Cyber Tree Systems
A Business IT Solution Company

Authentication & Authorization Policy

Statement of Purpose

This document will outline procedures for verifying user identities and granting access to systems, applications, and data based on the principle of least privilege, ensuring security and compliance. It is broken down into four sub policies: Acceptable Encryption, Acceptable Use, Unacceptable Use and Password Policy.

1.0 Acceptable Encryption Policy

1.1 Purpose

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. 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.

1.2 Scope

This policy applies to all CTS employees and affiliates.

1.3 Policy

Only encryption algorithms that align with current industry standards must be used for securing data, network communication, and remote access. Examples of acceptable encryption algorithms include those that meet modern security requirements, such as AES-based encryption for VPN connections and TLS for securing web traffic. These standards will be reviewed and updated as industry best practices evolve.

All access to encrypted data and secure communications must be controlled through Role-Based Access Controls (RBAC) and Multi-Factor Authentication (MFA) to ensure only authorized personnel can access sensitive information.

The use of proprietary encryption algorithms is not allowed for any purpose unless reviewed by qualified experts outside of the vendor in question and approved by InfoSec. 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.

2.0 Acceptable Use Policy

2.1 Overview

InfoSec's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to CTS's established culture of openness, trust, and integrity. InfoSec is committed to protecting CTS's employees, partners, and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of CTS. These systems are to be used for business purposes in serving the interests of the company and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every CTS employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

2.2 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at CTS. These rules exist to protect the employee and CTS. Inappropriate use exposes CTS to risks, including virus attacks, compromise of network systems and services, and legal action.

2.3. Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at CTS, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by CTS.

2.4. Policy

2.4.1 General Use and Ownership

While CTS's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of CTS. Because of the need to protect CTS's network, management cannot guarantee the confidentiality of information stored on any network device belonging to CTS.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

InfoSec recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on information classification, see InfoSec's Information Sensitivity Policy. For guidelines on encrypting email and documents, go to InfoSec's Awareness Initiative.

For security and network maintenance purposes, authorized individuals within CTS may monitor equipment, systems, and network traffic at any time, per InfoSec's Audit Policy.

CTS reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

2.4.2 Security and Proprietary Information

The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines, details of which can be found in Human Resources policies.

Examples of confidential information include but are not limited to company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information. Keep passwords secure, and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System-level passwords should be changed quarterly, user-level passwords should be changed every six months.

All PCs, laptops, and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Win2K users) when the host will be unattended. Use encryption of information in compliance with InfoSec's Acceptable Encryption Use Policy.

Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the “Laptop Security Tips.”

Postings by employees from a CTS email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of CTS, unless posting is in the course of business duties. All hosts used by the employee that are connected to the CTS

Internet/Intranet/Extranet, whether owned by the employee or CTS, shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.

Employees must use extreme caution when opening email attachments received from unknown senders, which may contain viruses, email bombs, or Trojan horse code.

3.0 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host that is disrupting production services).

Under no circumstances is an employee of CTS authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing CTS-owned resources.

The lists below are by no means exhaustive but attempt to provide a framework for activities, which fall into the category of unacceptable use.

3.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by CTS.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which CTS or the end-user does not have an active license is strictly prohibited.

- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using a CTS computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any CTS account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless prior notification to InfoSec is made.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network or account.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of, CTS employees to parties outside CTS.

3.2 Email and Communications Activities

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within CTS's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by CTS or connected via CTS's network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

3.3 Blogging

Blogging by employees, whether using CTS’s property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of CTS’s systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate CTS’s policy, is not detrimental to CTS’s best interests, and does not interfere with an employee's regular work duties.

Blogging from CTS's systems falls under CTS's Confidential Information Policy and Non-Discrimination and Anti-Harassment policy and is therefore subject to monitoring. As such, Employees are prohibited from revealing any Company confidential or proprietary information, trade secrets or any other material covered by Company's Confidential Information policy when engaged in blogging.

4.0 Password Policy

4.1 Purpose

This policy provides the requirements for creating and retrieving usernames and passwords (i.e., credentials) for use by employees that require authentication and access resources on CTS's network.

These credentials are meant to restrict access based on privileges as assigned by the IS/IT/InfoSec department and can be compromised when the credentials are improperly stored.

4.2 Scope

This policy applies to all users that will access CTS resources locally and through VPN/remote access.

4.3 Policy

4.3.1 General

In order to maintain the security of CTS's internal resources, access by user must be granted only after authentication on one of 3 Active Directory Domain Controller servers.

4.3.2 Specific Requirements

4.3.2.1 Username & Password Creation and Retention

- Usernames will consist of an employee's first initial and last name
- Passwords will be 8 to 12 characters in length
- Passwords will be a combination of upper- and lower-case alphanumeric values, which can include common symbols.
- Passwords will be valid for 45 days
- A minimum of 12 passwords will be kept in the system's history, not to be repeated.
- Passwords must be stored using reverse encryption

4.3.2.2 Retrieval of Usernames and Passwords

If a user forgets his/her password, they should contact the CTS technical support center (TSC) and request to have their password reset. The TSC will not have access to a user's password and therefore be unable to directly access a user's account without creating an audit log entry

When a member of the CTS TSC resets a user's password, an entry will be made into the system audit logs and said logs will be maintained for a period of one (1) year.

Usernames consist of a standard format, as previously stated of first initial and last name. In the event of duplication, the user's first name initials will be used until such that duplication will not exist.

5.0 Enforcement

Any employee found to be in violation this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

Term	Definition
Credentials	Something you know (e.g., a password or passphrase), and/or something that identifies you (e.g., a user name, a fingerprint, voiceprint, retina print). Something you know and something that identifies you are presented for authentication.
Entitlement	The level of privilege that has been authenticated and authorized. The privileges level at which to access resource
Executing body	The series of computer instructions that the computer executes to run a program.
Hash	An algorithmically generated number that identifies a datum or its location.
Name space	A logical area of code in which the declared symbolic names are known and outside of which these names are not visible.
Blogging	Writing a blog. A blog (short for weblog) is a personal online journal that is frequently updated and intended for general public consumption.
Spam	Unauthorized and/or unsolicited electronic mass mailings.
Proprietary Encryption	An encryption standard developed by a manufacturer for a specific product. Proprietary encryption solutions may be used if they are industry-accepted, integrated into CTS-approved security tools, and have been reviewed by CTS InfoSec. Examples include BitLocker for disk encryption.
Symmetric Cryptosystem	A method of encryption in which the same key is used for both encryption and decryption of the data.
Asymmetric Cryptosystem	A method of encryption in which two different keys are used: one for encrypting and one for decrypting the data (e.g., public-key encryption).
Role-Based Access Control (RBAC)	A security model that restricts system access based on users’ roles within the organization, ensuring least-privilege access.
Multi-Factor Authentication (MFA)	A security mechanism that requires users to verify their identity through multiple forms of authentication (eg., password + hardware token) before accessing secure systems.

7.0 Revision History

Revision Number	Date	Editor	Reason
2.0	1/16/2025	Aidan Schmeckpeper	Separated into library and prepared for future edits.
2.1	2/19/2025	Aidan Schmeckpeper	Removed deprecated policies. Revised encryption standards.