

Coppin State University

Information Technology Security Program

Purpose

The purpose of this policy is to establish rules necessary to protect Coppin State University (CSU) data and information systems by implementing a comprehensive IT Security Program. Such a program will enhance and protect the integrity, confidentiality, and availability of information resources by providing access controls to computing environments and information to authorized users.

It is ITDs responsibility to protect and maintain CSU data/information. Campus personnel including IT administrators must follow approved procedures and prevent corruption or misuse CSU's software or hardware. Listed below are security practices that are to be followed where technically feasible.

Definitions:

Acceptable Risk: A vulnerability that is acceptable to responsible management, due to the cost and magnitude of implementing countermeasures.

Accountability: A system's ability to determine the actions and behavior of a single individual within a system, and to identify that particular individual.

Authorized Software: Software owned or licensed and used in accordance with the software license or software approved for use by the agency for a specific job function.

Availability: Ensures the reliable and timely access to data or computing resources by the appropriate personnel.

Confidentiality: Restriction from disclosure, intentionally or unintentionally, to unauthorized persons, processes or devices.

Firewall: A safeguard used to control access between a trusted network and a less trusted one; a strategy for protecting an organization's Internet-reachable resources.

Incident: Any event, suspected event or attempted action that could pose a threat to the integrity, availability, confidentiality, or accountability of an IT System. Incidents include an attempted security breach, IT System disruption or outage.

Identification: Data uniquely labeling a user to a system.

Integrity: Freedom from corruption or unauthorized modification; internal and external consistency.

IT Systems: Automated systems: communications systems including wireless systems, computer systems, hardware and software, application systems, networks, workstations, servers, personal digital assistants and data on the IT System.

Network: A system containing any combination of computers, computer terminals, printers, audio or visual display devices or telephones interconnected by telecommunications equipment or cables, used to transmit or receive information.

Risk: The probability that a particular threat will exploit a particular vulnerability of an IT System.

Sensitive Information: Data pertaining to individuals or organizations that, if released, could cause harm.

Scope

This policy applies to all CSU information technology resources and personnel who access those resources. It pertains especially to those resources that support critical enterprise systems.

General Policy

It is the policy of CSU to maintain an IT security program that protects the integrity, confidentiality, and availability of information resources, as well as addresses compliance with all applicable laws and regulations. The program will encompass the following elements:

1. Risk assessment of information technology infrastructure
2. Access controls to information technology infrastructure and information
3. Network security, including firewalls, virtual private networks, etc.
4. Incident reporting
5. Disposal and reuse of storage media including workstations
6. Backup and recovery of Mission Critical Systems
7. Security awareness, training and education
8. Ensure segregation of duties

Access to critical enterprise systems will be provided for authorized individuals. CSU has separate standards and policies that address the various topics within its security program. These standards and policies are listed below:

IT Related Policies/Standards:

CSU System Monitoring Policy (ITD-CNS-002)
CSU Firewall Policy (ITD-CNS-003)
CSU Password Policy (ITD-CNS-005)
CSU Intrusion Prevention and Detection (ITD-CNS-012)
CSU Data Retention Policy (ITD-CNS-014)
CSU Systems Access Policy (ITD-GEN-001)

CSU Illegal File Sharing Prevention Policy (ITD-GEN-004)
CSU Student Computer Use and Internet Access Policy (ITD-GEN-005)
CSU Faculty/Staff Computer Use and Internet Access Policy (ITD-GEN-006)
CSU Incident Reporting and Escalation Policy (ITD-GEN-007)
CSU EagleLINKS Data Access Policy (ITD-IS-009)
CSU Segregation of Duties for Information Systems (ITD-IS-010)
CSU Access to Production/Non-Production Systems Policy (ITD-IS-011)
CSU Security Awareness Training Policy (ITD-TRN-001)