check an application that looks like it's been altered or forged
- The document has been torn up and reassembled

## Suspicious Personally Identifying Information

**Identity thieves may use personally identifying information that doesn't ring true.**

- Inconsistencies with what else you know – for example, an address that doesn't match the credit report, the use of a Social Security number that's listed on the Social Security Administration Death Master File
- The SSN hasn't been issued, according to the monthly issuance tables available from the Social Security Administration
- There are inconsistencies in the information the customer has given you – say, a date of birth that doesn't correlate to the number range on the Social Security Administration's issuance tables
- The address, phone number, or other personal information has been used on an account you know to be fraudulent
- The person uses a bogus address, an address for a mail drop or prison, a phone number that's invalid, or one that's associated with a pager or answering service
- The Social Security number has been used by someone else opening an account
- The address or telephone number has been used by many other people opening accounts
- The person who omits required information on an application and doesn't respond to notices that the application is incomplete
- The person can't provide authenticating information beyond what's generally available from a wallet or credit report – for example, a person who can't answer a challenge question

## Suspicious Account Activity

**Sometimes the tip-off is how the account is being used.**

- Soon after you're notified of a change of address, you're asked for new or additional credit cards, cell phones, etc., or to add users to the account
- The new account is used in ways associated with fraud – for example, the customer doesn't make the first payment, or makes only an initial payment or most of the available credit is used for cash advances or for jewelry, electronics, or other merchandise easily convertible to cash
- An account that's used in a way inconsistent with established patterns – for example, nonpayment when there's no history of missed payments, a big increase in the use of available credit, a major change in buying or spending patterns or electronic fund transfers, or a noticeable change in calling patterns for a cell phone account
- An account that's been inactive for a long time is suddenly used again
- Mail sent to the customer that's returned repeatedly as undeliverable although transactions continue to be conducted on the account
- Information that the customer isn't receiving their account statements in the mail
- Information about unauthorized charges on the account

Technical College System of Georgia

## **Personal Electronic Devices (PED) (ISS-16)**

**Definition of Personal Electronic Devices:** Personal Electronic Device is an electronic device that is not owned by TCSG that emits an audible or visual signal, displays a message, or otherwise summons the processor, including, but not limited to, cellular telephones, paging devices, electronic e-mailing devices, radios, tape players, CD players, DVD players, video cameras, monitors, projectors, iPods or other MP3 players, laser pointers, portable video game players, laptop computers, personal digital assistants (PDA's), cameras, tablets, iPad's, smart watches and any device that provides a wired or wireless connection to the Internet.

**Purpose of these Standards:** To ensure that the equipment that is installed and connected to TCSG owned systems can be supported and maintained.

1. Any personal electronic device that is not owned by TCSG is prohibited from being connected to TCSG systems unless approved by the College ISA.
2. If a TCSG employee, student or guest requires special accommodations due to a medical condition the individual should contact the ADA Compliance Officer for the College to receive these accommodations.
3. Any personal equipment that an individual would like to use will need to be approved by the College ISA and donated to the college so that the college can add this equipment to its inventory.
4. These Standards will be revised based on changing information and requirements.

**Definition of HIPAA Compliance:** All systems and networks that touch or store electronic Protected Health Information (e-PHI) data must meet the security criteria set forth by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the *Security Standards for the Protection of Electronic Protected Health Information (HIPAA Security Rule)*.

**Purpose of these Standards:** The purpose of these Standards is to assure that TCSG Colleges and affiliates that store e-PHI of any kind comply with HIPAA and the HIPAA Security Rule.

1. All TCSG Colleges and affiliates will provide access control to systems that are used to read, write, modify, or communicate data/information or otherwise use any system resource.
  - a. Users shall have only the minimum access rights and privileges necessary to perform job functions.
  - b. Each user is required to have a unique name and/or number for identifying and tracking user identity.
  - c. Each user's identity will have a password that meets Level 2 password complexity requirements in ISS-03.
  - d. There shall be a procedure for establishing access for obtaining necessary e-PHI during an emergency.
  - e. Systems shall provide a mechanism that will automatically logoff or terminate an electronic session after a predetermined time of inactivity.
2. Systems shall provide appropriate industry standard encryption mechanisms for storing or sending e-PHI.
  - a. Systems shall provide a mechanism that will encrypt and decrypt e-PHI when it is transmitted, and stored.
  - b. Implement a security mechanism that will ensure that e-PHI is not been improperly modified until disposed of.
3. Provide a mechanism that will record and examine activity of systems that contain e-PHI.
4. Implement electronic mechanism to corroborate that e-PHI has not been altered or destroyed in an unauthorized manner.

**Publicly Accessible Server Vulnerability Assessment Standard (ISS-18)**

**Definition of Publicly Accessible Server:** Any server that resides on-premises or within a subscribed cloud environment that is accessible via any network external to the Campus' local area network.

**Purpose of these Standards:** The purpose of these Standards is to permit authorized TCSG and TCSG approved personnel to perform information security vulnerability assessment for the purpose of determining areas of vulnerabilities of publicly accessible servers. Vulnerability assessment provides visibility into the vulnerability of assets deployed in the network. Vulnerability assessment consists of scanning to identify networked assets, determine potential vulnerabilities and assessment of potential vulnerabilities.

1. Vulnerability Assessments can be conducted on any asset, product or service at TCSG or TCSG Colleges.
2. The development, implementation and execution of the vulnerability assessment process is the responsibility of the TCSG Information Security Officer (ISO).
3. Weekly vulnerability assessment scans will be performed on all network assets deployed on TCSG or TCSG College IP Address Space to comply with requirements from Control 7 in the CIS Top 18 Controls.
4. A centrally managed vulnerability assessment system will be deployed. Use of any other network-based tools to scan or verify vulnerabilities must be approved, in writing, by TCSG.
5. College IT personnel should cooperate fully with any vulnerability assessment being conducted on systems.
6. College IT personnel should work with the TCSG ISO to develop a remediation plan.
7. Any vulnerability scans or follow-up activities, performed outside of the centrally managed vulnerability assessment tool, required to assess vulnerabilities must be approved, in writing, by TCSG.
8. The TCSG Information Security Officer is permitted, with approval of the TCSG Chief Information Officer (CIO), to hire third-party security companies to run external vulnerability scans against externally deployed TCSG or TCSG College assets, products or services.
9. Any exceptions to this policy, such as exemption from the vulnerability assessment process, must be approved by the TCSG CIO and TCSG ISO.
10. These Standards will be revised based on changing information security requirements.



**Cyber Security Awareness Training Standard (ISS-19)**

**Purpose of these Standards:** To ensure security awareness and training controls protect information systems and Personally Identifiable Information (PII) and ensure information availability, confidentiality, and integrity of data.

1. All employees must complete a minimum of 1 hour of cyber security awareness training upon employment.
2. All employees will participate in annual cyber security awareness refresher training.
3. All employees shall be trained on how to identify, report, and prevent security incidents and data breaches.
4. All employees will receive training appropriate for specific job roles and responsibilities.
5. Required cyber security awareness training must be approved by TCSG CIO or their designee.
6. A record of employees who have completed training and the type of training they completed will be maintained by the college Information Security Administrator (ISA), and available upon request.
7. Standards may be revised based on changing information security requirements.

## Cyber Security Risk Management Framework Standard (ISS-20)

**Definition of Risk:** The measure of the extent to which a college is threatened by a potential circumstance or event and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

**Definition of Cyber Security Risk:** The concept of cybersecurity risk includes operational risk to information and technology assets that have consequences affecting the availability, integrity or confidentiality of information or information systems. This includes the resulting impact from physical or technical threats and vulnerabilities in networks, computers, programs, and data. The data focus includes information flowing from or enabled by connections to digital infrastructure or information systems, including but not limited to, information security, supply chain assurance, information assurance, and hardware and software assurance. The process described in this policy is a tool used to arrive at an understanding of risk involving information systems. Risk can be modeled as the likelihood of adverse events over a period of time, multiplied by the potential impact of those events.

**Purpose of these Standards:** To manage cybersecurity risk by using a detailed framework to balance among academic / business needs, the potential impact of adverse events, and the cost to reduce the likelihood and severity of those events.

1. IT Staff shall understand that risk is never reduced to zero and that there is always a level of risk that must be accepted as a cost of doing business. Reducing the risk to an acceptable level is also a cost of doing business.
2. Systems shall be monitored to assure that the level of cybersecurity risk is maintained at or below an acceptable level.
3. There are policy and procedural safeguards to assure that personal privacy and academic freedom are respected.
4. The process for managing cybersecurity risk is adapted for Technical College System of Georgia from the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF), described in NIST Special Publication 800-37 revision 2. The NIST Special Publications provide a systematic method of managing risk that is particularly well-suited to large public organizations.
  - a. TCSG will also use the NIST Special Publication 800-53 revision 5 and the NIST Special Publication 800-171.
  - b. This framework can be mapped to other frameworks for audit purposes.
5. The risk assessment process will be phased in. With Higher risk systems first, and moderate and low risk systems to follow.
6. The organizational unit determines what level of cybersecurity risk is acceptable to that unit, constrained by that unit's legal and regulatory environment.
7. Cybersecurity risk will be managed to ensure likelihood and impact of threats and vulnerabilities are minimized to the extent practical.
8. Cybersecurity risk will be managed on those systems developed or purchased for integration with the existing information technology architecture and on existing information technology architecture.
9. The College Information Security Administrator as defined in ISS-00 shall ensure the appropriate security of all data, especially personally identifiable information, is not placed at undue risk of exposure.
10. The risk management process is established in the standards so that the TCSG community understands that:

- a. TCSG is determined to manage cybersecurity risk effectively. Not doing so is likely to have unacceptable consequences to individuals.
  - b. This is TCSG's mandatory and universally applicable process for managing cybersecurity risk.
  - c. This process can be tailored to specific technologies, processes or services. This policy applies to TCSG owned or operated information systems and architectures that are installed on campus or accessible through external services, such as cloud infrastructure, services or applications, vendor-operated systems using TCSG information, systems operated remotely from other universities, etc.
  - d. The process must include policy and procedural controls to assure that privacy and data integrity are not compromised.
11. The College Information Security Administrator makes decisions on network and cybersecurity defensive measures through a defined and shared process. The College Information Security Administrator will allow for the following:
- a. Allow for temporary security controls to be put into place when immediate defensive action is needed.
  - b. Review those temporary security controls through the decision-making process, to determine if the temporary security controls should become permanent changes within 30 days of implementation.

## IT System Maintenance Standards (ISS-21)

**Definition of System Maintenance:** Maintenance to IT systems includes application and operating system patches and updates, configuration changes, and system cleanup tasks.

**Definition of System Maintainer:** Administrator of the IT system that is performing system maintenance as defined previously.

**Purpose of these Standards:** To develop a system whereby IT systems can be properly and routinely maintained, patched, and updated to mitigate any identified risks and threats.

1. Procedures must be developed by the College Information Security Administrator as defined in ISS-00 and maintained to ensure system maintainers have a predetermined time window to perform necessary system maintenance.
2. Periodic system maintenance for standard bug fixes and non-critical updates should be performed at a minimum once a quarter.
3. Logs of by whom, when, what and why a system is being maintained should be kept by system maintainer in a location accessible to at a minimum the system maintainer and College Information Security Administrator for a period of one year.
4. Monitor systems for events such as hardware failure, software failure, or computer security-related issues to prepare for maintenance outside of the normal time windows.
5. Develop a plan for resiliency during system maintenance to ensure availability of critical systems.
6. Develop a roll-back plan in the event of a failure in system maintenance.
7. When possible, employ automated patching mechanisms to schedule and conduct system maintenance where appropriate.
8. Application and Operating System software shall be upgraded when the vendor has declared end of support for a product. No out-of-support products shall be utilized if there is a comparable, supported product available.
9. When a critical Application or Operating System patch is needed, the College Information Security Administrator, TCSG Chief Information Officer, or the TCSG Information Security Officer can declare an unscheduled system maintenance window to perform the critical maintenance.
10. These Standards will be reviewed annually and revised as necessary based on changing information security requirements.

## Malicious Code Detection and Prevention Standard (ISS-22)

**Definition of Malware, Malicious Code, Malicious Software:** A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or otherwise annoying or disrupting the victim. Major forms of malware include, but are not limited to, viruses, virus hoaxes, worms, Trojan Horses, malicious mobile code, blended attacks, spyware, attacker backdoors, ransomware, and toolkits.

**Purpose of these Standards:** To detect and prevent malicious code from being installed and spreading across the internal network.

1. This policy applies to all users with access to the internal network, including users accessing resources through secure remote access methods.
2. All systems shall have installed up-to-date anti-malware software and signature files.
3. Installed anti-malware shall be centrally logged and manageable. Locally installed anti-malware without central manageability is prohibited.
4. Response to malware incidents shall comply with the incident response and reporting procedures as determined by the College ISA as defined in ISS-00.
5. Additional technical controls such as network segmentation, access-control lists, advanced anti-malware software using heuristics and behavioral analytics should be used where appropriate.
6. These Standards will be reviewed annually and revised as necessary based on changing information security requirements.

## Physical Security and Access Control Standards (ISS-23)

Technical College System of Georgia

**Definition of Physical Access Control:** Limiting access to campuses, buildings, rooms, and physical IT assets.

**Definition of Physical Security:** Security measures that are designed to deny unauthorized access to physical locations.

**Definition of Protected IT Assets:** Equipment such as switches, servers, firewalls, appliances or other equipment designated by the College ISA as defined in ISS-00 that will ensure of the availability and cyber security of the college network and resources.

**Purpose of these Standards:** To protect IT assets from physical unauthorized access and to monitor who accesses locations that contain IT assets.

1. Access to rooms containing protected IT assets should be limited to only individuals that need access to the rooms.
2. Areas containing protected IT assets shall at a minimum have a secure door with key access.
3. Areas with key access should have a sign-in log that is regularly reviewed yearly by the College ISA or their designee.
4. It is recommended that monitoring access to these areas shall be recorded using CCTV, RFID, sign-in log, or mag stripe type card or cipher lock access that can be assigned to an individual.
5. No shared keys or access cards are allowed.
6. Access rights shall be reviewed at a minimum yearly by the College ISA or their designee.
7. All visitors to protected IT assets shall check in with the Information Security Administrator or their designee before accessing these areas.
8. These standards will be reviewed annually and revised as necessary based on changing information security requirements.