INFORMATION TECHNOLOGY SECURITY PROGRAM
Central Texas College Information Technology Division
November 2016
Table of Contents

Introduction ........................................................................................................................................... 2

Policies
Acceptable Encryption Policy .................................................................................................................. 3
Application Security Policy .................................................................................................................... 4
Authorized Software Policy .................................................................................................................. 6
Change Management Policy .................................................................................................................. 8
HR No. 294, Computer Security Policy .................................................................................................. 15
HR No. 295, Computer Usage ............................................................................................................... 23
Criminal Activity Policy ....................................................................................................................... 29
Identification/Authentication Policy ...................................................................................................... 31
Intrusion Detection Policy .................................................................................................................... 33
Login Banner Policy ............................................................................................................................. 36
Malicious Code Policy .......................................................................................................................... 37
Media Sanitization and Disposal Policy ............................................................................................... 40
Network Configuration Management Policy ......................................................................................... 45
Physical Access Policy ......................................................................................................................... 47
Platform Management Policy .............................................................................................................. 49
Portable Computing Policy .................................................................................................................. 51
Remote Access Policy .......................................................................................................................... 53
Risk Assessment Policy ....................................................................................................................... 55
Security Monitoring Policy .................................................................................................................. 56
Security Updates Policy ......................................................................................................................... 58
Server Security Policy .......................................................................................................................... 61
System Development and Deployment Policy ....................................................................................... 63
Third Party and Vendor Controls and Compliance Policy ...................................................................... 65
Wireless Communication Access Policy .............................................................................................. 67

Guidelines
Data Encryption Guidelines ..................................................................................................................... 72
Incident Response Guidelines ............................................................................................................. 84
Minimum Security Standards for Systems ............................................................................................. 90
INTRODUCTION

IT Division Security Program

In response to a security audit by an external consultant, the IT Division developed an IT Security Program that incorporates a comprehensive computer security policy, computer usage standards, computer security incident response program, disaster recovery planning, change management, and patch/update management. The goals of the IT Division security program are to protect and preserve electronic data, comply with applicable laws and regulations, and respond to and recover from exploitations. The IT Division will accomplish these goals through the aforementioned policies and programs, a computer security awareness/education program, and monitoring applications.

Information Security Mission Statement

The mission of the Information Technology Security Program is to:

- Ensure that electronic information entrusted to the Central Texas College District is secure
- Ensure that all applicable regulations regarding the privacy and security of that data are followed
- Support the College’s mission and policies
- Work with College data stewards, data custodians, subject matter experts, and leaders to understand current and emerging needs regarding information security

The Information Security Officer plays a crucial role in the information security process by evaluating security issues and making recommendations to the Director of Information Technology for protecting College data and computer systems through policy, awareness, incident response, and resource planning.
ACCEPTABLE ENCRYPTION POLICY

Purpose
The purpose of this policy is to provide guidance that limits the use of encryption to that which continually meets current standards. Additionally, this policy provides direction to ensure that Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

Scope
This policy applies to all Central Texas College District employees and affiliates.

Policy Statement
1. Currently viable and accepted encryption technologies, such as Encryption Wizard, shall be utilized in all instances where encryption is required or appropriate.

2. Users shall consult the CTCD Data Encryption Guidelines to better assure the confidentiality and integrity of the College's sensitive data should data encryption be used as an information protection control.

3. Be aware that the export of encryption technologies is restricted by the U.S. Government. Residents of countries other than the United States should make themselves aware of the encryption technology laws of the country in which they reside.

Export Control Regulations
Under export control regulations, any individual transporting a laptop with encrypted data must seek an export license. Because most encrypted data or technology is by nature confidential information or contains controlled technology, licensing may be required under Export Administration Regulations (EAR) or International Traffic in Arms Regulations 2009 (ITAR) in order to be able to “export or re-import” an encrypted system outside or back into the United States. Therefore data considered an Information Resource or otherwise confidential in nature by Central Texas College shall not be transported out of the country.

It is recommended that if you are taking a laptop or any other data storage device(s) out of the country, it should only contain public domain information and should not be encrypted. Please contact the IT Help Desk if you have any questions.

Disciplinary Actions
Violation of this policy may result in disciplinary action that may include termination of employees or suspension or expulsion in the case of a student. Additionally, users are subject to loss of CTCD Information Technology Resources access privileges and may face civil and criminal prosecution.
APPLICATION SECURITY POLICY

Purpose
The purpose of the Application Security Policy is to avoid inadvertent release of confidential or sensitive information, minimize risks to users and the College, and ensure the availability of critical applications. Central Texas College focuses its efforts on security applications that hold or utilize data sets containing student information/records, personally identifiable information such as social security numbers or credit card numbers, and other categories of data that are protected by federal or state laws or regulations. Ultimately, to ensure application availability and reliability, all applications must be secured regardless of the type of information they utilize.

Scope
The Application Security Policy applies to applications developed by college staff as well as to those acquired from outside providers. All applications are subject to this policy regardless of whether the application is hosted on college equipment or elsewhere.

Policy Statement
To keep risk to an acceptable level, CTCD shall ensure that the proper security controls will be implemented for each application.

Data stewards, data custodians, system administrators, and application developers are expected to use their professional judgment in managing risks to the information, systems, and applications they use and support. All security controls should be proportional to the confidentiality, integrity, and availability requirements of the data processed by the system.

1. CTC Information Technology Division, individual departments, and contractors shall implement application security standards to have effective controls over systems they directly manage.

   a. If CTC Information Technology Division manages an environment or application, the IT Division shall be responsible for implementing the application security controls.

   b. If a department manages an environment or application, that department shall be responsible for implementing the application security controls.

   c. If an outsourced contractor manages a CTCD environment or application for an individual department, the department must ensure that the contractor implements the application security controls.

   d. College faculty and staff who engage any third-party hosting services (such as cloud services, SaaS, or managed hosting) for educational, research or approved purpose:
i. Must obtain prior approval from the Information Technology Division.

ii. May not entrust that provider with sensitive or confidential business data as defined in HR No. 294, Computer Security Policy.

iii. Availability and support agreements (e.g., 24X7, Weekdays only) must be at a level commensurate with the applications expected availability and must be communicated to the IT Division.

2. Applications installed or being changed should follow the standardized application lifecycle established by the IT Information Systems Turnover Procedures manual.

3. Each individual user (whether a developer, administrator, or user) should have a unique set of credentials for accessing a computer application.

4. Authenticated users should have access to a computer application and should only be allowed to access the information they require (principle of least privilege).

5. Establishing and changing access for a user or group should be approved by the application’s data steward.

6. Developers should follow best practices for creating secure applications with the intention being to minimize the impact of attacks.

7. Developers should not develop or test an application against production data sources.

8. Logs for the server, application and web services should be collected and maintained in a viewable format for a period of time specified by applicable state regulations.

9. Maintain a full inventory of all applications, to include authentication and authorization systems, the data classification and level of criticality for each application.

10. Document clear rules and processes for reviewing, removing, and granting authorizations.

11. Remove critical authorizations for access to applications for individuals who have left the college, transferred to another department, or assumed new job duties.

**Disciplinary Actions**
Violations of this policy may result in disciplinary action that may include termination of employees or suspension or expulsion in the case of a student. Additionally, users are subject to loss of CTCD Information Technology Resources access privileges and may face civil and criminal prosecution.
AUTHORIZED SOFTWARE POLICY

Purpose
The purpose of the Authorized Software Policy is to provide a set of measures that will mitigate information security risks associated with unauthorized software. Authorized software is any software that is acceptable for use on Central Texas College District (CTCD) Information Technology Resources. CTCD has negotiated special pricing and licensing for a variety of software available to all students, faculty and staff.

Other software is readily available in the open market place that has some kind of licensing agreement under which the user is subject. Some software is considered to pose a security threat to CTCD and its use may be restricted. Users entrusted with CTCD Information Technology Resources are responsible for maintaining licensing information for any software the user installs, and if requested by CTCD, must provide the College with licensing information. This includes, but is not limited to, smart phones, iPads, tablets, laptops, etc. Non-compliance with copyright laws regarding software is subject to civil and criminal penalties imposed by federal and state laws. These penalties are applicable to the College and/or an individual.

Scope
The Authorized Software Policy applies to all users of CTCD Information Technology Resources.

Policy Statement
1. All software installed or used on CTCD-owned information technology resources must be appropriately licensed.

2. The Information Technology Division shall maintain sufficient documentation to validate that the software is appropriately licensed.

3. Persons installing or authorizing the installation of software should be familiar with the terms of the agreement.

4. Users shall accept the responsibility to prevent illegal software usage and abide with the use of copyrighted materials. These responsibilities include:
   a. Do not illegally distribute or share software with anyone.
   b. All software must be license compliant, including personally purchased software.
   c. All software licenses must be readily available.
   d. Report any suspected or known misuse of software to the CTC Information Technology Division Help Desk.
5. The following general categories of software are specifically prohibited on all CTCD information technology resources unless specifically authorized by the Information Technology Division:

   a. Software used to compromise the security or integrity of computer networks and security controls such as hacking tools, password descramblers, network sniffers, and port scanners.

   b. Software that proxies the authority of one user for another, for the purpose of gaining access to systems, applications, or data illegally.

   c. Software which instructs or enables the user to bypass normal security controls.

   d. Software which instructs or enables the user to participate in any activity considered a threat to local, state or national security, including the assistance or transfer of information leading to terrorist activity or construction or possession of illegal weapons.

   e. Any other software specifically prohibited by the Information Technology Division.

**Disciplinary Actions**

Violation of this policy may result in disciplinary action that may include termination of employees or suspension or expulsion in the case of a student. Additionally, users are subject to loss of CTCD Information Technology Resources access privileges and may face civil and criminal prosecution.
CHANGE MANAGEMENT POLICY

Purpose
Outlines the process for controlling changes to IT infrastructure including telephony, network communications, and computing.

Scope
The IT Change Management Policy applies to the employees of the CTC Information Technology Division.

Overview
A. Technical Scope
1. Tasks covered by the Change Management Policy
   a. Software development (refer to the IT Software Development Methodology)
   
   b. Hardware – all computing and communications infrastructure from the data center located in Building 139, the communication center in Building 107, and all data closets and wall jacks.
   
   c. Application software and database management systems
   
   d. System configurations
   
   e. Operational changes including times and frequencies
   
   f. Telephone system

2. Excluded tasks
   a. IT Disaster Recovery Plan
   
   b. Daily administration processes:
      • Password resets
      • User additions/deletions
      • Telephony additions/deletions
      • User modifications
      • Adding, deleting or revising security groups
      • Rebooting workstations when there is no change to system configurations
      • File permission changes
      • Backups
B. Risk Matrix

<table>
<thead>
<tr>
<th>Type of Change</th>
<th>Risk</th>
<th>Back-out Process</th>
<th>Lead Time</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Low</td>
<td>Simple</td>
<td>Low Visibility</td>
</tr>
<tr>
<td>Routine</td>
<td></td>
<td></td>
<td>1-2 days</td>
</tr>
<tr>
<td>Extraordinary</td>
<td>Low</td>
<td>Complex</td>
<td>High Visibility</td>
</tr>
<tr>
<td>Extraordinary</td>
<td>High</td>
<td>Simple</td>
<td>2 weeks</td>
</tr>
<tr>
<td>Extraordinary</td>
<td>High</td>
<td>Complex</td>
<td>3 weeks</td>
</tr>
</tbody>
</table>

C. Routine Request - Simplified
1. Change Initator submits change request on Change Management Request on the IT SharePoint Portal.
2. Department Director reviews request for feasibility, necessity, and approves/disapproves request
3. Notification sent IT Division Director
4. Change Initiator performs change

D. Extraordinary Request – Simplified
1. Change Initiator submits change request on Change Management Request on the IT SharePoint Portal.
2. Department Director reviews request for feasibility, necessity, and desirability, and approves/disapproves request
3. IT Division Director approves/disapproves request
4. Change Initiator performs change

E. Incident Report
Change Initiator completes a Change Incident Report if a change fails:
- Describes the incident, date, and time
- Describes the diagnosis
- Lists the recovery operations, date, and time
- Discusses recurrence prevention
- Submits it to department director and IT Division Director
- Logs report in IT SharePoint Portal
Appendix A

Detailed Instructions for Change Initiator

I. Change initiator researches and gathers change requirements.
   A. Determine risk type
   B. Determine implementation date and time
   C. Estimate user impact (e.g. number of users affected)
   D. Determine systems affected
   E. Develop a generalized implementation plan
   F. Develop a back-out plan
   G. Arrange for implementation assistance, if needed

II. Complete online submission form on the IT SharePoint Portal.

III. Department Director reviews request for feasibility, necessity, and approves/disapproves request.

IV. The Department Director determines if request is Routine or Extraordinary.
   A. If Routine (see Appendix C):
      1. Approve/Disapprove request
      2. Log approval/disapproval on IT SharePoint Portal
      3. Notification sent IT Division Director
   B. For Extraordinary, request discussed if questions arise with IT Division Director and department director (see Appendix D)
      1. Approve/Disapprove request
      2. Log approval/disapproval on IT SharePoint Portal

V. Performs requested change
   Completes Change Management Incident Report (see Appendix E) if change fails.
Appendix B

Glossary

Back-out Plan - undoing a change to restore a system or application back to its original state; categorized as simple or complex.

Change - an update, improvement, or configuration change to any CTC IT software or infrastructure component that has the ability to disrupt information technology services.

Change Initiator - an IT Division employee that desires to make a change to an IT system or application beyond routine maintenance and daily administration processes.

Change Management - the process of requesting, analyzing, approving, developing, implementing, and reviewing a planned change within IT. For unplanned changes, it is the process of reviewing and mitigating the effects of an uncontrolled or unanticipated change to an IT asset.

Emergency Change - a change that results from an unexpected occurrence due to an uncontrolled or unanticipated change that has high visibility and/or major impact.

Extraordinary Change - a change to an IT system or infrastructure component that is major in impact, high in visibility, possibly lengthy in installation, and has a complex or extensive back-out plan.

Hardware - computing and communications infrastructure from the data center in Building 139, the communications center in Building 107, the data closets in the various buildings on campus, and the wall jacks in the rooms.

Impact - depth of a change, i.e. the level of severity and how it affects users.

Infrastructure - all of the components: hardware, software, cables, and firmware, that together constitute the IT computing and communications system.

Incident Report - a post-emergency change report that describes the event that required a change, its resolution, and the steps taken to mitigate the likelihood of the event from happening again.

Routine Change - a change that is minimal in impact, such as a day-to-day or weekly update, with low visibility, and a quick and simple back-out plan.

Visibility - breadth of a change, i.e. the number of users affected by a change.
Appendix C

Change Management Request Workflow – Routine Change Request

1. **CHANGE INITIATOR**
   - SharePoint change request

2. **DEPARTMENT DIRECTOR**

3. **REVIEW REQUEST**

4. **FEASIBLE?**
   - No → **DISAPPROVED REQUESTS**
   - Yes → **NECESSARY?**

5. **NECESSARY?**
   - No → **DESIRABLE?**
   - Yes → **APPROVE REQUEST**

6. **APPROVED REQUESTS**

7. **SCHEDULE CHANGE**

Appendix D
Change Management Request Workflow – Extraordinary Change Request

CHANGE INITIATOR

Discusses Proposed Change With His/Her Department Director

DEPARTMENT DIRECTOR

REVIEW REQUEST

FEASIBLE?

No

DISAPPROVED REQUESTS

Yes

NECESSARY?

No

DESIRABLE?

Yes

CHANGE INITIATOR

SharePoint change request

DIRECTOR OF IT

Schedules CAB Meeting

CHANGE ADVISORY BOARD

APPROVED?

No

DISAPPROVED REQUESTS

Yes

APPROVED REQUESTS

SCHEDULE CHANGE
Change Management Incident Report

<table>
<thead>
<tr>
<th>INFORMATION TECHNOLOGY DIVISION</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHANGE MANAGEMENT INCIDENT REPORT</td>
</tr>
</tbody>
</table>

### I. INCIDENT

<table>
<thead>
<tr>
<th>Date/Time Reported</th>
</tr>
</thead>
</table>

### II. DIAGNOSIS

<p>| |</p>
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
</table>

### III. RECOVERY

<table>
<thead>
<tr>
<th>Date/Time Restored</th>
</tr>
</thead>
</table>

### IV. RECURRENCE PREVENTION

<p>| |</p>
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
</table>

### V. PERSONNEL

<table>
<thead>
<tr>
<th>Employee</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department Director</td>
</tr>
<tr>
<td>IT Division Director</td>
</tr>
</tbody>
</table>
I. PURPOSE
To identify the requirements needed to comply with applicable regulations and protect electronic data.

II. SCOPE
The students, faculty, staff, guests, and external individuals or organizations that use computing and communications resources and/or equipment owned, leased, or rented by Central Texas College District (CTCD).

III. ROLES AND RESPONSIBILITIES
The CTCD community is responsible for protecting information and Information Technology Resources. The level of responsibility depends on the role of the employee.

A. Users
A user is anyone who uses CTCD computing resources and or equipment. Users are responsible for: reading, understanding, and complying with this policy; the management and protection of both computerized and non-computerized information; and protecting and caring for information technology devices that have been assigned to them to perform the duties of their respective positions. The consequences of not doing so are detailed in Sections III.C and V.B of this policy.

1. User-Level Security
   a. CTCD users will adhere to the provisions of HR Policy 295, Computer Usage. Questions regarding appropriate computer and network usage should be directed to the user’s supervisor or Human Resources.

   b. Users will not share, write down, or send passwords via e-mail.

   c. CTCD provides open access to an unencrypted student/guest wireless network. Users must agree to the Terms of Use before access is granted to the wireless network. Wireless access points not authorized or managed by the IT Division are not permitted and will be shut down upon discovery by IT.

   d. Users utilizing the CTCD student/guest wireless network do so at their own risk. CTCD is not responsible for privately owned systems (e.g., laptops and mobile devices). Users are encouraged to transmit sensitive data only when strong encryption is available.

   e. CTCD is not responsible for any illegal content that is received, transmitted, or stored by users.
f. Users should not use systems or software that are not approved by the IT Division.

g. Users gaining access to CTCD computing resources via a virtual private network (VPN), the wireless network, or Outlook Web Access (OWA) are responsible for ensuring their systems are free of malware.

h. Users will follow the rules posted in computer labs. If computer usage rules are not available in the lab, users will follow local, state, and federal laws, or obey the computer and Internet usage laws of the applicable host country. Users will log off systems when they are finished.

i. Users will exercise caution when opening email and browsing the Internet. Users will not open unexpected or suspicious email attachments.

j. Users are responsible for the security, usage, and outcome of any computer system or network device they attach to the network.

k. Users will immediately report any suspected or known information security compromises to the IT Help Desk.

2. Computer Accounts
   a. Users will use strong passwords that are changed on a recurring basis, not exceeding 42 days.

   b. Users are responsible for all activities (i.e., their activities or another person’s activities) associated with any computer account assigned to them.

   c. Users will only use computer accounts that have been created for them.

   d. Users will immediately report any suspected unauthorized use of their account(s) to the IT Help Desk.

3. Individually Assigned Computing Resources
   Users will log off of their workstation at the end of the day and leave their computer(s) powered on to accept updates that are distributed overnight via the CTCD data communications network.

   Users will not turn on software firewalls. This prevents updates from being properly installed. The IT Division will maintain a network firewall to protect computers from malware.

4. Computer Security Incident
   Users are to immediately report suspected computer security incidents (e.g., hacking) to the IT Help Desk.
B. Managers
Managers are users who supervise other users. Managers are responsible for the following items:

1. Ensuring that the users they supervise have access to the information needed to perform their respective jobs.

2. Requesting information access for their appointed users from the appropriate data steward(s) (see section III, item C).

3. As data custodians for data stewards, managers will take direction and implement procedures and controls as directed by the Data Stewards.

4. Periodically reviewing the level and/or extent of access for their appointed users, and requesting removal of access for their users when employment is terminated.

5. Ensuring that any specific information security policies and procedures they establish for the users they supervise are consistent with this policy, as well as with other CTCD policies and laws.

6. Administrative units will stay abreast of software updates for their departmental and/or workgroup applications. Installation assistance will be sought from the IT Division.

7. Administrative units are required to provide the IT Division with a copy of the new or unique software being used by their department and/or workgroup. This copy will be stored in the IT Division’s software library.

C. Data Stewards
Data stewards are users who own, manage, and grant access to data. Data stewards consist primarily of Division directors, deans, and Ellucian Colleague functional custodians (i.e., users that oversee an entire Colleague module, such as the Colleague Financials, or a functional subset, such as Accounts Payable). Data stewards are responsible for the following:

1. Classifying and labeling the information for which they are responsible (see section IV).

2. Determining which users are authorized to have access to their data.

3. Directing the Information Technology Division to grant or remove access for their authorized users.

4. Informing their users of the classification of data they can access and the rules that correspond with protecting Class 2 or Class 3 information from unauthorized access or usage.
5. Collaborating with the Information Technology Division to establish specific information security policies and controls for the Information Technology Resources they manage based on the results of annual risk assessments. Such policies and controls must be consistent with this policy, other CTCD policies, and the law.

6. Protecting their data and exercising discretion concerning access, usage, and dissemination.

IV. CLASSIFYING, STORING, AND TRANSMITTING DATA

A. Classes of Data
Data stewards should classify their information into one of the three classes listed below and declare who is authorized to access and disseminate that data. The three classes of data are as follows:

1. Class 1 - Public information. Information made available either to the public or to specific individuals who need it with few, if any, restrictions. The published class schedule is an example of Class 1 data.

2. Class 2 - Information with limited distribution. The loss, corruption, or unauthorized disclosure of this information would not affect the operational effectiveness of CTCD. A document detailing a fund-raising strategy is an example of Class 2 data.

3. Class 3 - Private information. Information that is confidential and protected from external access and unauthorized internal access. Loss, corruption, or unauthorized disclosure of this information would impair the business or research functions of CTCD; result in business, financial, or legal loss; or be a violation of federal or state laws/regulations or CTCD contracts. Data integrity is vital. An example of private information would be a student’s academic record.

B. Storing and Transmitting Data
1. Class 3 information should not be stored on users’ workstations.

2. Class 3 information, such as social security numbers, passwords, and other potentially name-linked data, should never be transmitted unless it is encrypted using IT approved encryption. For questions about encryption, contact the IT Help Desk.

V. User Security Violations
User violations include, but are not limited to, the following:

- Interfering with the operation of anti-virus/malware detection software installed by the IT Division or willfully introducing computer malware into the CTCD network.
- Generating malicious or illegal traffic and/or attempting to gain unauthorized access to sensitive or personal data belonging to CTCD or other entities or executing port scans, security scans, or any form of network monitoring that intercepts data not intended for you.

- Examining, copying, modifying, or deleting data or electronic mail belonging to other users without their prior consent or proper authorization.

- Using CTCD computer systems and/or networks to gain unauthorized access to remote systems.

- Attempting to obtain unauthorized access to or interfering with the operation of network systems or programs.

- Intentionally operating any network-intensive application that overloads the network.

- Performing any unauthorized action that damages or disrupts a computing system, alters its normal performance, or causes it to malfunction.

- Forging or attempting to forge electronic mail messages or header information.

- Making illegal copies of software licensed to CTCD.

- Using CTCD-owned computer accounts, computer equipment, communications equipment, software, or networks for commercial or non-work related purposes.

- Modifying configuration options or installing software that may cause increased security vulnerabilities. (e.g., remotely accessing a CTCD-owned computer in a way that bypasses existing security measures.)

- Interfering with the ability of other users to utilize shared computing resources. (e.g., deliberately deleting data from shared resources, moving shared files or folders without permission, or storing inappropriate material on shared drives or folders.)

- Offering “server-class” services from your workstation or other device without prior approval from the Information Technology Division.

- Connecting any wireless access device to the campus network without prior approval from the Information Technology Division.

- Attempting to decrypt passwords or other encrypted information.
• Attempting to secure a higher level of privilege on network systems or attempting to subvert the restrictions associated with your account(s) and/or software.

• Revealing your account password to others, except for the purpose of technical support by Information Technology Division personnel or allowing use of your account by others such as family and other household members.

A. Privacy And Confidentiality

1. Information Handling
   You are responsible for knowing the privacy and confidentiality restrictions associated with any information to which you have access. You agree to safeguard information that is classified Class 2 or Class 3. Such safeguards include, but are not limited to, the following:

   a. Storage of Information
      i. Users will store Class 2 and Class 3 information on secure network drives provided by the Information Technology Division.
      ii. Users will not transfer or store Class 2 or Class 3 information on removable or mobile devices without a method of encryption approved by IT.

   b. Distribution and Transmission of Information
      i. Users will not distribute or make Class 2 or Class 3 information available to persons who are not authorized to access the information.
      ii. Users will appropriately protect Class 2 or Class 3 information that is transmitted electronically, physically, or spoken in conversation from unauthorized interception.

   c. Destruction and Disposal of Information and Devices
      i. Class 2 or Class 3 documents will not be placed in recycling bins or trash cans. All such documents will be cross-shredded when discarded.
      ii. Users will ensure that Class 2 or Class 3 data is rendered unreadable when disposing of computers or removable media.

2. Electronic Communications and Data
a. CTCD does not routinely intercept or monitor electronic mail, other electronic communications, or other data stored in electronic format. Capture and/or "reading" of electronic communications and/or other data stored in electronic format by technical staff or others is expressly prohibited, except under the following circumstances:

i. To resolve technical or delivery problems.

ii. To prevent illegal, unauthorized, or inappropriate use.

iii. To meet externally imposed legal requirements.

iv. In the course of an internal or external investigation.

v. To protect health and safety.

vi. To prevent interference with the mission of CTCD.

vii. To locate information required for CTCD business that is not readily available elsewhere.

b. CTCD reserves the right to disclose the contents of our electronic communications, or other data stored in electronic format, without permission of the user.

c. Users agree that electronic mail, electronic communications, or data stored in electronic format with the use of CTCD resources may be made available for review by any authorized CTCD official for purposes related to CTCD business.

d. User correspondence in the form of electronic mail may be subject to public inspection as a public record under the Open Records Act.

e. The Family Educational Rights and Privacy Act (FERPA) of 1974 protects students against the release of some information. Electronic correspondence may become a student record under FERPA and may be available to disclosure under that act. All use of electronic mail, including use for sensitive or confidential information, will be consistent with FERPA.

3. Confidential Data

Users agree to comply with the following:

a. FERPA. If your account gives you access to student data, you must comply with all FERPA regulations regarding disclosure of student information.

b. The laws of the State of Texas, the United States, and other regulatory agencies. This includes all applicable federal and state laws that govern the privacy and confidentiality of
data, including, but not limited to, the Electronic Communications Privacy Act of 1986, the Health Insurance Information Portability and Accountability Act (HIPAA), the Foreign Corruptions Practice Act, the Gramm-Leach-Bliley Act, and the Computer Fraud and Abuse Act.

c. All CTCD policies and handbooks.

B. Consequences Of Policy Violations

1. Failure to comply with the IT Security Policy or related policies will be reported to the CTCD Human Resources Department.

2. Violations of local, state, federal, or other laws will be reported to the appropriate, respective authorities.

3. The Information Technology Division may revoke a user’s account at any time if computing privileges are abused. This revocation may be temporary, if such action is deemed necessary for the successful management and operation of the facilities, or permanent through the normal CTCD disciplinary process.

4. Failing to maintain a secure system, or any violation of HR Policy 295, Computer Usage, may result in immediate loss of network connectivity and account lockout.

5. Systems that appear to be infected or compromised will be immediately disconnected from the CTCD network until the system is scanned and cleared for use. IT Division staff will attempt to notify the user when his/her system is taken offline.

6. Any individual found violating this policy to include; misusing data, divulging confidential data, or otherwise violating these guidelines will be subject to disciplinary action in accordance with the Human Resources Management Policies and Procedures Manual up to and including termination of employment with CTCD. Any known violations of these guidelines must be reported to a supervisor or Human Resources.

VI. EXCEPTION TO POLICY

Individuals or departments seeking exception to this policy will do so in writing from the appropriate data steward (i.e. the Director of Student Services) or IT Division.
COMPUTER USAGE, HR NO: 295

Purpose
This policy provides guidelines to protect the College, its computing resources and employees from liability, harassment and business interruptions due to inappropriate computer usage.

Scope
This document applies to all persons, using property owned or operated by CTCD, who have been granted use of Central Texas College’s computing resources for use at work, home or while traveling. Users include, but are not limited to, students, faculty, staff, vendors and guests of the College.

Use Agreement
Computing resources are to be used only for the College-related activities for which they are assigned. These resources include all computer files, e-mail messages, Internet usage, voice mail messages and business telephone conversations on CTCD equipment. CTCD reserves the right to inspect any equipment and resources for prohibited files and downloads at any time and for any reason. The College reserves the right to limit, restrict or extend computing privileges and access to its computing resources. Administrative units within the College may define additional procedures and conditions for use of computing resources under their control as long as they are consistent with this policy statement.

User Responsibilities
All users of computing, networking, and other Information Technology (IT) resources of the College are required to:

A. Be ethical and respectful of the rights of others and of the diversity of the College community;

B. Protect the confidentiality and integrity of institutional data;

C. Protect the integrity of passwords (computer accounts and passwords are for use only by individual users and should not be shared);

D. Ensure computers are logged off when leaving their desk;

E. Check regularly for operating system and browser software updates and security patches;

F. Scan their computer for known viruses and other malicious programs that may be present;

G. Backup files and folders regularly; and,

H. Use resources responsibly and refrain from acts that waste resources or prevent others from using those resources.
I. Abide by local, state, and federal laws.

**Inappropriate Uses**

A. **Using Emoticons/Wallpaper/Screensavers/Marquee screensavers.** The use of emoticons, wallpaper, marquee screensavers, and third party screensavers does not present a professional image. Their use can result in a loss of productivity, be offensive to some, and interfere with the normal functioning of other programs on your computer. Wallpaper and screensavers are limited to those included with the Microsoft Windows® operating system.

B. **Sending personal e-mail.** Personal e-mails are to be limited and will be closely monitored for abuse. Distributing joke e-mails, keeping in touch with friends, online dating, and sending resumes to prospective employers are examples of personal e-mail. E-mail accounts shall be used for the purpose for which they were created: College business communications. All violations will be reported. Employees that spend an excessive amount of time sending/receiving personal e-mail will be disciplined accordingly.

C. **Storing personal data on College computers.** This is an unauthorized use of the College’s computing resources. An example would be storing your resume in a Word folder, or using the address book feature of Outlook to store contact information for personal acquaintances.

D. **Generating SPAM.** Any e-mail, which is not official business, could be considered Spam if sent to everyone on the Outlook directory. Over time, the accumulation of these unsolicited e-mail messages will slowly degrade the performance of the e-mail system and generate unnecessary traffic on the network. It is preferable to use CTC website links to communicate general information rather than to create mass, campus or district-wide e-mail messages.

E. **Web surfing.** Web surfing, including online shopping, and dating, consumes inordinate amounts of Internet bandwidth and causes business-processing bottlenecks.

F. **Sending chain letters.** These actions waste bandwidth, congest the e-mail system, and spread misinformation.

G. **Running two or more concurrent sessions (connection between user and server).** Multi-user computers do not have unlimited resources. If a user logs into a multi-user system such as Colleague two or more times (two or more concurrent sessions), he/she may prevent other users from having access to that computing resource.

H. **Termination of an Unattended Colleague session.** If a critical business operation is delayed by another user’s Colleague session, and that user is unavailable, the IT Division will contact his/her department and request permission to terminate the session. The IT Division will not terminate the original user’s session without the approval of the user, approval by an in-charge member of the user’s department, or lastly, unless directed by the CTC administration that a mission-critical operation warrants the termination.
I. Listening to Internet radio. Listening to Internet radio and other forms of non-work related streaming media consumes network bandwidth, thus taking resources from essential business processes.

J. Using public IM tools or chat rooms (chatting). Instant messaging may only be used when authorized by the employee’s supervisor and the IT Division. Use of instant messaging applications can seem easier and more convenient to use than the telephone or e-mail, yet they pose many risks to the College. Use of IM tools and chat rooms can affect employee productivity, waste network bandwidth, and pose a possible legal risk to the College. System security is also threatened as hackers can introduce viruses and worms into networks through files that are transmitted through IM tools and chat rooms. Hackers posing as legitimate business contacts can steal confidential information.

K. Downloading/installing unauthorized applications. Downloading or installing shareware, free screensavers, or games pose risks to user privacy and network security. These software applications can contain spyware that collect information about the user and send it to information collection services who will sell that information to third parties.

L. Unauthorized use of confidential data. When a user obtains access to data on a system, he or she must safeguard that information by not sharing it with third parties. Failure to do so poses a significant legal risk to the College and the user.

M. Downloading MP3 music or movies to DVD. Peer-to-peer (P2P) file-sharing programs such as Bit Torrent are used to illegally trade copyrighted music, movies, software, and games. Illegally copying or downloading copyrighted music, software, or movies (software piracy) is prohibited. P2P applications can leave a breach in an otherwise secure network, degrade network performance, provide unauthorized users access to your hard drive and the network, and can be an entry point into the network for malicious software. Many of the P2P programs contain spyware, allowing third parties to secretly gather information about users.

N. Playing computer games. Games adversely affect productivity. A number of gaming applications use excessive amounts of bandwidth, thus directing resources away from business critical tasks.

O. Maintaining confidential data on desktops. Unattended personal computers face exposure to theft and unauthorized access. Users shall always logoff of their PCs when they are away from their desks. Laptop shall not be left unattended and unsecured. Users must follow password guidelines, and install the latest software security updates. Laptops should have recovery software installed in the event of theft. Any PC with sensitive data and information should be safeguarded to reduce the possibility of theft and the resultant legal risks to the College.

P. Destroying equipment, information, or data. The confidentiality, integrity, and availability of computing resources can be compromised by the malicious or accidental damage of equipment, information, or data. Spilling coffee on a keyboard, dropping a laptop on the floor, and/or deleting files and data can result in
resource and financial loss to the College. Reasonable precautions shall be taken with respect to the operation, handling, and maintenance of computing equipment and the contents therein.

Q. **Unauthorized equipment or software modifications.** Users shall not add hardware and/or software to a computer, modify system files or settings, or delete standard software on a computer without prior approval of the IT Division. Unauthorized alterations to computers eventually result in lost productivity. Such changes often involve a technician to fix both the original problem, and the problem caused by the would-be technician. Poor documentation of the procedures performed, and the order in which they were completed further complicate unauthorized changes to computers. The IT Division will determine the use and specifications of all technology equipment used. Contact the Director of IT Customer Service to coordinate requests for new computing equipment and modifications.

R. **Harassment.** Employees shall not access or send files, data, pictures, games, or jokes that contain pornographic, obscene or lewd material, derogatory remarks, slurs or gestures that demean, ridicule or torment an individual. Harassing behavior can create an intimidating, hostile or offensive work environment, thus making way for the College and the employee to incur legal liability. All violations shall be reported to your supervisor.

S. **Mobile devices/removable storage devices.** These devices provide excellent convenience for storage and transportation of data. The possibility of losing such a device puts the College and individuals at risk for data theft if personally identifiable information is stored on the device. Individuals should use a virtual private network (VPN) to access data stored by the College when working away from their desktop or at a remote location.

**Social Networking Policy**

Students and higher education institutions are increasingly using social networking Web sites and on-line communities to communicate with each other and post events and updates. Refer to the Social Media Guidelines found on the Marketing & Outreach webpage for more information on disseminating official college information. The absence of, or lack of explicit reference to a specific site does not limit the extent of the application of this policy. Where no policy or guideline exists, employees should use their professional judgment and take the most prudent action possible. Employees should consult their supervisor, Human Resources, IT or Marketing & Outreach if uncertain how this policy applies.

A. College employees authorized by their departments may use approved social media or social networking sites to conduct College business in accordance with established guidelines. College social media pages or sites must be created and approved by Marketing & Outreach. Publication guidelines for official college or department/organization social media content is similar to any other media. Oversight of all CTC-affiliated pages is the responsibility of Marketing & Outreach, who will periodically review pages to ensure College policies are followed and that the pages are being produced in accordance with the best interests of the College.
B. Personal use of the College’s electronic resources to access social media and social networking sites is to be limited and must not interfere with an individual’s job performance or compromise the functionality of the campus network.

C. The College does not permit individuals or groups within the College community to present personal opinions in ways that imply endorsement by the College. Personal blogs should have clear disclaimers that the views expressed by the author in the blog is the author’s alone and do not represent the views of the College.

D. Be respectful to the College, other employees, students, vendors, and guests.

E. Employees’ online presence reflects the College. Employees should be aware that their actions captured via images, posts, or comments can reflect on the College.

F. Do not reference or cite faculty, staff, students, vendors, or guests without their express consent.

G. Respect copyright laws and reference cite sources appropriately. Plagiarism applies online as well.

**Consequences of Misuse**

Any employee found to have violated this policy will be subject to disciplinary action in accordance with the Human Resource Management Operating Policies and Procedures Manual up to and including termination of employment with CTCD.

**Definitions**

- **Application.** A software program that serves a specific purpose for the user. Word processors, such as Microsoft Word®, are applications.

- **Bandwidth.** The amount of data, measured in bits per second that can travel through a communications channel such as a network or modem.

- **BitTorrent.** Bit Torrent is a P2P file sharing protocol used for distributing large files such as movies and videos.

- **Chat.** A real-time typed conversation that takes place on a computer.

- **Emoticon.** “Smiley” keyboard letters and symbols used to show emotions in plain text messages.

- **Hacker.** A person who tries to break the security of a computer or network.

- **Instant message (IM).** A real-time Internet communications service that notifies a user when one or more people are online and then allows the user to exchange messages or files or join in a private chat room with those people.
Malicious code. Programs that can negatively affect a computer’s operation and capture information about a user, such as passwords and bank account information.

Marquee. Text animated to scroll across the screen. Often used as a screensaver.

Mobile device. Any pocket-sized computing device that has a small visual display screen for output and a miniature keyboard or touch screen for input.

Personally Identifiable Information. Information that can be used to identify, contact, or locate an individual. Names, addresses, and social security numbers are examples.

P2P. A peer-to-peer network on which users connect directly to each other’s hard disks and exchange files over the Internet. MP3 file-sharing applications are an example.

Removable storage devices. Storage devices used to store data and used for data transportation and/or data backup. USB Flash drives, cell phones, CDs, DVDs, and floppy disks are examples.

Shareware. Proprietary software that is provided to users free on a trial basis but may be limited in functionality, availability, or convenience with the understanding that the user may want to purchase it later. Shareware is available through download from an Internet Website or CD.

Software piracy. The illegal copying of computer software for distribution within an organization or distribution among friends and family without purchasing the appropriate amount of licenses.

Spam. The e-mail equivalent of junk mail that is unsolicited and usually unwanted by its recipients.

Spyware. Includes programs placed on a computer without the user’s knowledge and secretly collect information about the user. The program communicates information to an outside source while the user is online.

Streaming media. Streaming is the transfer of data in an even and continuous flow. Streaming media includes interactive and high-bandwidth applications, such as Internet radio.

Virtual Private Network (VPN). A private network over public network. A VPN provides users a secure channel between their home computer and a computer at a remote location.
CRIMINAL ACTIVITY POLICY

In 1985, the State of Texas passed a computer crimes law. Over the years, the law has been amended several times to meet the needs of changing technology. Under this state law, it is a crime to make unauthorized use of protected computer systems or data files on computers, or to make intentionally harmful use of such computers or data files. The seriousness of such a crime ranges from Class B misdemeanor to third-degree felony.

The complete text of the computer crimes chapter of the Texas Penal Code is available at the first link below. Users should make sure they are familiar with this law and the consequences of violating it.

Computer Crimes Chapter
Telecommunication Crimes Chapter

In addition to the computer and telecommunication statutes mentioned above, students, faculty and staff should also be familiar with CTC HR Policy No. 294, Computer Security Policy, CTC HR Policy No. 295, Computer Use Policy, and other IT policies on the CTC Information Technology web site.

The CTC Information Technology Division takes a very serious view regarding the misuse of Central Texas College District’s hardware, software, and/or network. This applies to misuse of facilities located on-campus or sites accessed through the CTCD network.

The IT Division will work with campus police as well as external law enforcement agencies in cases of suspected or confirmed misuse.

The IT Division will not hesitate to press for suspension of privileges, suspension from CTCD, or various legal actions when the situation warrants.

The IT Division’s primary goal in this regard is to protect the safety and privacy of our students, faculty, and staff. Our secondary goal is to provide consistent and quality service. We will utilize appropriate legal resources at our disposal to meet these goals.

Texas and Federal Statutes
Below you will find the state and federal laws in place regarding internet usage and copyright.

State Laws Regarding Internet Use
- Computer Crimes
- Obscenity Statute
Federal Laws Regarding Internet Use

- Child Pornography
- Obscenity
- Stalking
- Terrorism
- Computer Fraud and Abuse Act

Copyright

General Information

Privacy

- FERPA
- Gramm-Leach-Bliley
- Spam

Amendment to the Communications Act of 1934 (CDA)

Disciplinary Actions

Violation of this policy may result in disciplinary action that may include termination of employees or suspension or expulsion in the case of a student. Additionally, users are subject to loss of CTCD Information Technology Resources access privileges and may face civil and criminal prosecution.
IDENTIFICATION/AUTHENTICATION POLICY

Purpose
The purpose of the Identification/Authentication Policy is to ensure the security and integrity of Central Texas College District (CTCD) data and Information Technology Resources by ensuring controls for securing user identification and authentication credentials.

To ensure the security and integrity of CTCD data, identified users will securely authenticate to CTCD Information Technology Resources and access only resources which they have been authorized to access. If user identities are not properly authenticated, CTCD has no assurance that access to Information Technology Resources is properly controlled. This policy will mitigate the risk of unauthorized access of information, as well as establish user accountability and rules for access.

Scope
The Identification/Authentication Policy applies to all users of Central Texas College District Information Technology Resources.

Definitions
Authentication Credentials - The verification of the identity of a user who wishes to access a system, commonly using a password in conjunction with a unique UserID.

Data Steward - Departmental position responsible for classifying business data, approving access to data, and protecting data by ensuring controls are in place.

Mitigate - The elimination or reduction of the frequency, magnitude, or severity of exposure to risks in order to minimize the potential impact of a threat.

Principle of Least Privilege - The practice of limiting user profile privileges on computers to only the information and resources that are necessary, based on users’ job necessities.

Unauthorized Access - Access by a person who has not been given official permission or approval to access CTCD systems.

User Identification - A unique sequence of characters used to identify a user and allow access to a computer system or computer network.

Policy Statement
A. CTCD shall require that systems are protected from unauthorized access by establishing requirements for the authorization and management of user accounts, providing user authentication (any or all of the basic authentication methods), and implementing access controls on CTCD Information Technology Resources.
B. Access control is provided at the firewall, network, operating system, and application levels.

C. CTCD managers/supervisors have the responsibility of requesting access to information systems and approving user access privileges based upon their assigned duties, as well as notifying Data Owners and the CTC IT Help Desk of the termination of access to Information Technology Resources.

D. Prior to being granted access to CTCD Information Technology Resources, the needs of the employee, student worker, contractor, vendor, guest, or volunteer shall be given ample consideration and authorization granted to allow access to CTCD Information Technology Resources.

E. Access shall be granted according to the principle of least privilege.

F. CTCD accounts will have a unique identifier that is associated with a single user. Once an identifier is assigned to a particular person, it is always associated with that person. It is never subsequently reassigned to identify another person.

G. Use of any CTCD authentication source to identify oneself to a CTCD system constitutes an official identification of the user to Central Texas College, in the same way that presenting an ID card does.

H. Security is everyone’s responsibility, and everyone has a responsibility to protect their own “identity”. Users will be held accountable for all actions of their accounts.

I. Regardless of the authentication method used, users must use only the authentication information that they have been authorized to use; i.e., must never identify themselves falsely as another person. Additionally, users must keep their authentication information confidential; i.e., must not knowingly or negligently make it available for use by an unauthorized person. Anyone suspecting that their authentication information has been compromised should contact the CTC IT Help Desk immediately.

J. Users must adhere to the requirements of the CTCD HR Policy 294: Computer Security Policy and CTCD HR Policy 295: Computer Usage.

K. CTCD Data Stewards shall be responsible for ensuring that authorization and account management processes are documented and that the appropriate people have been assigned the responsibility of creating and maintaining authorization records. CTCD Data Stewards may monitor related activities of individuals as a condition for continued access. At a minimum, CTCD Data Stewards must review user access privileges annually.

Disciplinary Actions
Violation of this policy may result in disciplinary action that may include termination of employees or suspension or expulsion in the case of a student. Additionally, users are subject to loss of CTCD Information Technology Resources access privileges and may face civil and criminal prosecution.
INTRUSION DETECTION POLICY

Purpose
The purpose of this policy is to identify and respond to malicious activity targeted at computing and networking resources. It is intended to increase the level of security by actively searching for signs of unauthorized intrusion, preserve the integrity of organizational data on the network, prevent unauthorized use of organizational systems, keep hosts and network resources available to authorized users, and increase security by detecting weaknesses in systems and network design early.

Scope
The Intrusion Detection Policy applies to the CTC Information Technology Division Infrastructure staff.

Definitions
Information Technology Resources (IR) - Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to servers, personal computers, notebook computers, hand-held computers, smart phones, tablets, pagers, Internet of Things technology, distributed processing systems, network-attached and computer-controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit data.

Security Incident - In information operations, an assessed event of attempted entry, unauthorized entry, or an information attack on an automated information system. It includes unauthorized probing and browsing; disruption or denial of service; altered or destroyed input, processing, storage, or output of information; or changes to information system hardware, firmware, or software characteristics with or without the users’ knowledge, instruction, or intent.

Information Attack - An attempt to bypass the physical or information security measures and controls protecting an automated information system. The attack may alter, release, or deny data. Whether an attack will succeed depends on the vulnerability of the computer system and the effectiveness of existing countermeasures.

Information Operations - Actions taken to affect adversary information and information systems while defending one’s own information and information systems.

Intrusion Detection - Provides two important functions in protecting Information Technology Resources:
1. Feedback - information as to the effectiveness of other components of the security system. If a robust and effective intrusion detection system is in place, the lack of detected intrusions is an indication that other defenses are working.
2. Trigger - a mechanism that determines when to activate planned responses to an intrusion incident e.g. Security Incident Response Guidelines.

3. Host - A computer system that provides computer service for a number of users.

4. Server - A computer program that provides services to other computer programs in the same or another computer. A computer running a server program is frequently referred to as a server, though it may also be running other client (and server) programs.

5. Firewall - An access control mechanism that acts as a barrier between two or more segments of a computer network or overall client/server architecture, used to protect internal networks or network segments from unauthorized users or processes.

Policy Statement

A. All traffic that passes through the firewall will be monitored by an intrusion detection system.

B. All host-based and network-based intrusion detection systems must be checked on a regular basis and their logs reviewed. All servers will be monitored.

C. All intrusion detection logs must be kept for a minimum of 30 days.

D. All systems are monitored by anti-virus and data control monitoring software by the Information Security Officer.

E. Alarm, alert functions, and threat detection capabilities of firewalls and other network perimeter access control systems will be enabled.

F. Audit logging of any firewalls and other network perimeter access control systems must be enabled.

G. Audit logs from the perimeter access control systems must be monitored/reviewed regularly by the IT Network Engineer.

H. An annual vulnerability assessment or penetration test by a third party will be conducted to assess the potential for intrusion.

I. Audit logs for servers on the internal, protected, network are monitored by the network performance monitoring application.

J. Abnormal system activity and anomalous network traffic will be reviewed for symptoms that might indicate intrusive activity.
K. All suspected and/or confirmed instances of successful and/or attempted intrusions, suspicious activity, or unexplained erratic system behavior must be immediately reported according to the Security Incident Response Policy.

Disciplinary Actions
Violation of this policy may result in disciplinary action that may include termination of employees or suspension or expulsion in the case of a student. Additionally, users are subject to loss of CTCD Information Technology Resources access privileges and may face civil and criminal prosecution.
CENTRAL TEXAS COLLEGE DISTRICT LOGIN BANNER

Purpose
This page provides samples of login banner text that conforms to the requirements set forth in policy.

Scope
All users with systems connected to the Central Texas College District network.

Policy Statement
1. CTCD Direct Example
   “Unauthorized use of Central Texas College District computer and networking resources is prohibited. If you log on to this computer system, you acknowledge your awareness of and concurrence with the CTC HR Policy No. 295, Computer Usage. The College will prosecute violators to the full extent of the law.”

2. Public Network Access (PNA) Example
   “Access to the College's Public Network is restricted to Central Texas College students, faculty, staff, and sponsored guests. The wireless access point that you are using requires that you authenticate in order to use the Public Network.

   Unauthorized access to CTC computing and network resources is prohibited. By authenticating, you agree to abide by the College's policies as shown in CTC HR Policy No. 294, Computer Security Policy, and CTC HR Policy No. 295, Computer Usage.”
MALICIOUS CODE POLICY

Purpose
This policy is intended to provide information to college information technology resource administrators and users to improve the resistance to, detection of, and recovery from the effects of malicious code. Central Texas College District (CTCD) information technology resources are strategic assets that, as property of the State of Texas, must be managed as valuable State resources. The integrity and continued operation of college information technology resources are critical to the operation of CTCD. Malicious code can disrupt normal operation of college information technology resources. The number of information technology resource security incidents and the resulting cost of business disruption and service restoration continue to escalate. Implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents are some of the actions that can be taken to reduce the risk and decrease the cost of security incidents.

Scope
The Malicious Code Policy applies equally to all individuals utilizing CTCD Information Technology Resources (e.g. employees, faculty, students, alumni, agents, consultants, contractors, volunteers, vendors, temps, etc.). This policy does not apply to approved faculty research and academic programs where students and instructors develop and experiment with malicious programs in a controlled environment.

Policy Statement
The following requirements shall be adhered to at all times to ensure the protection of CTCD Information Technology Resources:

Prevention and Detection:
A. All desktops, wireless-enabled products, and laptops connected to the CTC network must use virus protection software.

B. Each file server attached to the CTC network must utilize CTC approved virus protection software and must be setup to detect and clean viruses that may infect file shares.

C. Software to safeguard against malicious code (e.g. antivirus, anti-spyware, etc.) shall be installed and functioning on susceptible information technology resources that have access to the College’s network.

D. All information technology resource users are prohibited from intentionally developing or experimenting with malicious programs (e.g. viruses, worms, spyware, keystroke loggers, phishing software, Trojan horses, etc.) unless a part of an approved research or academic program.

E. All information technology resource users are prohibited from knowingly propagating malicious programs including opening attachments from unknown sources.
F. Email attachments and shared files of unknown integrity shall be scanned for malicious code before they are opened or accessed.

G. Flash drives, external hard drives, and other mass storage devices will be scanned for malicious code before accessing any data on the media.

H. Software safeguarding information technology resources against malicious code shall not be disabled or bypassed by end-users.

I. The settings for software that protect information technology resources against malicious code shall not be altered in a manner that will reduce the effectiveness of the software.

J. The automatic update frequency of software that safeguards against malicious code shall not be disabled, altered or bypassed by end-users to reduce the frequency of updates.

Response and Recovery
A. All reasonable efforts shall be made to contain the effects of any system that is infected with a virus or other malicious code. This may include disconnecting systems from the network or disabling service.

B. If malicious code is discovered, or believed to exist, an attempt should be made to remove or quarantine the malicious code using current antivirus or other control software.

C. If malicious code cannot be automatically quarantined or removed by antivirus software, the system should be disconnected from the network to prevent further possible propagation of the malicious code or other harmful impact. The presence of the malicious code shall be reported to the Information Technology Division by contacting the IT Help Desk.

D. Personnel responding to an incident should be given the necessary access privileges and authority to afford the necessary measures to contain/remove the infection.

E. If possible, identify the source of the infection and the type of infection to prevent recurrence.

F. Any removable media (including flash drives, external hard drives, mass storage cards, etc.) recently used on an infected machine shall be scanned prior to opening and/or executing any files contained therein.

G. CTCD IT personnel shall thoroughly document an incident noting the source of the malicious code (if possible), resources impacted, and damage or disruption to information technology resources and submit a corresponding report to the Director of Information Technology in accordance with the Security Incident Response Guidelines.
Disciplinary Actions
Violation of this policy may result in disciplinary action that may include termination of employees or suspension or expulsion in the case of a student. Additionally, users are subject to loss of CTCD Information Technology Resources access privileges and may face civil and criminal prosecution.
MEDIA SANTIZATION AND DISPOSAL POLICY

Purpose
The purpose of this policy is to protect Central Texas College District data from unauthorized disclosure. This policy defines the requirements for ensuring College data are permanently removed from media before disposal or reuse, a process called "media sanitization," and properly disposing of media. The reuse, recycling, or disposal of computers and other technologies that can store data pose a significant risk since data can easily be recovered with readily available tools - even data from files that were deleted long ago or a hard drive that was reformatted. Failure to properly purge data in these circumstances may result in unauthorized access to College data, breach of software license agreements, and/or violation of state and federal data security and privacy laws.

Scope
This policy applies to all Central Texas College District employees and affiliate organizations.

Policy Statement
To prevent unauthorized disclosure of College data, media leaving control of Central Texas College and destined for reuse or disposal must have all College data purged in a manner that renders the data unrecoverable. Media that will be reused within the institution should likewise have all College data purged to prevent unauthorized disclosure.

Roles and Responsibilities
The Information Technology Division is responsible for ensuring that College data are properly removed or destroyed from media that is to be used no longer. Affiliated organizations such as the Europe, Pacific Far East, Service Area and Continental Campuses are required to follow the options below:

Implementation Procedures
A. Local Disposal
   1. Follow the instructions for purging data under specific instructions for media.
   2. Complete a Property Disposal Form and send it to Inventory Management.

B. Transfer of Media
   1. Follow the instructions for purging data under specific instructions for media.
   2. Send the media through a certified mailing service to the Information Technology Division at the Central Campus for proper disposal.
   3. Complete a Property Transfer Form and send it to Inventory Management.
Specific instructions for different types of media:

A. **Electronic Storage Media:** (hard disk drives in computers/servers, external hard drives, USB flash drives, magnetic tapes, etc.)
   1. If purging is done by overwriting the data, the entire media/device must be overwritten with a minimum of three passes.
   
   2. Equipment that can store College data, such as desktop and laptop computers or external hard drives, and is permanently leaving the control of the College should have all data storage devices removed before disposition. If the equipment leaving the College’s control must retain the data storage devices, all College data must be properly purged.
   
   3. The only acceptable methods for physically destroying a hard drive are shredding, pulverizing, disintegration, or incineration.
   
   4. Degaussing is an acceptable method of purging data from magnetic media. Be aware that this normally renders the media unusable.

B. **Paper-Based Media**
   
   1. Any paper-based or other hard copy media containing confidential College data must be shredded with a cross-cut shredder before disposal or transferred to an authorized third party contracted by the College for secure disposition of documents. The maximum particle size for paper-based media containing confidential data should be 1x5 mm (1/32"x1/5"). Media containing internal data should likewise be shredded with a cross-cut shredder if disclosure of the information contained therein might adversely impact the institution, an affiliated organization, or an individual. The maximum particle size for media containing internal data is 2x15 mm (1/16"x3/5").
   
   2. Incineration by methods compliant with all relevant health, safety, and environmental laws and regulations is an acceptable method for disposal of paper-based media.

C. **Optical Media** (e.g., CDs and DVDs)
   
   Optical media containing internal or confidential College data must be physically destroyed before disposal. An appropriate method of physical destruction is shredding with a cross-cut shredder.

D. **Smartphones and other handheld devices**
   
   Mobile devices like Smartphones (e.g., Android or iPhone/iPad), MP3 players, and even cell phones, store information and often contain personal or other sensitive information. Any College data must be purged from these devices before reuse or disposal, like any other storage media. It is also advisable to purge all other data from the device before reuse or disposal to protect your personal information.
E. **Other Media Types**  
For other media and additional guidelines, refer to [NIST Special Publication 800-88, Revision1: Guidelines for Media Sanitization](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf), Appendix A, Minimum Sanitization Recommendations.

F. **Export controls**  
Media containing College data in equipment that will be reused outside the United States must comply with export laws and regulations according to Export Control Guidelines in the CTCD [Acceptable Encryption Policy](https://www.ctcd.org/accepted/eicp.html).

G. **Electronic Protected Health Information**  
CTCD units responsible for electronic protected health information covered by HIPAA must also have media sanitization and disposal policies and procedures in accordance with HIPAA Security Final Rules, Section 164.310, *Physical Safeguards*, part (d), (1) & (2).

H. **Federal Tax Information**  
CTCD units handling Federal Tax Information must also have media sanitization and disposal policies and procedures in accordance with [IRS Publication 1075: Tax Information Security Guidelines for Federal, State, and Local Agencies](https://www.irs.gov/publications/p1075).

I. **More Information**  
For more information about media sanitization and disposal, including suggested software tools for purging hard drives and other CTCD-specific resources and procedures, contact the CTC IT Help Desk.
Definitions

**Affiliated Organization** - Any organization associated with the Central Texas College District that uses college information technology resources to create, access, store or manage College data to perform their business functions.

**College Data** - Any data related to Central Texas College District functions that are a) stored on College information technology systems, b) maintained by CTCD faculty, staff, or students, or c) related to institutional processes on or off campus. This applies to any format or media (in other words, it is not limited to electronic data).

**Degaussing** - Demagnetizing magnetic storage media like tape or a hard disk drive to render it permanently unusable. Since the media typically can no longer be used after degaussing, it should only be used to purge data from media that will be discarded.

**Disintegration** - A physically destructive method of sanitizing data; the act of separating into component parts.

**HIPAA** - Health Insurance Portability and Accountability Act of 1996 that among other things established standards for the security and privacy of human health-related information.

**Incineration** - A physically destructive method of sanitizing media; the act of burning completely to ashes.

**Media** - Material on which data are or may be recorded, such as magnetic disks or tapes, solid state devices like USB flash drives, optical discs like CDs and DVDs, or paper-based products.

**Media sanitization** - The process of removing data from storage media such that there is reasonable assurance that the data may not be retrieved and reconstructed.

**Pulverization** - A physically destructive method of sanitizing media; the act of grinding to a powder or dust.

**Purging** - A media sanitization process that removes all data and any remnant of the data so thoroughly that the effort required to recover the data, even with sophisticated tools in a laboratory setting (i.e., a "laboratory attack"), exceeds the value to the attacker. A common method of purging data is to overwrite it with random data in three or more passes.

**Disciplinary Actions**
Violation of this policy may result in disciplinary action that may include termination of employees or suspension or expulsion in the case of a student. Additionally, users are subject to loss of CTCD Information Technology Resources access privileges and may face civil and criminal prosecution.
CENTRAL TEXAS COLLEGE CERTIFICATE OF DESTRUCTION

Campus: ________________________________

Campus representative: ____________________________

Campus telephone number: ______________________________

Campus representative email: ______________________________

Date of destruction: ________________

Method of destruction:
( ) Disk Wiping
( ) Shredding
( ) Dismantle
( ) Other: ________________________________

<table>
<thead>
<tr>
<th>MODEL NUMBER</th>
<th>SERIAL NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

I, ________________________________, do hereby certify that the equipment listed above was destroyed in accordance with Central Texas College District policy, CTCD Hard Drive Destruction Policy.

______________________________
Signature

______________________________
Date

Central Texas College
Form ITD-0010
Information Technology Division
June 27, 2013
NETWORK CONFIGURATION POLICY

Introduction
The Central Texas College District network infrastructure is provided as a central utility for all users of the College’s information technology resources. It is important that the infrastructure, which includes cabling and the associated equipment such as routers and switches, continues to develop with sufficient flexibility to meet user demands while at the same time remaining capable of exploiting anticipated developments in high speed networking technology to allow the future provision of enhanced user services.

Purpose
The purpose of the CTCD Network Configuration Policy is to establish rules for the maintenance, expansion and use of the network infrastructure. These rules are necessary to preserve the integrity, availability, and confidentiality of CTCD data.

Scope
The CTCD Network Configuration Policy applies equally to all individuals with access to any of the College’s information technology resources. Additional requirements may apply depending on applicable laws, regulations, and/or standards.

Policy Statement
A. The CTC IT Infrastructure Department group is solely responsible for the CTCD network infrastructure and will continue to manage further developments and enhancements to this infrastructure.

B. To provide a consistent CTCD network infrastructure capable of exploiting new networking developments, all cabling must be installed by CTC IT Infrastructure Department, CTC Facilities Management or an approved contractor.

C. All network connected equipment must be configured to a specification approved by the CTC IT Infrastructure Department.

D. All hardware connected to the CTCD network is subject to CTC IT Infrastructure Department’s management and monitoring standards.

E. Changes to the configuration of active network management devices must not be made without the approval of the CTC IT Infrastructure Department.

F. The CTCD network infrastructure supports a well-defined set of approved networking protocols. Any use of non-sanctioned protocols must be approved by the CTC IT Infrastructure Department.

G. The networking addresses for the supported protocols are allocated, registered and managed centrally by the CTC IT Infrastructure Department.
H. All connections of the network infrastructure to external third party networks are the responsibility of the CTC IT Infrastructure Department. This includes connections to external telephone networks.

I. CTCD firewalls must be installed and configured in accordance with the CTC IT Infrastructure Department’s documentation.

J. The use of departmental firewalls is not permitted without the written authorization from CTC Infrastructure Department.

K. Users must not extend or re-transmit network services in any way. This means you must not install a router, switch, hub, or wireless access point to the CTCD network without approval from the CTC IT Infrastructure Department.

L. Users must not install network hardware or software that provides network services without approval from the CTC IT Infrastructure Department.

M. Users are not permitted to alter network hardware in any way.

Disciplinary Actions
Violation of this policy may result in disciplinary action that may include termination of employees or suspension or expulsion in the case of a student. Additionally, users are subject to loss of CTCD Information Technology Resources access privileges and may face civil and criminal prosecution.
PHYSICAL ACCESS POLICY

Purpose
The purpose of the CTCD Information Technology Physical Access Policy is to establish the rules for the granting, control, monitoring, and removal of physical access to Information Technology Resources facilities. Technical support staff, security administrators, system administrators, and others may have Information Technology Resources physical facility access requirements as part of their function. The granting, controlling, and monitoring of the physical access to Information Technology Resources facilities is extremely important to an overall security program.

Scope
The CTCD Information Technology Physical Access Policy applies to all individuals within the CTCD community that are responsible for the installation and support of Information Technology Resources, individuals charged with Information Technology Resources security and data stewards.

Policy Statement
   A. All physical security systems must comply with all applicable regulations such as, but not limited to, building codes and fire prevention codes.

   B. Physical access to all Information Technology Resources restricted facilities must be documented and managed.

   C. All Information Technology Resources facilities must be physically protected in proportion to the criticality or importance of their function at CTCD.

   D. Access to Information Technology Resources facilities must be granted only to CTCD support personnel and contractors, whose job responsibilities require access to that facility.

   E. Access cards and/or keys must not be shared or loaned to others.

   F. Access cards and/or keys that are no longer required must be returned to the person responsible for the Information Technology Resources facility.

   G. Access cards and/or keys must not be reallocated to another individual bypassing the return process.

   H. A service charge may be assessed for access cards and/or keys that are lost, stolen or are not returned.

   I. The IT Division will coordinate with CTC Facilities Management to remove card and/or key access rights of individuals that change roles within CTCD or are separated from their relationship with CTCD.

   J. Visitors must be escorted in card access controlled areas of Information Technology Resources facilities.
K. Signage for restricted access rooms and locations must be practical, yet minimal discernible evidence of the importance of the location should be displayed.

Disciplinary Actions
Violation of this policy may result in disciplinary action that may include termination of employees or suspension or expulsion in the case of a student. Additionally, users are subject to loss of CTCD Information Technology Resources access privileges and may face civil and criminal prosecution.
PLATFORM MANAGEMENT POLICY

Purpose

The focus of this policy is to ensure that appropriate management guidelines exist to maintain adequate security for the computer platforms connected to the Central Texas College District communications network.

Scope

Any individual assigned a computer (server or workstation) on the college network or accessing college resources using a non-college computer.

Policy Statement

A. Background

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

Given the number of computer workstations and servers that comprise the CTCD network, it is necessary to utilize a comprehensive patch management solution that can effectively distribute security patches automatically when they are made available. The patch management solution has the ability to evaluate individual computer workstations and servers for vulnerabilities. Effective security is a campus-wide effort involving the participation and support of every college employee and affiliate who is a user of the CTCD network.

B. Patch Management

Computer operating systems such as Microsoft Windows, Linux, Mac OS and many software application programs contain security flaws. Occasionally, a flaw permits a hacker to compromise security. A compromised computer threatens the integrity of the network and all computers connected to it. All operating systems and many software applications have periodic patches released by the vendor that need to be applied. Patches which are security related or critical in nature will be installed as deemed necessary by the Information Technology Division.

1. Patch Deployment

   a. Most patches or updates are typically released automatically by the IT Division through the use of a patch management application.

   b. In the event that a critical or security patch cannot be centrally deployed by the IT Division, it must be installed in a timely manner using the best resources available. In the case of non-
Microsoft desktop operating systems where a centralized deployment is not available, the installation should occur in a timely manner by the most appropriate method as determined by the IT Division.

2. Vulnerability Response Process
   a. If a user connected to the college’s network identifies a vulnerability, the user is required to call the IT Help Desk as soon as possible.

   b. If the IT Division, through its scans or other means, identifies a vulnerability on a computer connected to the campus network, the IT Division will take necessary action to alleviate or minimize the risk and notify the user.

C. Virus Protection
   1. Campus Community
      a. All workstations whether connected to the Central Texas College communications network, or standalone, must use the IT-approved virus protection software and configurations.

      b. The virus protection software shall not be disabled or bypassed.

      c. The settings for the virus protection software shall not be altered in a manner that will reduce the effectiveness of the software.

      d. The automatic update frequency of the virus protection software shall not be altered to reduce the frequency of updates.

      e. Every virus that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to the IT Help Desk.

   2. Internal Information Technology Division Servers
      Each file server attached to the college’s communications network must utilize IT-approved virus protection software and be setup to detect and clean viruses that may infect file shares.

Disciplinary Actions
Violation of this policy may result in disciplinary action that may include termination of employees or suspension or expulsion in the case of a student. Additionally, users are subject to loss of CTCD Information Technology Resources access privileges and may face civil and criminal prosecution.
PORTABLE COMPUTING POLICY

Introduction
Portable computing devices are becoming increasingly powerful and affordable. Their small size and functionality are making these devices ever more desirable to replace traditional desktop devices in a wide number of applications. However, the portability offered by these devices may increase the security exposure to groups using the devices.

Purpose
The purpose of the Central Texas College Portable Computing Security Policy is to establish the rules for the use of mobile computing devices and their connection to the network. These rules are necessary to preserve the integrity, availability, and confidentiality of the College’s Information Technology Resources.

Scope
The CTCD Portable Computing Security Policy applies equally to all individuals that utilize Portable Computing devices and access the College’s Information Technology Resources.

Policy Statement
A. Portable computing devices must be password protected.

B. College-issued mobile computing devices must be encrypted.

C. CTCD data should not be stored on portable computing devices. However, in the event that there is no alternative to local storage, all confidential CTC data must be encrypted using approved encryption techniques.

D. Any personally-owned computing devices on which Confidential College Data will not be stored on personally-owned computing devices.

E. CTCD data must not be transmitted via wireless to or from a portable computing device unless approved wireless transmission protocols, along with approved encryption techniques, are utilized.

F. Unattended portable computing devices must be physically secure and must enable a password protected screen saver. This means they must be locked in an office, locked in a desk drawer or filing cabinet, or attached to a desk or cabinet via a cable lock system.
Disciplinary Actions
Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of College Information Technology Resources access privileges, civil, and criminal prosecution.
REMOTE ACCESS POLICY

Purpose
The purpose of this policy is to define standards for connecting to Central Texas College District network from any host. These standards are designed to minimize the potential exposure to the College from damages which may result from unauthorized use of CTCD resources. Damages include the loss of confidential data, intellectual property, damage to public image, damage to critical internal systems, etc.

Scope
This policy applies to all CTCD Information Technology Resources users (e.g., employees, students, contractors, vendors, agents, guests, etc.) who access college resources with any device whether university-owned or personally-owned. Remote access implementations that are covered by this policy include, but are not limited to DSL, VPN, SSH, cable modems, etc.

Policy Statement

General
C. It is the responsibility of CTCD Information Technology Resources users with remote access privileges to college resources ensure that their remote access connection are given the same consideration as the user's on-site connection.

D. By using CTCD Information Technology Resources, users agree to bear the responsibility for the consequences should the access be misused.

E. Users should review the following policies for details of protecting information when accessing the network via remote access methods, and acceptable use of the Central Texas College's network:
   1. Acceptable Encryption Policy
   2. Computer Security Policy
   3. Virtual Private Network (VPN) Policy
   4. Wireless Communications Policy

Requirements
A. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the How to Create a Secure Password Tech Tip on the CTC IT Division website.

B. At no time should any Central Texas College District employee provide their login or email password to anyone, not even family members.

C. Users with remote access privileges must ensure that their Central Texas College-owned or personal computer, workstation or device, which is remotely connected to CTCD Information Technology
Resources, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.

D. Users with remote access privileges to CTCD Information Technology Resources (e.g., network, etc.) must not use non-CTCD email accounts (i.e., Hotmail, Yahoo, Gmail, etc.), or other external resources to conduct college business; thereby ensuring that official business is never confused with personal business, and that college information/information resources are not placed at risk.

E. All hosts that connect to CTCD Information Technology Resources via remote access technologies must have the anti-virus software signatures or definitions updated daily.

F. Note that these requirements also apply to personal computers.

G. Third party connections must comply with requirements as stated in the [Vendor and Third-Party Controls and Compliance Policy](#).

H. Personal equipment that is used to connect to CTCD Information Technology Resources must meet the same requirements of CTCD-owned equipment for remote access. Organizations or individuals wishing to implement non-standard remote access solutions on CTCD Information Technology Resources must obtain prior approval from the IT Division.

**Disciplinary Actions**

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of College Information Technology Resources access privileges, civil, and criminal prosecution.
RISK ASSESSMENT POLICY

Purpose
The purpose of the IT Risk Assessment Policy is to empower the Information Technology Division to perform periodic information security risk assessments (RAs) for the purpose of determining areas of vulnerability and to initiate appropriate remediation.

Scope
Information security risk assessments can be conducted on any entity within the Central Texas College District or any outside entity that has signed a Third Party Agreement with CTCD. Information security risk assessments can be conducted on any information system, to include applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained.

Policy Statement
The execution, development and implementation of remediation programs are the joint responsibility of the IT Division and the department responsible for the systems area being assessed. Employees are expected to cooperate fully with any risk assessment being conducted on systems for which they are held accountable. Employees are further expected to work with the IT Division in the development of a remediation plan.

Disciplinary Actions
Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of College Information Technology Resources access privileges, civil, and criminal prosecution.
SECURITY MONITORING POLICY

Purpose
The purpose of the IT Security Monitoring Policy is to ensure that Information Technology Division security controls are in place, are effective, and are not being bypassed. One of the benefits of security monitoring is the early identification of security issues or new security vulnerabilities.

This early identification can help to prevent a security issue or vulnerability before harm can be done, or to minimize the potential impact. Other benefits include Audit Compliance, Service Level Monitoring, Performance Measuring, Limiting Liability, and Capacity Planning.

Scope
The Central Texas College District Security Monitoring Policy applies to all individuals that are responsible for the installation of new Information Technology Resources, the operations of existing Information Technology Resources, and individuals charged with Information Technology Security.

Policy Statement
Automated tools will provide real time notification of detected security issues and vulnerability exploitation. Where possible a security baseline will be developed and the tools will report exceptions. These tools will be deployed to monitor:

- Internet traffic
- Electronic mail traffic
- LAN traffic, protocols, and device inventory
- Operating system security parameters including security software

The following files will be checked for signs of security issues and vulnerability exploitation at a frequency determined by risk:

1. Automated intrusion detection system logs
2. Firewall logs
3. User account logs
4. Network scanning logs
5. System error logs
6. Application logs
7. Data backup and recovery logs
8. Help Desk Service Requests
9. Telephone activity - Call Detail Reports

Any security issues discovered will be reported to the Director of Information Technology for follow-up investigation.
Disciplinary Actions
Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of CTCD Information Technology Resources access privileges, civil, and criminal prosecution.
SECURITY UPDATES POLICY

Purpose
The purpose of the IT Security Updates Policy is to ensure that Information Technology Resources are up to date with issued updates and patches from vendors. This early identification can help to prevent a security issue or vulnerability before harm can be done, or to minimize the potential impact.

Scope
The IT Security Updates Policy applies to the CTC Information Technology Division Staff.

Policy Statement
A. The Information Security Officer will check for software updates weekly for:
   a. Adobe
   b. AIX
   c. Cisco
   d. Java
   e. Linux (Red Hat)
   f. Microsoft

B. Pertinent information will be entered in the Security Updates Report in SharePoint if the software manufacturers listed above have issued updates.

C. If an update is entered in the Security Updates Report then an email will be automatically sent to the following at 4:30 p.m. on the date of entry.
   a. Director of Information Technology
   b. IT Network Engineer
   c. IT Systems Engineers
   d. IT Windows System Administrator
   e. Systems Programmer

D. Updates will be designated as:
   a. Critical
   b. Important
   c. Moderate
   d. Low

E. Updates will be treated accordingly based on their designation.
   1. Critical Updates
      a. Critical updates must be reviewed on date of issue from SharePoint Administrator. If an administrator knows a critical update has been issued but has not received notification from SharePoint Administrator then the critical update must still be reviewed.
b. Critical updates must be applied within 48 hours of review, if applicable, and the installation date must be annotated on the Security Updates Report in SharePoint.

c. If the critical update is not applicable then it must be annotated on the comments section of the Security Updates Report on SharePoint.

2. Important Updates
   a. Administrators have 48 hours to review important updates.
   
b. Important updates must be applied with 96 hours of notification.
   
c. The installation date must be annotated in the Security Updates Report in SharePoint.
   
d. Administrators must annotate in the comments section of the Security Updates Report in SharePoint if the important update is not applicable.

3. Moderate/Low Updates
   a. Updates designated Moderate or Low must be reviewed within one (1) week of notification.
   
b. Moderate and Low updates can be applied during the next scheduled installation date.
   
c. If a Moderate or Low update is not applicable then it must be annotated in the comments section of the Security Updates Report in SharePoint.

<table>
<thead>
<tr>
<th>Update Type</th>
<th>Review Period</th>
<th>Update Installation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>Immediate (Same workday received)</td>
<td>48 hours</td>
</tr>
<tr>
<td>Important</td>
<td>48 hours</td>
<td>96 hours</td>
</tr>
<tr>
<td>Moderate</td>
<td>1 week</td>
<td>Next scheduled installation date</td>
</tr>
<tr>
<td>Low</td>
<td>1 week</td>
<td>Next scheduled installation date</td>
</tr>
</tbody>
</table>
Disciplinary Actions
Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of CTCD Information Technology Resources access privileges, civil, and criminal prosecution.
SERVER SECURITY POLICY

Purpose
The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by Central Texas College District. Effective implementation of this policy will minimize unauthorized access to confidential, PCI, proprietary, and other information and technology.

Scope
This policy applies to server equipment owned and/or operated by the Central Texas College District, and to servers registered under any CTCD-owned internal network domain. This policy is specifically for equipment on the internal CTCD network.

Policy Statement
A. A server must be protected and cannot be connected to the CTCD network until it meets the standards set in the IT Minimum Security Standards for Systems.

B. The Minimum Security Standards for Systems provides the detailed information required to harden a server. Some of the general steps in this standard include, but are not limited to:

   1. Installing the operating system from an ITD approved source
   2. Applying vendor supplied patches
   3. Anti-virus software must be installed and enabled
   4. Removing unnecessary software, accounts, system services, and drivers
   5. Setting security parameters, file protections, firewall, and enabling audit logging
   6. Disabling or changing the password of default accounts
   7. Insure appropriate permissions are granted on the system as well as any share folders
   8. Servers should be physically located in an access-controlled environment.
   9. Servers are specifically prohibited from operating from uncontrolled areas (e.g., cubicles, under desks, etc.).

C. Servers will be classified, secured, and protected by data stewards/owners, IT owners and custodians accordingly based on the highest level of data residing on the system.

D. The Information Security Officer will monitor security issues, both internal to CTCD and externally. The ISO or other approved team will manage the release of security patches on behalf of CTCD.

E. Security patches must be implemented within the specified timeframe of notification from the ISO in accordance with the IT Security Updates Policy.

F. Configuration changes for production servers must follow the CTC IT Change Management Policy.
G. Security-related events will be reported to the Information Security Officer, who will review logs and report incidents as appropriate. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:

- Port-scan attacks
- Evidence of unauthorized access to privileged accounts
- Anomalous occurrences that are not related to specific applications on the host.

H. All security-related events on critical or confidential systems must be logged and audit trails saved.

**Disciplinary Actions**
Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of CTCD Information Technology Resources access privileges, civil, and criminal prosecution.
SYSTEM DEVELOPMENT AND DEPLOYMENT POLICY

Purpose
Central Texas College must adopt institutional policies, standards and/or procedures to ensure that the protection of Information Technology Resources (including data confidentiality, integrity, and availability) is considered during the development or purchase of new Information Systems or services.

Scope
All users with systems connected to the Central Texas College District network.

Policy Statement
A. Redundant Information Systems or Services

Information Systems that duplicate services provided by the CTCD Information Technology Division are discouraged because they increase opportunity for exposure of data. The IT Division must ensure that the protection of Information Technology Resources (including data confidentiality, integrity, and accessibility) is considered during the development or purchase of new computer applications. The following procedures are required:

1. All associated systems and applications must restrict access and must provide methods for appropriately restricting privileges of authorized users. Access to applications is granted on a need-to-access basis.

2. All applications processing Class III Data must comply with the HR No. 294, Computer Security Policy.

3. Separate production and test environments will be maintained to ensure the security and reliability of the central production system. Whenever possible, new development or modifications to a production system will be made first in a test environment. These changes should be thoroughly tested for valid functionality before being released to the production environment.

4. Information technology outsourcing contracts must address security, backup, and privacy requirements, and should include a right for Central Texas College to conduct a security assessment or a right to review security assessments performed by third parties, or other provisions to provide appropriate assurances that applications and data will be adequately protected when Confidential Data is associated.

Vendors must adhere to all Federal and State laws and rules pertaining to the protection of Information Resources and privacy of Confidential Data.
B. Security Review and Approval.
The Director of Information Technology has the right to call for a review and approve security requirements, specifications, and, if applicable, third-party risk assessments for any new computer hardware, software, applications, or services that are mission critical or that receive, maintain, and/or share Confidential Data.

Disciplinary Actions
Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of CTCD Information Technology Resources access privileges, civil, and criminal prosecution.
Appendix A.

IT INFORMATION SYSTEMS TURNOVER SOP

Purpose
To document the process of moving Colleague packages to test and live environments. Further move, email layout, and environment details can be found within the IT Information Systems Turnover Procedures manual.

Scope
This document is intended for new and current IT Information Systems and IT Infrastructure Department employees.

Procedure Statement
1. Test Environment Moves
   a. The IT Software Process Coordinator builds and sends the IT Infrastructure Support Specialist a package to move into testing. The information needed for the move is included in the email.
   b. If the IT Infrastructure Support Specialist is out, an IT System Engineer will receive the move request. The IT Infrastructure Support Specialist (or one of the previously mentioned IT Infrastructure personnel) replies to the IT Software Process Coordinator via email that the move request has been received.
   c. The package is moved into the specified test environment and a confirmation of the move is emailed to the IT Software Process Coordinator. This process is to be completed within approximately an hour’s time.

2. Live Environment Moves
   a. The IT Software Process Coordinator emails move and project details to the IT Information Systems Director for approval. If the IT Information Systems Director approves the move, the IT Software Process Coordinator builds and sends the IT Infrastructure Support Specialist the package to move into live. The information needed for the move is included in the email.
b. If the IT Infrastructure Support Specialist is out, an IT System Engineer will receive the move request. The IT Infrastructure Support Specialist (or one of the previously mentioned IT Infrastructure personnel) replies to the IT Software Process Coordinator via email that the move request has been received.

The package is moved into the specified live environment and a confirmation of the move is emailed to the IT Software Process Coordinator. This process is to be completed within approximately an hour’s time.
VENDOR AND THIRD-PARTY CONTROLS AND COMPLIANCE POLICY

Purpose
Central Texas College recognizes that vendors and other contractors serve an important function in the development and/or support of services, hardware, and software and, in some cases, the operation of computer networks, servers, and/or applications.

Scope
This standard applies to contracts entered into by Central Texas College that involves third-party access to or creation of Information Technology Resources or College Data by a third-party.

Policy Statement
A. Contracts
   1. Contracts of any kind, including purchase orders, memoranda of understanding (MOU), letters of agreement, or any other type of legally binding agreement, that involve current or future third-party access to or creation of Information Technology Resources and/or Data must include terms determined by Business Services and Contracting Office as sufficient to ensure that vendors and any subcontractors or other third-parties that maintain, create, or access College Data as the result of the contract comply with all applicable Federal and State security and privacy laws, this policy, and any applicable Central Texas College District Policies or Standards, and must contain terms that ensure that all College Data affected by the contract is maintained in accordance with those standards at all times, including post-termination of the contract.

   2. The Data Steward, Business Services and Contracting Office, and the Director of Information Technology are jointly and separately responsible for ensuring that all contracts are reviewed to determine whether the contract involves third-party access to, outsourcing, maintenance, or creation of College Data; and that all such access, outsourcing, or maintenance fully complies with CTCD policies and standards at all times.

   3. Any contract involving third-party access to, creation, or maintenance of Protected Health Information (PHI) as defined in 45 C.F.R. § 164.501, must include a Health Insurance Portability and Accountability Act (HIPAA) business associate agreement in a form approved by CTCD counsel.

   4. Any contract involving third-party-provided credit card services must require that the Contractor provides assurances that all subcontractors who provide credit card services pursuant to the contract will comply with the requirements of the Payment Card Industry Data Security Standard (PCI DSS) in the provision of the services.
B. Vendor or other Third-Party Assessment
   1. Prior to access, maintenance, or creation of College Data by a Vendor or any other third-party, the College must perform an assessment to ensure that:
      a. The Vendor has sufficient technological, administrative, and physical safeguards to ensure the confidentiality, security, and integrity of the Data at rest and during any transmission or transfer; and
      b. Any subcontractor or other third-party that will access, maintain, or create Data pursuant to the contract will also ensure the confidentiality, security, and integrity of such Data while it is at rest and during any transmission or transfer.

   2. As part of the College’s assessment of a vendor or other third-party, the College will request copies of any self-assessments or third-party assessments that the vendor or third-party has access to.

C. Access Control Measures
   Each institutional unit must control vendor and other third-party access to its Data based on Data sensitivity and risk. Controls must incorporate the following:

   Vendor must represent, warrant, and certify it will:

   1. Hold all Confidential Data in the strictest confidence
   2. Not release any Confidential Data unless Vendor obtains the College’s prior written approval and performs such a release in full compliance with all applicable privacy laws, including the Family Educational Rights and Privacy Act (FERPA);
   3. Not otherwise use or disclose Confidential Data except as required or permitted by law
   4. Safeguard Data according to all commercially reasonable administrative, physical, and technical standards (e.g., such standards established by the National Institute of Standards and Technology or the Center for Internet Security)
   5. Continually monitor its operations and take any action necessary to assure the Data is safeguarded in accordance with the terms of Central Texas College Security Policy
   6. Comply with the Vendor access requirements that are set forth in this policy
D. Access for Third-Parties
If CTCD intends to provide College Data to a third-party acting as an agent of or otherwise on behalf of Central Texas College (example: an application service provider) a written agreement with the third-party is required.

Such third-party agreements must specify:

1. The Data authorized to be accessed;
2. The circumstances under and purposes for which the Data may be used; and
3. That all Data must be returned to Central Texas College, or destroyed, in a manner specified by Central Texas College upon end of the third-party engagement.

If Central Texas College determines that its provision of Data to a third-party will result in significant risk to the confidentiality, integrity, or availability of such Data, the agreement must specify terms and conditions, including appropriate administrative, physical, and technical safeguards for protecting the Data.

E. Breach Notification
The following shall be required of the Vendor. If an unauthorized use or disclosure of any Confidential Data occurs, the Vendor must provide:

1. Written notice within one business day, or if the Data Stewards, CTCD procurement officers, and the CTC Information Technology Division are satisfied that a longer period is acceptable, within that period, after Vendor’s or third-party’s discovery of such use or disclosure; and,
2. All Information Central Texas College requests concerning such unauthorized use or disclosure.

F. Return of Data
Within 30 days after the termination or expiration of a purchase order, contract, or agreement for any reason, the vendor must either:

1. Return or securely destroy, as specified by contract or agreement, all Data provided to the Vendor by the College, including all Confidential Data provided to the vendor’s employees, subcontractors, agents, or other affiliated persons or institutions; or
2. In the event that returning or securely destroying the Data is infeasible, provide notification of the conditions that make return or destruction infeasible, in which case the Vendor or third-party must:
a. Continue to protect all Data that it retains

b. Agree to limit further uses and disclosures of such Data to those purposes that make the return or destruction infeasible for as long as Vendor or other third-party maintains such Data

c. To the extent possible, de-identify such Data

Disciplinary Actions
Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of CTCD Information Technology Resources access privileges, civil, and criminal prosecution.
WIRELESS COMMUNICATION POLICY

Purpose
The purpose of the Wireless Communication Policy is to provide the best possible quality of wireless network service, ensure wired and wireless network security and integrity, and minimize interference between the campus wireless network and other products deployed throughout campus.

Scope
This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, tablets, etc.) connected to any of the College’s Information Technology Resources. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to CTCD’s Information Technology Resources do not fall under the purview of this policy except that wireless access points or networks operating on campus without permission of the Information Technology Division or any device found to be interfering with the CTCD wireless networks are within the scope of this policy and subject to confiscation and removal from service.

Policy Statement
Installation, engineering, maintenance, and operation of wired and wireless networks serving CTCD faculty, staff, or students, on any property owned or tenanted by the College, are the sole responsibility of the CTC Information Technology Division. Individuals and departments are prohibited from extending college communications network without written permission.

Standards
For equipment supported by the IT Division please contact the IT Help Desk.

Disciplinary Actions
Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of CTCD Information Technology Resources access privileges, civil, and criminal prosecution.
IT SECURITY PROGRAM GUIDELINES
DATA ENCRYPTION GUIDELINES

Purpose
This guideline serves as a supplement to CTC HR No. 294, Computer Security Policy and the CTC IT Acceptable Encryption Policy. Adherence to these guidelines will better assure the confidentiality and integrity of the College's sensitive data should data encryption be used as an information protection control.

The objective of this guideline is to provide guidance in understanding encryption and the encryption key management required for maintaining the confidentiality and integrity of the College's sensitive data.

The most reliable way to protect the College's Confidential Data is to avoid handling sensitive College data. Confidential Data should be retained or handled only when required. Encryption can be an effective information protection control when it is necessary to possess sensitive college data.

However, Data Stewards and Data Managers should understand that data encryption is not a substitute for other information protection controls, such as access control, authentication, or authorization; that data encryption should be used in conjunction with those other controls; and that data encryption implementations should be proportional to the protection needs of the data.

Scope
These guidelines apply to all devices, physical or virtual where College Data is classified as defined by CTC HR No. 294, Computer Security Policy.

Requirements
A. Encryption Applicability

1. Transmission: In order to protect the confidentiality and integrity of the College's sensitive data; any data classified as Class III Data, and having a required need for confidentiality and/or integrity, shall be transmitted via encrypted communication to ensure that is does not traverse the network in clear text. It is further recommended, but not required, that data classified as Class II be transmitted via encrypted communications when possible. See CTC HR No. 294, Computer Security Policy, for further clarification on the classification of college data. Applications of encryption for data transmission include, but are not limited to, those identified in APPENDIX-A.

2. Storage: In order to protect the confidentiality and integrity of the College's Data; any data classified as Class III Data, and having a required need for confidentiality and/or integrity, shall be stored encrypted in systems and/or databases and/or portable media. Class II and Class I Data classifications do not require such encrypted storage. See CTC HR No. 294, Computer Security Policy, for further clarification on data classification. Applications of encryption for data storage include, but are not limited to, those identified in APPENDIX-B.
3. A combination of business practices and technology can act as mitigating factors and could significantly reduce the risk of unauthorized data exposure, thereby offsetting the specific need to implement data encryption. Examples of such mitigating factors include, but are not limited to, those identified in APPENDIX-C.

B. Encryption Services

1. The symmetric algorithms referenced in APPENDIX-D shall be used for encrypting Class III Data.

2. The algorithms referenced in APPENDIX-E shall be used for public key asymmetric encryption of Class III Data.

3. The encryption services referenced in APPENDIX-F shall be used for digital signature purposes when private information is involved.

4. Digital signatures shall be used to associate a user or entity with a respective public key.

5. Digital certificates shall apply recognized standards (e.g., X.509v3) and shall at least:

   a. Identify the issuing certificate authority; the certificate authority shall be one authorized by DIR or strictly designated for internal CTCD usage

   b. Identify its subscriber

   c. Provide the subscriber's public key

   d. Identify its operational period

   e. Be digitally signed by the issuing certificate authority
C. Encryption Key Management

1. Encryption keys used to protect confidential data shall also be considered Class III Data.

2. Professional key management is critical to prevent unauthorized disclosure of Class III Data or irretrievable loss of important data. The College Data managed by all key management infrastructures shall be considered both Class III Data and mission critical.

3. The IT Infrastructure Department shall create and implement an encryption key management plan to address the requirements of these encryption guidelines, CTCD regulations, and applicable State and Federal law.
   
   a. The encryption key management plan shall ensure data can be decrypted when access to data is necessary. Backup or other strategies (e.g., recovery agents) shall be implemented to enable decryption; thereby ensuring data can be recovered in the event of loss or unavailability of encryption keys.
   
   b. The encryption key management plan shall address handling the compromise or suspected compromise of encryption keys. The plan shall address what actions shall be taken in the event of a compromise (e.g., with system software and hardware, private keys, or encrypted data.)
   
   c. The encryption key management plan shall also address the destruction or revocation of encryption keys that are no longer in use (e.g., the user has left the college) or that aren't associated with a key management program.

4. All symmetric encryption keys used on systems associated with Class III Data shall be randomly generated according to industry standards. Acceptable standards include, but are not limited to, those referenced in APPENDIX-G.

5. Where symmetric encryption is used to protect Class III Data:
   
   a. Master keys shall be changed at least once per year.
   
   b. Key encrypting keys shall be changed at a minimum of twice per year.
   
   c. Data encrypting keys shall be changed once per session or every 24 hours.

6. When asymmetric encryption is used, the operational period of asymmetric keys associated with a public key certificate are defined by the encryption key management plan of the issuing certificate authority.

7. Encryption keys shall be stored within an encrypted key store or an otherwise encrypted form using approved algorithms; or the keys may be stored on a security token (e.g., a smart card). The encryption keys shall never leave the device if stored on a security token.
This requirement does not pertain to keys (e.g. SSH host keys) or protocols (e.g. encryption used by backup technologies) that are providing layers of encryption transport in addition to the strong encryption that has already been applied to Confidential Data.

8. Encryption keys are confidential information, and access shall be strictly limited to those who have a need-to-know.

9. Encryption keys that are compromised (e.g., lost or stolen) shall be reported immediately to the Information Technology Division and the Data Steward of the data being protected. The key shall be revoked or destroyed and a new key generated. Key re-assignments shall require re-encryption of the data.

D. Legal Requirements
The encryption systems used by the IT Division must comply with applicable laws and regulations. Any export or import of encryption products (e.g., source code, software, or technology) must comply with the applicable laws and regulations of the countries involved, including those countries represented by foreign nationals affiliated with the College. The United States Department of Commerce provides additional guidance specific to such encryption export controls, http://www.bis.doc.gov/encryption/.
Responsibilities

A. Information Security Officer
   2. Assess the secure installation and maintenance of all equipment supporting encryption controls in the IT Division.
   3. Assess the performance and security monitoring for all elements of the encryption control processes.
   4. Assess all related key management processes.
   5. The Information Security Officer, acting on behalf of the College, reserves the right to refuse any encryption request that may compromise the security of the College's networks or sensitive data.

B. Senior Systems Administrator
   1. Adherence to the College’s Data Encryption Guidelines and related policies established by the college.
   2. Ensure secure installation and maintenance of all respective equipment supporting encryption controls.
   3. Ensure performance and security monitoring for all respective elements of the encryption control process.
   4. Ensure all related key management processes can be accounted for in detail and, if possible, that no single key management supporting staff member can individually obtain full access to master keys or Certificate Authority encryption keys (e.g., separation of duties, dual control, etc.).

C. User Responsibilities
   1. All users shall adhere to the college's Data Encryption Guidelines and related policies established by Central Texas College.
   2. All users shall be familiar with the college's CTC HR No. 294, Computer Security Policy.
   3. All users must manage the storage and transmission of data files in a manner which safeguards and protects the confidentiality, integrity, and availability of such files.
   4. Questions about the classification of a specific piece of data should be addressed to the local supervisor or respective Data Steward. Questions about these guidelines should be addressed to the Information Security Officer.
APPENDICES
APPENDIX A: Application of Encryption for Data Transmission

1. File Transfers
   Encryption of confidential file transfers can be achieved via the use of an encrypted transmission protocol or network service (e.g., SCP, SFTP, etc.) or by transferring a Confidential File that has been encrypted prior to the transmission.

2. E-mail
   Confidential Data transmitted in e-mail messages shall be encrypted prior to transmission, presented via a secure web application, or encrypted in a secure message format, given e-mail is exposed to the possibility of unauthorized access at a number of points throughout the delivery process. The IT Division recommends that users use Encryption Wizard to encrypt files that will be sent through e-mail.

3. Interactive Sessions
   Encryption of Confidential Data, including login passwords, transmitted during remote login sessions (e.g., Telnet, TN3270, and remote control software for PCs) shall be provided through the use of secure applications or protocols.

4. Web-Based Applications
   Encryption of Confidential Data communicated between a user's browser and a web-based application shall be provided through the use of secure protocols (e.g., HTTPS, TLS/SSL, etc.) The display of Confidential Data shall be limited to only what is required by the user's authorized use of the application.

5. Remote File Services
   Encryption of Confidential Data transmitted by remote files services shall be provided through the use of encrypted transmission protocols (e.g., IPSec, ISAKMP/IKE, SSL/TLS) to prevent unauthorized interception.

6. Database Access
   Encryption of Confidential Data transmitted between an application server and a database shall be implemented to prevent unauthorized interception. Such encryption capabilities are generally provided as part of, or an option to, the database server software.

7. Application-to-Application Communications
   Encryption of Confidential Data transmitted between cooperating applications shall be provided through the use of commonly available encrypted protocols (e.g., SOAP with HTTPS) to prevent unauthorized interception.

8. Virtual Private Network (VPN)
A VPN connection offers an additional option to protecting Confidential Data transmitted via the network when other alternatives are not feasible. Users shall contact the IT Help Desk to create a VPN access and receive instructions.

APPENDIX B: Applications of Encryption for Data Storage

1. Whole Disk Encryption
   Encryption of Class III Data stored on portable computing devices (e.g., PDAs, tablet PCs, laptops, and smart phones), as well as storage media, (e.g., CDs, DVDs, and USB drives) shall be provided through the use of a whole disk encryption tool or one that can at least be configured to encrypt all Confidential Data.

2. File Encryption
   Encryption of Confidential Data shall be provided to facilitate the secure transport of individual files over a network without transmission encryption or to off-line storage devices (e.g., CDs, DVDs, or USB drives.) Encryption Wizard is an excellent tool for file encryption.

3. Database Storage
   Encryption of Confidential Data contained in a database server shall be provided through the use of whole disk encryption or through features native to the database server software. Encryption capabilities native to database server software may allow for encryption of specific tables or columns of a database and may also be required to segregate access rights among multiple applications that utilize a single database server.

4. Backup and Archiving
   Encryption of Confidential Data contained in backups and/or archives copies shall be provided to prevent unauthorized access.

APPENDIX C: Examples of Potential Mitigating Factors

- Firewall Restricting Capabilities
- Detailed Audit Logging
- Detailed Process Logging
- Intrusion Detection Capabilities
- Intrusion Prevention Capabilities
- Integrity Checking Capabilities
- Separation of Sensitive Duties
- Physical Security Capabilities
APPENDIX D: Symmetric Algorithms
- AES (128, 192, or 256 bit)
- RC6 (256 bit)
- Serpent (128, 192, or 256 bit)
- Twofish (128, 192, or 256 bit)

APPENDIX E: Public Key Asymmetric Algorithms
- RSA (minimum 1024 bit)
- ECC (minimum 384 bit)

APPENDIX F: Digital Signature Algorithms
- RSA (minimum 1024 bit) with SHA-2
- DSA (minimum 2048 bit) with SHA-2
- ECDSA (minimum 384 bit) with SHA-2

APPENDIX G: Industry Standards for Symmetric Key Generation
- FIPS 186-2
- ANSI X9.31
- ANSI X9.62
- ANSI X9.82

Definitions
Asymmetric Encryption - The problem with secret keys is exchanging them over the Internet or a large network while preventing them from falling into the wrong hands. Anyone who knows the secret key can decrypt the message. One answer is asymmetric encryption, in which there are two related keys—a key pair. A public key is made freely available to anyone who might want to send the user a message. A second, private key is kept secret, so that only the user knows it.

Any message (text, binary files, or documents) that are encrypted by using the public key can only be decrypted by applying the same algorithm, but by using the matching private key. Any message that is encrypted by using the private key can only be decrypted by using the matching public key. This means that a user does not have to worry about passing public keys over the Internet (the keys are supposed to be public). A problem with asymmetric encryption, however, is that it is slower than symmetric encryption. It requires far more processing power to both encrypt and decrypt the content of the message.

Class I Data – Public information. Information made available either to the public or to specific individuals who need it with few, if any, restrictions. The published class schedule is an example of Class I Data.

Class II Data – Limited distribution information. The loss, corruption, or unauthorized disclosure of this information would not affect the operational effectiveness of CTCD. A document detailing a fund-raising strategy is an example of Class II Data.
Class III Data – Private information. Information that is confidential and protected from external access and unauthorized internal access. Loss, corruption, or unauthorized disclosure of this information would impair the business or research functions of CTCD; result in business, financial, or legal loss; or be a violation of federal or state laws/regulations or CTCD contracts. Data integrity is vital. An example of private information would be a student’s academic record.

Data Stewards (Owners) – Data stewards are users who own, manage, and grant access to data. Data Stewards consist primarily of division directors, deans, and Colleague functional custodians (i.e., users that oversee an entire Colleague module, such as the Colleague Financials, or a functional subset, such as Accounts Payable). Data Stewards are responsible for classifying and labeling the data for which they are responsible; determining which users are authorized to have access to their data; directing the Information Technology Division to grant or remove access for their authorized users; informing their users of the classification of data they can access and the rules that correspond with protecting Class II Data or Class III Data from unauthorized access or usage; collaborating with the Information Technology Division to establish specific information security policies and procedures for the Information Technology Resources they manage; and, protecting their data and exercising discretion concerning access, usage, and dissemination.

Digital Certificates - To use asymmetric encryption, there must be a way for people to discover other public keys. The typical technique is to use digital certificates (also known simply as certificates). A certificate is a package of information that identifies a user or a server, and contains information such as the organization name, the organization that issued the certificate, the user's e-mail address and country, and the user's public key. When a server and client require a secure encrypted communication, they send a query over the network to the other party, which sends back a copy of the certificate. The other party's public key can be extracted from the certificate. A certificate can also be used to uniquely identify the holder.

Encryption - The process of converting data into a cipher or code in order to prevent unauthorized access. Encryption obfuscates data in such a manner that a specific algorithm and key are required to interpret the cipher or code. The keys are binary values that may be interpretable as the codes for text strings, or they may be arbitrary numbers. The purpose of encryption is to prevent unauthorized access to data while it is either in storage or being transmitted.

File-level encryption - A technique where individual files or directories are encrypted by the computer's file system itself. Unlike whole-disk encryption, file-level encryption generally does not encrypt file metadata (e.g., the directory structure, file names, modification timestamps or sizes.)

Managers (Custodians) – Managers are users who supervise other users. Managers are responsible for ensuring that the users they supervise have access to the information needed to perform their respective jobs; request information access for their appointed users from the appropriate Data Steward(s); periodically review the level and/or extent of access for their appointed users and request removal of access for their users when employment is terminated; ensure that any specific information security policies and procedures they establish for their users they
Symmetric Encryption - Symmetric encryption is the oldest and best-known technique. A secret key, which can be a number, a word, or just a string of random letters, is applied to the text of a message to change the content in a particular way. This might be as simple as shifting each letter by a number of places in the alphabet. As long as both sender and recipient know the secret key, they can encrypt and decrypt all messages that use this key.

Users – A user is anyone who uses CTCD Information Technology Resources or equipment. Users are responsible for: reading, understanding, and complying with CTC HR Policy No. 294, Computer Security Policy; the management and protection of both computerized and non-computerized information; and protecting and caring for information technology devices that have been assigned to them to perform the duties of the respective positions.

Whole-disk encryption - A technique where software or hardware encrypts every bit of data that is stored on a disk (e.g., everything on the hard drive including the operating system.)
INCIDENT RESPONSE GUIDELINES

Objective

- Protect the organization’s reputation, as well as its information.
- Develop an incident response plan with clearly delineated roles and responsibilities for quickly discovering an attack and then effectively containing the damage, eradicating the attacker’s presence, and restoring the integrity of the network and systems.
- Data Recovery Capability
- Minimize the damage from an attack.
- Implement a trustworthy plan for removing all traces of an attack. Automatically back up all information required to fully restore each system, including the operating system, application software, and data.

Back up all systems at least weekly; back up sensitive systems more often. Regularly test the restoration process.

A. Computer security incident definition

1. Any unlawful, unauthorized, or unacceptable action that involves a computer system or a computer network. Such an action can include any of the following events:
   a. Theft of confidential data or personally identifiable information
   b. Unauthorized or unlawful intrusions into computing systems
   c. Online harassment
   d. Sending email spam
   e. Possession or dissemination of illegal material e.g. child pornography
   f. Denial-of-Service (DoS) attacks
   g. Interference with business relations

2. Any unlawful action where the evidence of such action that may be stored on computer media such as fraud, threats, and/or traditional crimes.

3. Reported violation HR 294, Computer Security Policy, and/or HR 295, Computer Usage.

B. Computer security incident response goals

1. Provide rapid detection and containment
2. Confirm or dispel whether an incident occurred
3. Prevent a disjointed, non-cohesive response
4. Promote accurate information accumulation
5. Establish controls for proper retrieval and handling of evidence
6. Protect privacy rights established by law and policy
7. Minimize disruption to business and network operations
8. Allow for criminal or civil action against perpetrators
9. Provide accurate reports and useful recommendations
10. Minimize exposure and compromise of confidential data or personally identifiable information
11. Protect the organization’s reputation and assets
12. Inform senior management
13. Promote rapid detection and/or prevention of such incidents in the future via lessons learned, policy changes, etc.

C. Questions to be answered by a computer security incident response report
   1. Who reported the incident?
   2. What happened exactly?
   3. What system(s) was affected by the incident?
   4. What information was compromised?
   5. What files were created, modified, copied, or deleted?
   6. Who may have caused the incident?
   7. Who should be notified?
   8. What steps can we take to rapidly restore normal business procedures?

Incident Response Methodology

A. Initial response
   Perform an initial investigation, recording the basic details surrounding the incident, assembling the incident response team, and notifying the individuals who need to know about the incident.

B. Formulate a response strategy
   Based on the results of all the known facts, determine the best response and obtain management approval. Determine what civil, criminal, administrative, or other actions are appropriate to take, based on the conclusions drawn from the investigation.

C. Investigate the incident
   Perform a thorough collection of data. Review the data collected to determine what happened, when it happened, who did it, and how it can be prevented in the future.

D. Reporting
   Accurately report information about the investigation in a manner useful to decision makers.

E. Resolution
   Employ security measures and procedural changes, record lessons learned, and develop long-term fixes for any problems identified.
Incident Response Guidelines

A. Identify potential risks
   1. Confidential business information
   2. Nonpublic personally identifiable information

B. Prepare individual hosts for incident response and recovery
   1. Increase or enable secure audit logging
   2. Build up hosts’ defenses
      a. OS updates/patches
      b. Application updates/patches
      c. Disable unnecessary services

C. Back up critical data and store media securely
   1. Conducted nightly
   2. Safe Site Inc. of Austin, TX picks up backup tapes daily

D. Educate users about host-based security
   1. Training sessions conducted annually
   2. Departmental and individual training upon request
   3. IT Security News page on the Information Technology Division website

E. Establish policies and procedures that allow us to meet our incident response objectives
   1. Security Awareness Education Program
   2. Educate users how to contact IT about a security incident
   3. Train the Help Desk in initial response procedures

F. Prepare network by implementing network security measures
   1. Install firewalls and intrusion detection systems
   2. Use access control lists on routers
   3. Create a network topology conducive to monitoring
   4. Encrypt network traffic
   5. Require authentication

G. Create a Computer Security Incident Response Team (CSIRT)
   1. CSIRT’s Mission
      a. Respond to all security incidents or suspected incidents using an organized, formal investigative process
      b. Conduct a complete investigation free from bias
      c. Quickly confirm or dispel whether an intrusion or security incident actually occurred
      d. Assess the damage and scope of an incident
e. Control and contain the incident
f. Collect and document all evidence related to an incident
g. Maintain a chain of custody (protect the evidence after collection)
h. Select additional support when needed
i. Protect privacy rights established by law and/or institutional policy
j. Provide liaison to proper law enforcement and legal authorities
k. Maintain appropriate confidentiality of the incident to protect the organization from unnecessary exposure
l. Provide expert testimony
m. Provide management with incident-handling recommendations that are fully supported by facts

2. Create a response toolkit for the CSIRT

3. Create a CSIRT that can assemble to handle incidents:
   a. Michael Hunter (Information Security Officer, responsible for external liaison/CSIRT coordinator)
   b. Kemar Carridge (IT Network Engineer, responsible for network traffic analysis)
   c. James Atchley (IT User Services Manager, responsible for IT Help Desk & desktop support)
   d. Sean Ferreira (IT Windows System Administrator, responsible for Windows servers)
   e. Timothy Lofton (IT User Services Technician II, responsible for desktop forensic investigation)
   f. Michael Lloyd (Sr. Systems Administrator, responsible for Colleague servers)

4. CSIRT reports to the Central Texas College’s decision makers for further dispensation:
   a. Cliff Gaines, Director of Information Technology, Information Technology Division
   b. Michele Carter, Deputy Chancellor Finance and Administration
   c. Carla Littlefield, Director of IT Customer Service, Information Technology Division
   d. Mary Wheeler, Chief of Police, Campus Police-Security Services
   e. Deborah Shibley, Director, Risk Management
   f. Barbara Merlo, Director, Marketing & Outreach
   g. Jacqueline E. Thomas, Coordinator, Affirmative Action/Equal Employment Opportunity, Human Resources

H. Initial Response Phase
1. Goals of the Initial Response Phase:
   a. Rapid and effective decision making
   b. Rapid accumulation of information in a forensically sound manner
   c. Proper escalation of the incident
   d. Rapid notification of the participants required to assemble your CSIRT
2. What is our response to a computer intrusion, denial-of-service, attack, insider theft of intellectual property, or other network-based computer crime?
   a. Perform surveillance and counterintelligence data gathering
   b. Defend against further attacks
   c. Defend against further attacks by identifying and disabling the initiators (by criminal arrest or civil action)

3. Four general factors will influence our response:
   a. The effect the incident has on the college
   b. Legal issues and constraints
   c. Technical capabilities of the response team
   d. Funding and available resources

4. Incident Declaration. Questions to ask before declaring an incident:
   a. Was there a scheduled system or network outage that caused resources to be unavailable during the time the incident occurred?
   b. Was there an unscheduled and unreported outage of a network service provider that caused resources to be unavailable during the time the suspected incident was reported?
   c. Was the affected system recently upgraded, patched, reconfigured, or otherwise modified in such a way as to cause the suspicious activity that was reported?
   d. Was testing being performed on the network that would lock out accounts or cause resources to be unavailable?
   e. For CTC users (insider incidents), are there any justifications for that actions an employee has taken that remove or lessen the suspicions?

5. Questions to be answered for victims of a security breach
   a. How do I find out if my personal information was included in the data accessed through the incident?
   b. What specific information was disclosed?
   c. Where did this happen and why was my information in these computers?
   d. What did you do when the information was accessed?
   e. What are you doing to make sure this does not happen again?
   f. Were there other individuals by this breach, or am I the only one?
   g. Was my spouse or other family members’ information also affected?
   h. Has the person who accessed the information been caught?
   i. Will we receive any additional information or update?
6. Recommended Practices
   a. Be certain to involve the appropriate decision makers
   b. Understand the nature of the incident, including the potential business impact, possible perpetrators, who is aware of the issue, and how the incident occurred.
   c. Identify the individual(s) who will have responsibility for deciding the response strategy, as well as those individuals whose input may be needed to finalize that strategy.
   d. Determine the institution’s priorities and how they affect the response.
   e. Identify viable response options that address the priorities.
   f. Select the alternative that best fits the situation.

It is important to remember:

• Incidents get people worked up and they want answers right away. It is the Computer Security Incident Response Team’s responsibility to maintain a level and realistic view of what can be accomplished and when.

• In the case of incident response, preparation is key. Preparation for investigators ensures swift, appropriate response and minimizes the chance of errors. Preparation for system administrators involves configuring hosts and networks in a manner that reduces the risk of incidents and eases the task of resolving incidents.
MINIMUM SECURITY STANDARDS FOR SYSTEMS

Purpose
These minimum standards serve as a supplement to the Information Security Program, which was drafted in response to Texas Administrative Code 202. Adherence to the standards will increase the security of systems and help safeguard College Information Technology Resources.

These minimum standards exist in addition to all other college policies and federal and state regulations governing the protection of the College's Information Technology Resources. Compliance with these requirements does not imply a completely secure system. Instead, these requirements will be integrated into a comprehensive system security plan.

Scope
These standards apply to all with systems connected to the Central Texas College District (CTC) network; as well as all devices, physical or virtual, connected to the CTC network through a physical, wireless, or VPN connection where data is classified as Category I, II, or III (see HR No. 294, Computer Security Policy, Section IV). Systems that store and/or process credit card information must also comply with the Payment Card Industry (PCI) requirements.

Definitions
Class I Data – Public information. Information made available either to the public or to specific individuals who need it with few, if any, restrictions. The published class schedule is an example of Class I Data.

Class II Data – Limited distribution information. The loss, corruption, or unauthorized disclosure of this information would not affect the operational effectiveness of CTCD. A document detailing a fund-raising strategy is an example of Class II Data.

Class III Data – Private information. Information that is confidential and protected from external access and unauthorized internal access. Loss, corruption, or unauthorized disclosure of this information would impair the business or research functions of CTCD; result in business, financial, or legal loss; or be a violation of federal or state laws/regulations or CTCD contracts. Data integrity is vital. An example of private information would be a student's academic record.

Roles and Responsibilities
This section lists the minimum standards that shall be applied and enabled in Class I, II, and III data systems that are connected to the CTC network. Standards for Class III are generally required.

If products are not available from reputable commercial or reliable open source communities for a specific requirement, then the specific requirement is waived until an appropriate solution is available. In such cases a Security Exception Report shall be filed.
Systems engineers and administrators are expected to use their professional judgment in managing risks to the information and systems they use and/or support. All security controls should be proportional to the confidentiality, integrity, and availability requirements of the data processed by the system.

<table>
<thead>
<tr>
<th>#</th>
<th>Practice</th>
<th>Class III</th>
<th>Class I &amp; Class II</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Backups</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1</td>
<td>Systems engineers and administrators shall establish and follow a procedure to carry out regular system backups.</td>
<td>Required</td>
<td>Recommended</td>
</tr>
<tr>
<td>1.2</td>
<td>Backups must be verified at least monthly, either through automated verification, through customer restores, or through trial restores.</td>
<td>Required</td>
<td>Recommended</td>
</tr>
<tr>
<td>1.3</td>
<td>Systems engineers and administrators must maintain documented restoration procedures for systems and the data on those systems.</td>
<td>Required</td>
<td>Recommended</td>
</tr>
<tr>
<td></td>
<td><strong>Change Management</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1</td>
<td>There must be a change control process for systems configuration. This process must be documented.</td>
<td>Required</td>
<td>Recommended</td>
</tr>
<tr>
<td>2.2</td>
<td>System changes should be evaluated prior to being applied in a production environment.</td>
<td>Required</td>
<td>Recommended</td>
</tr>
<tr>
<td></td>
<td>- Patches must be tested prior to installation in the production environment if a test environment is available.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- If a test environment is not available, the lack of patch testing should be communicated to the service subscriber or data steward, along with possible changes in the environment due to the patch.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Computer Virus Protection</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.1</td>
<td>Anti-virus software must be installed and enabled.</td>
<td>Required</td>
<td>Recommended</td>
</tr>
<tr>
<td>3.2</td>
<td>Anti-spyware must be installed and enabled if the machine is used by administrators to browse Web sites not specifically related to the administration of the machine. In addition, anti-spyware software must be installed if users are able to install software.</td>
<td>Required</td>
<td>Recommended</td>
</tr>
<tr>
<td>3.3</td>
<td>Anti-virus and, if applicable, anti-spyware software should be configured to update signatures daily.</td>
<td>Required</td>
<td>Recommended</td>
</tr>
<tr>
<td>3.4</td>
<td>System engineers and administrators should maintain and keep available a description of the standard configuration of anti-virus software.</td>
<td>Required</td>
<td>Recommended</td>
</tr>
<tr>
<td></td>
<td><strong>Physical Access</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Systems must be physically secured in racks or areas with restricted access. Portable devices shall be physically secured if left unattended.</td>
<td>Required</td>
<td>Recommended</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>4.2</td>
<td>Backup media must be secured from unauthorized physical access. If the backup media is stored off-site, it must be encrypted or have a documented process to prevent unauthorized access.</td>
<td>Required</td>
<td>Recommended</td>
</tr>
</tbody>
</table>

### System Hardening

<table>
<thead>
<tr>
<th></th>
<th>Systems must be set up in a protected network environment or by using a method that assures the system is not accessible via a potentially hostile network until it is secured.</th>
<th>Required</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2</td>
<td>Operating system and application services security patches shall be installed expediently and in a manner consistent with change management procedures.</td>
<td>Required</td>
<td>Recommended</td>
</tr>
<tr>
<td>5.3</td>
<td>If automatic notification of new patches is available, that option should be enabled.</td>
<td>Required</td>
<td>Recommended</td>
</tr>
<tr>
<td>5.4</td>
<td>Services, applications, and user accounts that are not being utilized should be disabled or uninstalled.</td>
<td>Required</td>
<td>Recommended</td>
</tr>
<tr>
<td>5.5</td>
<td>Methods should be enabled to limit connections to services running on the host to only the authorized users of the services. Software firewalls, hardware firewalls, and service configurations are a few of the methods that may be employed.</td>
<td>Required</td>
<td>Recommended</td>
</tr>
<tr>
<td>5.6</td>
<td>Services or applications running on systems manipulating Class III Data should implement secure (that is, encrypted) communications as required by confidentiality and integrity needs.</td>
<td>Required</td>
<td>Recommended</td>
</tr>
<tr>
<td>5.7</td>
<td>Systems will provide secure (that is, encrypted) storage for Class III Data as required by confidentiality, integrity, and availability needs. Security can be provided by means such as, but not limited to, encryption, access controls, file system audits, physically securing the storage media, or any combination of thereof as deemed appropriate.</td>
<td>Required</td>
<td>Recommended</td>
</tr>
<tr>
<td>5.8</td>
<td>If the operating system supports it, integrity checking of critical operating system files should be enabled and tested. Third-party tools may also be used to implement this.</td>
<td>Required</td>
<td>Recommended</td>
</tr>
<tr>
<td>5.9</td>
<td>Integrity checking of system accounts, group memberships, and their associated privileges should be enabled and tested.</td>
<td>Required</td>
<td>Recommended</td>
</tr>
<tr>
<td>5.10</td>
<td>The required college warning banner shall be installed.</td>
<td>Required</td>
<td>Recommended</td>
</tr>
</tbody>
</table>
### 5.11 Whenever possible, all non-removable or (re-) writeable media must be configured with file systems that support access control.

<table>
<thead>
<tr>
<th>Required</th>
<th>Recommended</th>
</tr>
</thead>
</table>

### 5.12 Access to non-public file system areas must require authentication.

<table>
<thead>
<tr>
<th>Required</th>
<th>Recommended</th>
</tr>
</thead>
</table>

### 5.13 Strong password requirements shall be enabled, as technology permits, based on the class of data the account is allowed to access (CTC Data Classification Standard).

<table>
<thead>
<tr>
<th>Required</th>
<th>Recommended</th>
</tr>
</thead>
</table>

### 5.14 Apply the principle of least privilege to user, administrator, and system accounts.

<table>
<thead>
<tr>
<th>Required</th>
<th>Recommended</th>
</tr>
</thead>
</table>

### 5.15 System processes (for example: batch or automated jobs) should not run under the credentials of an authorized user. A system account needs to be created and used for these processes.

<table>
<thead>
<tr>
<th>Required</th>
<th>Required</th>
</tr>
</thead>
</table>

### Security Monitoring

#### 6.1 If the operating system comes with a means to log activity, enabling and testing of those controls is required.

<table>
<thead>
<tr>
<th>Required</th>
<th>Recommended</th>
</tr>
</thead>
</table>

#### 6.2 Operating system and service log monitoring and analysis should be performed routinely. This process should be documented.

<table>
<thead>
<tr>
<th>Required</th>
<th>Recommended</th>
</tr>
</thead>
</table>

#### 6.3 The systems engineer or administrator must follow a documented backup strategy for security logs (for example, account management, access control, data integrity, etc.). Security logs should retain at least 14 days of relevant log information (NOTE: data retention requirements for specific data should be considered. For example, Payment Card Industry audit trail history and log retention should be retained for at least one year depending on PCI system classification – SAQ-A; B; C; or D).

<table>
<thead>
<tr>
<th>Required</th>
<th>Recommended</th>
</tr>
</thead>
</table>

#### 6.4 All administrator or root access must be logged.

<table>
<thead>
<tr>
<th>Required</th>
<th>Recommended</th>
</tr>
</thead>
</table>
Related Policies, Procedures, Best Practices and Applicable Laws

The policies and practices listed herein form the system hardening procedures described in this document and with which you should be familiar. (This is not an all-inclusive list of policies and procedures that affect information technology resources).

Central Texas College District employees are required to comply with institutional rules and regulations. In addition to CTCD rules and regulations, employees are required to comply with Federal and state laws and regulations.
IT SECURITY PROGRAM FORMS
CENTRAL TEXAS COLLEGE CERTIFICATE OF DESTRUCTION

Campus: __________________________________________

Campus representative: __________________________________________

Campus telephone number: _______________________________________

Campus representative email: _____________________________________

Date of destruction: ____________________

Method of destruction:
( ) Disk Wiping  ( ) Shredding  ( ) Dismantle
( ) Other: ______________________________________________

<table>
<thead>
<tr>
<th>MODEL NUMBER</th>
<th>SERIAL NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

I, ____________________________________________, do hereby certify that the equipment listed above was destroyed in accordance with Central Texas College District policy, CTCD Hard Drive Destruction Policy.

________________________________________
Signature

______________________________
Date

Central Texas College
Form ITD-0010  Information Technology Division  June 27, 2013
<table>
<thead>
<tr>
<th>Date/Time Reported</th>
<th></th>
</tr>
</thead>
</table>

**II. DIAGNOSIS**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>

**III. RECOVERY**

<table>
<thead>
<tr>
<th>Date/Time Restored</th>
<th></th>
</tr>
</thead>
</table>

**IV. RECURRENCE PREVENTION**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>

**V. PERSONNEL**

<table>
<thead>
<tr>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee</td>
</tr>
<tr>
<td>Department Director</td>
</tr>
<tr>
<td>IT Division Director</td>
</tr>
</tbody>
</table>