


**Coppin State University  
Information Technology Division  
Policies and Procedures**

**Policy #:** ITD – GEN – 011                      **Version:** 02  
**Subject:** CSU IT Security Program    **Effective Date:** 09/01/2013  
**Approved by:**                       **Review Date:** 07/31/2017  
**Approval Date:** 07/01/2013

---

**I. Purpose**

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

Responsibility to protect and maintain CSU systems, data, and information is shared between administrators and end users. Campus personnel, including IT administrators, must follow approved procedures and prevent corruption or misuse CSU's software or hardware. In addition, end users must follow established proper usage policies for the appropriate use of systems and data as well as the protection of usernames and passwords. It is important for all CSU system users to review the following information to ensure awareness of current security practices employed at CSU.

**II. 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 CSU IT Security Program encompasses many key elements, including the following:

1. Planning for Security
  - Vulnerability Assessment
  - Consultation Services
2. Designing for Security
  - System Hardware and Application Architecture
  - Firewall Hardware/Software Provisioning

3. Access Control
  - Physical Security
  - VPN Services
  - Authentication/ Authorization
  - Identity Management
4. Monitoring & Response
  - Intrusion Prevention and Detection
  - Incident Reporting and Response
  - Patch Diligence
  - Contingency Planning- Continuity & Disaster Recovery
5. End User Diligence
  - IT Security Awareness and Training
  - E-mail Filtering (Spam & Virus), White Lists/Black Lists
  - Risk Alerts- Viruses, Phishing Scams
  - Virus Software Availability
6. Governance
  - IT Security Specialist
  - IT Related Policies/Standards
  - Intellectual Property (IP)/Illegal File Sharing Policy

### **III. Procedure**

#### **PLANNING FOR SECURITY**

##### **Vulnerability Assessment**

The Information Technology Division provides consultation services for CSU departments wishing to evaluate vulnerabilities in systems and procedures. Consultation can include documenting and mapping current processes, performing system audits, identifying areas for risk, reviewing Family Educational Rights and Privacy Act (FERPA) compliance, and developing mechanisms to remediate risk. In addition, the Information Technology Division Team will assist with queries for data in response to requests by auditors.

##### **Consultation Services**

The Information Technology Division provides consultation services to departments and academic entities planning new systems in order ensure acceptable availability, reliability, and maintainability. In addition, the ITD assists in planning for backup and restoration of data.

#### **DESIGNING FOR SECURITY**

##### **System Hardware and Application Architecture**

During the system development process, security architecture of the desired system is designed after completion of a security assessment in order to refine logical and physical security components to include:

- Logical architecture: Includes processes, technology and people and consists of system perimeter security, risk and threat analysis, incident response, antivirus policy, security administration, Disaster Recovery Plans (DRP), data security, application security, and infrastructure security.
- Physical architecture: Includes networking components such as firewalls, mail gateways, proxies, VLANs, Demilitarized Zone (DMZ), internal and external connections and devices.

### **Firewall Hardware/Software Provisioning**

In order to promote and maintain the security of Coppin State University (CSU) data and its network infrastructure, firewalls have been strategically installed as part of the overall network architecture. Requests for the opening or closing specific firewall ports to support applications are reviewed, researched, and acted upon by the Information Technology Division, who manages this service. Modifications to security protocols are made only upon review of requirements to ensure all changes meet CSU Security standards.

## **ACCESS CONTROL**

### **Physical Security**

As part of a comprehensive security program, physical security of information technology assets includes placement of equipment in locations with controlled access, as well as locations less likely to be impacted by floods, fires, and other calamities. Physical security also includes access to back-up power supplies where applicable.

Commensurate with the assessment of risks, physical access controls are in place for the following:

- Data Centers
- Areas containing servers and associated media
- Networking cabinets and wiring closets
- Power and emergency backup equipment
- Operations and control areas

Access to data centers and secured areas will be granted for those employees, contractors, technicians and vendors who have legitimate business responsibilities in those areas. Authorization should be based on need and approved by the manager responsible for the secured area.

Assets within the data center secured under this policy are listed in the Coppin State University Disaster Recovery Plan (ERP), Appendix C. Risks associated

with these assets are addressed in the Coppin State University Disaster Recovery Plan (ERP), Appendix E.

As part of maintaining access control, CSU is responsible for:

- Issuing picture ID badges to all employees and contractors
- Ensuring that all portable storage media containing sensitive information such as hard drives, diskettes, magnetic tapes, laptops, and CDs are physically secured
- Ensuring that proper environmental and physical controls are established to prevent accidental or unintentional loss of sensitive information residing on IT systems
- Ensuring that any physical access controls are auditable

***Storage Media Disposal*** - When no longer usable, diskettes, compact disks, tape cartridges, ribbons, and other similar items that contain sensitive data shall be destroyed by a NIST approved method such as shredding, incineration, overwriting, or degaussing. All IT equipment shall not be released from the university's control until the equipment is sanitized and all stored information has been cleared and documented. This requirement applies to all permanent disposal of equipment regardless of the identity of the recipient, including equipment transferred to schools. It also applies to equipment sent for maintenance or repair.

***Media Reuse***-When no longer required for mission or project completion, media (tapes, disks, hard drives, etc) to be used by another employee in the university should be overwritten with software and protected consistent with the sensitivity of data on the IT storage media.

***Redundancy***- A key component to physical security is the use of redundancy in critical systems. These systems utilize multiple mirrored servers placed at separate locations on campus to ensure continued operation in the event of a server failure. As an added measure of protection, CSU utilizes IT resources at a separate University of Maryland System institution to provide a secondary operation site in the event of disaster.

## **VPN Services**

CSU provides remote access to internal protected resources using Virtual Private Network (VPN) technology. Faculty, staff, and students may access shared network drives, applications, and protected systems after successful login to the VPN. After login, the menu provides links to common CSU applications as well as anti-virus software.

Faculty and staff individual digital file storage is provided on campus systems. Student digital file storage is provided by Office 365.

Faculty/Staff use <https://eaglevpn.coppin.edu>

Students use <https://eaglevpn.student.coppin.edu>

Access to VPN services are initially handled as part of the onboarding process. Privileges within CSU systems are provisioned automatically upon hiring as a faculty or staff member or as students are matriculated and are based on the individual's role as faculty, staff, or student, as well as user role. Additional system access requests shall be evaluated and privileges provided as needed.

SSL VPN demonstration video:

<http://www.coppin.edu/ITDNetwork/Training/sslvpn.html>

### **Authentication/ Authorization**

Coppin State University (CSU) employs a layered approach to accessing systems and data. This includes a robust approach to ensure that system access is granted only to users that are properly identified using login and password as a valid user (authentication) and that appropriate level of access (least privileged) is provided to the users to perform their tasks (authorization).

### **Identity Management**

Coppin State University (CSU) employs a highly centralized and integrated means of managing identity management for faculty, staff, and students. Identity management includes the provisioning of network accounts to new faculty, staff, and students, as well as role management, account termination, and password resets and synchronization.

Tutorial: <http://eaglepass.coppin.edu>

## **MONITORING & RESPONSE**

### **Intrusion Prevention and Detection**

CSU systems are monitored routinely in order to detect any signs of intrusion attempts. Automated review of system logs is performed using specialized software. In addition, system domain policies have been put in place to lock out system access in cases of successive login failures.

Upon detection, the affected system(s) shall be isolated and suspected user accounts suspended, if applicable. CSU personnel shall investigate the scope and impact of the incident.

### **Incident Reporting and Response**

Users are instructed to report any known breach of computer security as well as any suspicious or unusual computer incidents. In the event of an incident, the Information Technology Division will contact users and provide follow-up

including forensic investigation, documentation, and systems and process remediation.

### **Patch Diligence**

Coppin State University systems and applications require periodic updates in response to existing or emerging security threats. Approved patches are applied to operating systems and applications as they are made available and updates may be installed outside of normal maintenance windows if deemed necessary by the Information Technology Division.

### **Contingency Planning- Continuity, Disaster Recovery**

The Information Technology Division provides Disaster Recovery (DR) planning assistance to departments including risk assessment and development of Business Impact Assessments (BIA) and Disaster Recovery plans. Services include consultation with departments to collect process details and assistance with documenting risks and remediations.

Disaster Recovery planning, Risk Assessments, and Business Impact Assessments are provided on an as-needed basis to departments and academic units requesting assistance.

## **END USER DILIGENCE**

### **IT Security Awareness and Training**

All Coppin State University system users shall be provided an overview of fundamental security practices in use at CSU in order minimize risk when using IT systems. The training shall include a discussion including, but not limited to:

- ***Passwords*** - The use of strong passwords.
- ***Usernames*** - In conjunction with a valid password, the use of a unique identifier that will provide access to authorized systems.
- ***Screen Saver Locks*** - Users shall be encouraged to utilize automated screen savers that employ a lock that requires them to enter a password after a period of inactivity.
- ***Sensitive information*** – Protection of sensitive information.
- ***Logoff*** – Protection of assets and information through timely system logoff.
- ***Use by Proxy*** - Users shall be reminded never to access systems on behalf of someone else by logging into systems with another individual's username and password.
- ***Business purpose only*** – Appropriate use of systems and information limited to CSU business only.

### **E-mail Filtering (Spam & Virus), White Lists/Black Lists**

As a part of Coppin State University's (CSU) comprehensive security program, incoming email is automatically filtered for potential unwanted and potentially malicious email (spam).

Generally, the configuration of the filter adequately removes unwanted email while allowing appropriate email through. Occasionally, adjustments may be needed to ensure known and approved domains are added to the allowed (white) list and known and disapproved domains are added to the disallowed (black) list. Modifications to these lists will be made upon request.

### **Risk Alerts- Viruses, Phishing Scams**

CSU monitors for emerging threats in the form of viruses and phishing scams. The Information Technology Division will send alerts to system users in cases where known and credible threats exist.

### **Virus Software Availability**

The Information Technology Division (ITD) provides tools and consultation services to aid CSU staff, faculty, and students in maintaining a virus-free computing environment.

As a preventive measure, ITD offers free anti-virus software to faculty, staff, and students for computers used to access CSU systems. In addition, ITD offers consultation on how to minimize the threats to systems and data and best practices for safe computing.

ITD will also provide assistance to faculty, staff, and students using CSU-owned systems in the event their system has been infected with malicious software.

Faculty and staff may obtain free anti-virus software by logging in to the Faculty/Staff EagleVPN site at:

<https://eaglevpn.coppin.edu>

Students may obtain free anti-virus software by logging in to the Student EagleVPN site at:

<https://eaglevpn.student.coppin.edu>

A link to the free software is provided upon successful login.

## **GOVERNANCE**

### **IT Security Specialist**

The Coppin State University Office of Information Technology includes an IT Security Specialist, reporting directly to the CIO. The IT Security Specialist helps minimize the risk of cyber-attacks, educates employees on computer security, monitors networks for security breaches, and responds to cyber-attacks as

necessary with the appropriate countermeasures. In addition, the IT Security Specialist enforces IT security policy compliance and supports security and audit inquiries.

### **Intellectual Property (IP)/Illegal File Sharing Policy**

In support of Higher Education Opportunity Act (HEOA) and Digital Millennium Copyright Act of 1998 (DMCA) directives, CSU expects that all members of the university community (users) respect the rights of ownership of intellectual property by adhering to United States copyright laws, CSU policies, and state and federal laws. Users shall utilize copyrighted material, including materials and software, for authorized purposes only and in accordance with their specific copyrights, licenses, or agreements.

Users shall not copy, download, store, or share unauthorized copyrighted material (e.g. music and videos) on CSU computers, IT systems or networks. In addition, users shall not engage in the sharing of copyrighted material through the use of peer-to-peer networks.

#### ***Policy Compliance***

All members of the campus community including faculty, staff, and students shall:

- Observe the copyright law as it applies to music, videos, games, images, texts and other media in both personal and academic use.
- Be aware that file sharing in violation of copyright is prohibited.
- Not use, copy, or share copyrighted works unless possessing a legal right to do so.

Failure to comply with the above may provide the basis for sanctions or disciplinary action, and in serious violations, civil litigation and/or criminal prosecution.

***Technology Support:*** CSU shall minimize the potential for illegal file sharing by implementing the following measures:

- Block access to Peer-to-Peer connections between CSU equipment and external networks. Special requests to access Peer-to-Peer networks shall be evaluated by OIT on a case-by-case basis and permission determined by academic need and potential risk.
- Utilize media monitoring software such as Audible Magic to determine if infractions have occurred.
- Violators risk losing access to the Internet until illegal file sharing activities/software are removed from their computing device(s)

***Student Awareness:***



Students shall be notified of the applicable policies and laws regarding copyrighted materials and use of Peer-to-Peer networks through the following mechanisms:

- Student Orientation
- Technology Fluency Course
- Student Handbook
- Faculty Advisories

#### IV. Definitions

The following terms apply for the purpose of this policy. Definitions for these terms may be found at <https://lookup.coppin.edu/cpd/Pages/Home.aspx>:

[Acceptable Risk](#)

[Incident](#)

[Accountability](#)

[Identification](#)

[Authorized Software](#)

[Integrity](#)

[Availability](#)

[IT Systems](#)

[Confidentiality](#)

[Network](#)

[Copyright](#)

[Peer-To-Peer File Sharing](#)

[DMCA](#)

[Risk](#)

[Firewall](#)

[Sensitive Information](#)

#### V. References

- Policy: ITD-CNS-002, CSU System Monitoring Policy
- Policy: ITD-CNS-003, CSU Firewall Policy
- Policy: ITD-CNS-005, CSU Password Policy
- Policy: ITD-CNS-012, CSU Intrusion Prevention and Detection
- Policy: ITD-CNS-014, CSU Data Retention Policy
- Policy: ITD-GEN-001, CSU Systems Access Policy
- Policy: ITD-GEN-004, CSU Illegal File Sharing Prevention Policy
- Policy: ITD-GEN-005, CSU Student Computer Use and Internet Access Policy
- Policy: ITD-GEN-006, CSU Faculty/Staff Computer Use and Internet Access Policy
- Policy: ITD-GEN-007, CSU Incident Reporting and Escalation Policy
- Policy: ITD-IS-009, CSU EagleLINKS Data Access Policy

- Policy: ITD-IS-010, CSU Segregation of Duties for Information Systems
- Policy: ITD-IS-011, CSU Access to Production/Non-Production Systems Policy
- Policy: ITD-TLT-007, CSU Security Awareness Training Policy
- Coppin State University Disaster Recovery Plan (ERP)