# Christopher Newport University

## Policy: Unified Data Policy
## Policy Number: 6015

| | |
|---|---|
| Executive Oversight: | Chief Information Officer |
| Contact Office: | Information Technology Services |
| Frequency of Review: | Biennially |
| Date of Last Review: | July 2025 |

### A. PURPOSE

The University relies upon data and related data platforms in all of its activities and programs in pursuit of its mission. This policy directs the development of and compliance with standards that protect institutional data and systems in a manner that both complies with federal and state laws and maintains appropriate data accessibility in support of Christopher Newport University's core academic mission.

### B. POLICY STATEMENT

All persons who use and access university data or information systems for any purpose, shall conform their use to the following standards established by Information Technology Services (ITS). The following standards are governed by this policy:

- Data Access Standard: Governs who can access specific types of university data and under what conditions.
- Data Classification Standard: Securely classifies university data based on its sensitivity and impact level, guiding its handling, access, and protection.
- Data Protection Standard: Outlines measures required to safeguard university data from unauthorized access, use, disclosure, disruption, modification, or destruction.
- Data Sharing Standard: Specifies rules and procedures for sharing university data internally and externally with authorized entities.

These standards are available via the Christopher Newport University Information Technology Services Knowledge Base.

### C. DEFINITION(S)

**Data**: University data includes all data collected, maintained, or used by university personnel, vendors, or partners as part of their role in fulfilling the university's mission. Data are recorded information that documents a university business-related transaction or activity by or with any board member, officer, or employee of the university. University data may include but are not limited to: personnel records, student records, academic records, financial records, client records and administrative records. Data can be stored in a number of formats including but not limited to: email, electronic databases, electronic files, audio, video and images stored electronically.

**Sensitive Data:** Non-public university data that is subject to legal requirements, contractual obligations, or privacy considerations, and whose unauthorized disclosure, alteration, or destruction could result in significant harm to individuals or the University.

**Data Stewardship:** The responsible and ethical management of data assets, including their collection, maintenance, protection, and use, to ensure their availability, integrity, and confidentiality

## D. PROCEDURES

1. Oversight and Responsibility:

   The Chief Information Officer is responsible for the oversight and security of university information and data in digital form.

2. Standards Development and Maintenance:

   ITS shall develop and adopt data access, data classification, data protection, and data sharing standards sufficient to ensure the secure classifying, handling, access to, and protection of university data. The standards will incorporate current best practices and shall conform to federal and state law, while facilitating access to and use of university data in support of the university's business, programs and activities, in pursuit of its mission. Guidance from the Library of Virginia Records Management, will be incorporated throughout these standards for data lifecycle management.

   The university Information Security Officer shall review these standards annually, and revise them as necessary to maintain data and system security and compliance with state and federal law. Revised standards will be reviewed by the IT Executive Steering Committee, and posted electronically and made readily available to data and system users.

3. Compliance:

   All individuals who use and access university data or information systems shall conform their use to these established standards. Non-compliance with these standards is a violation of this policy. Violations of this policy or its associated standards may result in disciplinary action, up to and including termination of employment or dismissal from the university, in accordance with applicable university policies and procedures, including the Christopher Newport University Policy 6010: Acceptable Use of Computing Resources.

## E. REFERENCES

- Family Educational Rights and Privacy Act (FERPA)
- Gramm-Leach-Bliley Act (GLBA)
- Payment Card Industry Data Security Standard (PCI DSS)
- Virginia Freedom of Information Act (FOIA)
- Virginia Government Data Collection and Dissemination Practices Act
- Virginia Public Records Act

## F. APPROVAL AND REVISIONS

**Approved By:** Policy Committee, October 18, 2017
**Revision 1**: Policy Committee, March 22, 2019
**Revision 2**: Policy Committee, March 4, 2020
**Revision 3**: Policy Committee, August 25, 2021
**Revision 4**: Policy Committee, July 8, 2025

## G. NEXT REVIEW DATE: Summer 2027