Christopher Newport University

Policy: Information Security Policy
Policy Number: 6045

Executive Oversight:	Vice President for Finance and Planning
Contact Office:	Information Technology Services
Frequency of Review:	Annually
Date of Last Review:	Spring 2021

A. PURPOSE

Christopher Newport has invested significant resources in its information technology systems and relies on them to perform its most essential functions and to communicate within and outside the university community. Information systems, and the data they allow us to gather and maintain, support everything we do. The data stored in those systems is often confidential and protected by law. Compromise of these systems would threaten the University's operations and ability to accomplish its mission.

There exists a variety of internal and external threats to the security of the University's technology systems and the data they use and maintain. Some are intentional and perpetrated by bad actors, others are created by mistakes or misuse that result from a failure to know and understand the limits and vulnerabilities of our systems.

This policy is adopted to direct and support efforts to keep the University's information technology systems - and the data they use and maintain - secure from internal and external threats and risks of compromise. It is also intended to ensure that the University's use of information technology systems protects data as required by state and federal law.

B. POLICY STATEMENT

The Office of Information Technology Services (ITS) shall be responsible for establishing and maintaining the physical security of the University's central computing facilities.

All users must protect the integrity and confidentiality of the information they create, access or store.

The University's Information Security Officer (ISO) shall develop and adopt a security program, establish security standards, provide technical direction and support to university offices and departments to develop local security procedures and train all users to protect the systems and data they use.

The University's security program shall take a risk-based approach with particular focus on sensitive information and critical data and applications. It should be guided by the security policies established by the Virginia Information Technologies Agency (VITA).

All departments and offices shall review and comply with University security standards necessary to protect the systems and data they use, in conformance with the University's security program and with direction and support from the ISO.

C. PROCEDURES

The University's security program shall address:

Access Control;
Awareness and Training;
Audit and Accountability;
Security Assessment and Authorization;
Configuration Management;
Contingency Planning;
Identification and Authentication;
Incident Response;
Maintenance;
Media Protection;
Physical and Environmental Protection;
Planning;
Personnel Security;
Risk Assessment;
System and Services Acquisition;
System and Communications Protection
System and Information Integrity; and
Program Management.

In the development of department and office-specific standards and practices, the vice presidents and deans must identify critical functions within their areas of responsibility and ensure backup of key software systems and data on systems for which they share operating responsibility. They shall designate a system owner for any server or application system under their control, that is not administered by ITS.

Any user who becomes aware of a potential information security incident must report the concern to the information security officer, ISO staff or iso@cnu.edu immediately. Release of University information, electronic devices or electronic media to any outside entity, in the course of an information security incident response, must be approved by the ISO or CIO.

D. DEFINITIONS

Centrally Managed: Systems, services, and data primarily maintained by IT Services (ITS).

Hardware, software, and information systems: University technology-related assets which work together or independently to provide a service to the University.

Information Security Program:
The set of managerial, operational and technical controls instituted to protect the integrity, availability and, if needed, confidentiality of information and the technology resources used to enter, store, process, and communicate electronic information.

Information Technology Resources:
Specific items such as telecommunications devices, computer systems, media, and other equipment, goods, services and personnel related to the collection, storage or transport of electronic information.

Production Systems: Systems critical to the operation of a specific department or the University.

Sensitive Data:
Non-public data subject to legal requirements (e.g., Federal or State privacy laws) or the privacy or compliance considerations, which define and regulate its responsible use. The University's Data Classification Standard defines two types of sensitive data: protected and highly confidential.

Significant Risk: Poses operational concern for a majority of the University, or impairs an entire department.

System Owners: Designated owner of a given production system and the data contained in that system.

User: Users: Affiliates, employees, students, vendors, and visitors authorized to use University communication and computing resources.

E. REFERENCES

VITA SEC 501: Virginia Commonwealth IT Information Security Standard

- https://www.vita.virginia.gov/it-governance/itrm-policies-standards/

University Acceptable Use of Computing Resources 6010: Policy document which establishes the terms of use for University communication and computing resources.

- https://cnu.edu/public/policies/

University Unified Data Policy 6015: Overall policy document which provides the framework for the University's approach to data management.

- https://cnu.edu/public/policies/

University Security Standards: Security standards that are designed to protect university information systems and data. These standards are regularly updated and include (but are not limited to) Account Management, Data Access, Data Classification, Data Protection, and Security Awareness.

- https://my.cnu.edu/its/

State and Federal Regulations:

- Family Educational Rights and Privacy Act (FERPA)
- Gramm-Leach-Bliley Act of 1999 (GLBA)
- Payment Card Industry Customer Information Security Program (PCI)

F. APPROVAL AND REVISIONS

Approved By: Policy Committee, April 8, 2021

G. NEXT REVIEW DATE: Spring 2022