POLICY NAME	**Intrusion Detection System**		
DATE OF LAST REVISION:	9/4/2003	**VERSION NO.**	1.43
ADMINISTRATOR RESPONSIBLE	Kevin McKnight		

Purpose

The purpose of this policy is to provide guidelines for Intrusion Detection systems as implemented within the CTS network both within the network infrastructure and on the perimeter of the network.

Scope

This policy applies to all CTS InfoSec employees.

Policy Statement

- Guidelines

  There must be a minimum of two network-based Intrusion Detection Systems always running on CTS's network. Both should be located at the perimeter of the network, at the firewall bordering the DMZ. The IDS signatures must be updated every 2 weeks from the vendor to keep the IDS(s) at the current signature level. Any suspected intrusions, suspicious activity, or unexplained erratic system behavior discovered by administrators, users, or computer security personnel must be reported to the organizational IT computer security office within 1 hour, and the Incident Response Plan should be initiated. All intrusions with financial or customer data loss must be reported to CEO, CFO, CIO within 7 days of the loss.

  Refer to the CTS Incident Response Policy Manual for further details regarding events.

- Logging

  The IDS logs must be kept for a minimum of 1 year. The IDS Event logs must be monitored daily by InfoSec Staff for abnormal activities.

- Ownership

  Responsibility for maintenance, including signature updates, firmware updates, and system testing, as well as any future iterations of IDS implementations, will fall to the InfoSec team with ultimate approval from the CISO and InfoSec manager.

Enforcement

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

Terms and Definitions

Define any acronyms, jargon, or terms that might have multiple meanings.

TERM	DEFINITION
Intrusion Detection System (IDS)	Used to detect several types of malicious behaviors that can compromise the security and trust of a computer system.

Revision History

Revisions made 9/4/2023