Cyber Tree Systems
A Business IT Solution Company

| | | | |
|---|---|---|---|
| **POLICY NAME** | **Enterprise Information Security Policy (EISP)** | | |
| **DATE OF LAST REVISION:** | 9/4/2003 | **VERSION NO.** | 1.43 |
| **ADMINISTRATOR RESPONSIBLE** | Kevin McKnight | | |

## Statement of Purpose

This document will identify the elements of a good security policy, explain the need for information security, identify the information security roles and responsibilities, and establish minimum information security practices for Cyber Tree Systems (CTS) computer resources and associated communication networks utilizing the CTS enterprise network.

## Information Security Elements

Information security is defined as the protection of information and the systems and hardware that use store and transmit that information. Therefore, this policy is intended to give direction on accepted security practices designed to ensure information confidentiality, integrity, and availability of company assets by managing threats and reducing vulnerabilities.

Assets are defined, in this case, as items that are owned by the company that have an assessed financial value. This would include computer hardware, software, information, and lines of communication coming into and leaving the company campus.

Threats are defined as objects, people, or other entities representing a risk of loss to an asset(s). Threats occur in several categories. These include:

1. Acts of human error or failure (Accidents, employee mistakes)

2. Compromises to intellectual property (Piracy, copyright infringement)

3. Deliberate acts of espionage or trespass (Unauthorized access)

4. Deliberate acts of information extortion (Blackmail of disclosure)

5. Deliberate acts of sabotage or vandalism (Destruction of information)

6. Deliberate acts of theft (Illegal confiscation of equipment)

7. Deliberate software attacks (Viruses, worms, denial-of-service)

8. Deviations in QOS from service providers (Power and WAN issues)

9. Forces of nature (Fire, flood, earthquake, lightning)

10. Technical hardware failures or errors (Equipment failure)

11. Technical software failures or errors (Bugs, unknown loopholes)

12. Technical obsolescence (Antiquated or outdated technology)

Vulnerabilities are weaknesses or faults in a system or protection mechanism that exposes information to an attack or damage. Attacks are acts of intentional or unintentional attempt to compromise the information and/or the systems that support it.

## Need for Information Security

The continued use of information technology resources throughout CTS' working infrastructure has continued to evolve with the intent of improving services for our constituency. These improvements allow for rapid and efficient communication among various departments and often directly with the directors of the surrounding business community. Consequently, our constituency has become heavily dependent upon the availability of a reliable information technology infrastructure to meet its business needs. Unfortunately, the "electronic highways" that facilitate our ability to instantaneously share information also create vulnerabilities, potentially allowing unauthorized persons to gain access to CTS resources. To control threats to information technology resources across the enterprise network and associated domains, a series of Information security instructions, entitled "INFORMATION SECURITY POLICY, INSTRUCTIONS, AND TECHNICAL STANDARDS," is established.

## Information Security Roles & Responsibilities

CTS technology resources will proactively track threat activity and work to prohibit or correct such activity. Where unintentional unauthorized access is detected, the affected organization will be advised to correct exploitable vulnerabilities to prevent future occurrences. Where unauthorized access is determined to be intentional, it will be assumed to be malicious, and an appropriate response will be initiated. All CTS faculty members, staff, students, contractors, agents, or other individuals utilizing computer resources, data communication networks, or other information technology infrastructure resources owned or leased by CTS, including any other state agencies having electrical connectivity to the network, are subject to this policy.

Additionally, any remote access, such as dial-up connections, personal Internet Service Provider access or VPN connection, onto the CTS enterprise network or associated domains will have the same effect as direct access via CTS-provided equipment or facilities.

## General Policy Elements

1. Protection of Information:

    - Policy: Information must be protected in a manner commensurate with its sensitivity, value, and criticality.
    - Audience: Technical Staff

2. Use of Information:

    - Policy: CTS computer and communications systems must be used for appropriate business purposes only by authorized personnel.
    - Audience: All

3. Information Handling, Access, & Usage:

    - Policy: All data and information sent over the CTS enterprise network and associated domain communications systems are the property of CTS.

- Audience: All

4. Data & Program Damage Disclaimers:

   - Policy: CTS is not held responsible for any loss or damage to data or software that results from its efforts to protect the confidentiality, integrity, and availability of the information handled by computers and communications systems.
   - Audience: End Users

5. Legal Conflicts:

   - Policy: CTS information security policies were drafted to meet or exceed existing federal and state laws and regulations. Any policy implemented by CTS that is found to be in conflict with any existing laws or regulations should immediately be brought to the attention of the Chief Information Security Officer.
   - Audience: End Users

6. Exceptions to Policies:

   - Policy: Exceptions to information security policies exist on occasion where a risk assessment examining the implications of being out of compliance has been performed, where a standard risk acceptance form has been prepared by the data owner or management, and where this form has been approved by both the Chief Information Security Officer and Internal Audit Management.
   - Audience: Management

7. Non-enforcement:

   - Policy: Management's non-enforcement of any policy requirement does not constitute its consent.
   - Audience: End Users

8. Violation of the Law:

   - Policy: CTS will prosecute violators of federal and state computer crime laws as laid out within the applicable laws.
   - Audience: End Users

9. Revocation of Access Privileges:

   - Policy: CTS reserves the right to revoke a user's information technology privileges at any time.
   - Audience: End Users

10. Industry-Specific Information Security Standards:

    - Policy: CTS information systems must employ industry-specific information security standards.
    - Audience: Technical Staff

11. Use of Information Security Policies and Procedures:

    - Policy: All CTS information security documentation, including, but not limited to, policies, standards, and procedures, must be classified as "Internal Use Only", unless expressly created for external business processes and partners.
    - Audience: All

12. Authority Over Data:

- Policy: CTS reserves the right to examine all information transmitted through these systems. Examination of such information may take place without warning to the parties sending or receiving such information.
- Audience: All

13. Expectation of Privacy:

- Policy: Staff, contractors, agents, or other individuals should have no expectation of privacy associated with the information they store in or send through these systems; most files and documents maintained by CTS are subject to public review under the Georgia Open Records Act. This includes computer files and other stored material regardless of the medium of storage.
- Audience: All

14. Mission Critical Systems Information Handling:

- Policy: CTS reserves the right to delete, summarize, or edit any information posted to, or transiting through, CTS information systems. These systems are scarce, Company-owned resources designed to support mission-critical Company activities and goals.
- Audience: All

## Review & Evaluation

1. Review Period:

- Policy: This policy and associated instructions require a quarterly review by the Chief Information Officer's Departmental Directors or agents.
- Audience: Management & Board of Directors

2. Authority:

- Policy: Authority to establish and enforce this policy and associated security policy documents are made by Chief Information Officer and Chief Information Security Officer.

## Reference

The Georgia Computer Systems Protection Act (O.C.G.A. 16-9-90) specifies unlawful acts involving information resources and subsequent penalties upon conviction. As data residing or transiting CTS networks and machines are held in great trust, it must be afforded the greatest safeguards. Therefore, information security policy, instruction, processes, and standards created in furtherance of protecting CTS Company information assets rely upon the Georgia Computer Systems Protection Act (O.C.G.A 16-9-90) TO ENSURE COMPLIANCE. Violators may be prosecuted accordingly.

** Portions of this policy were copied and or modified from tables 4-1 and 4-2 (pages 111-115) of Management of Information Security by Dr. Michael Whitman and Professor Herbert Mattord.