

Board of Governors Policy



POLICY NAME	Information Security		POLICY NO.	BOG 6.1	
RESPONSIBLE OFFICE	Information Technology	EFFECTIVE DATE	10/01/2020	DATE APPROVED	10/01/2020
DATE OF LAST REVISION	10/01/2020	DATE OF NEXT REVIEW	10/01/2023		

SCOPE

This Policy applies to all employees and third-party Agents of the College as well as any other College affiliate who is authorized to access Institutional Data.

Compliance – Legislative Rule

W. Va. Code §18B-1-6

POLICY STATEMENT

New River Community and Technical College ("College") has adopted the following Information Security Policy ("Policy") as a measure to protect the confidentiality, integrity and availability of Institutional Data as well as any Information Systems that store, process, or transmit Institutional Data.

PURPOSE

To protect all **Institutional Data** in a manner that is considered reasonable and appropriate, as defined in the College's Data Governance Plan.

GENERAL PROVISIONS

Violations of this Policy may result in suspension or loss of the violator's use privileges, with respect to Institutional Data and College-owned Information Systems. Additional administrative sanctions may apply up to and including termination of employment or contractor status with the College. Civil, criminal and equitable remedies may also apply.

TERMS AND DEFINITIONS

TERM	DEFINITION
Agent	For the purpose of this Policy, is defined as any employee or third-party person who has been contracted by the College to provide a set of services and who stores, processes, or transmits Institutional Data as part of those services.
Policies	Subject to review and comment by the President's Cabinet before submission to the Board of Governors for final approval and adoption.
Information System	Any electronic system that stores, processes, or transmits information.
Institutional Data	Any data that is owned or licensed by the College.
Chief Data Officer	The Chief Data Officer is a senior executive responsible for the utilization and governance of data across the organization. The Director of Institutional Effectiveness and Grants currently serves as the Chief Data Officer.

SECTION 1: Policy

- 1.1 Throughout its lifecycle, all **Institutional Data** shall be protected in a manner that is considered reasonable and appropriate, as defined in the College's Data Governance Plan (as approved by the Chief Data Officer, Vice President for Information Technology Services, and President's Cabinet), given the level of sensitivity, value and criticality that the Institutional Data has to the College.
- 1.2 Any **Information System** that stores, processes or transmits Institutional Data shall be secured in a manner that is considered reasonable and appropriate, as defined in the College's Data Governance Plan (as approved by the Chief Data Officer, Vice President for Information Technology Services, and Cabinet), given the level of sensitivity, value and criticality that the Institutional Data has to the College.
- 1.3 Individual **Agents** who are authorized to access **Institutional Data** shall adhere to the appropriate [Information Security Roles and Responsibilities](#), as defined in the College's Data Governance Plan (as approved by the Chief Data Officer, Vice President for Information Technology Services, and Cabinet).

SECTION 2: Additional Information

If you have any questions or concerns related to this Policy, please send email to the College's Chief Information Security Officer (CISO), Steven L. Garlow (sgarlow@newriver.edu).

Additional information can also be found using the following resources:

CISA Incident Reporting System

<https://us-cert.cisa.gov/forms/report>

New River CTC Data Governance Plan

<https://web.newriver.edu/projects/data-governance/>

WVHEPC Data Classification and Protection Policy

<http://www.wvhepc.edu/wp-content/uploads/2020/03/Data-Classification-and-Protection-Policy.pdf>

WVHEPC Cybersecurity Incident Response Form

<http://www.wvhepc.edu/wp-content/uploads/2020/03/Incident-Reporting-Form.docx>

WVHEPC Privacy Management and Incident Response Plan

<http://www.wvhepc.edu/wp-content/uploads/2020/03/Incident-Response-Plan.pdf>

EXCEPTIONS/EXCLUSIONS

Exceptions to this Policy must be formally documented and approved by the Vice President for Information Technology Services, under the guidance of the President's Cabinet. Policy exceptions will be reviewed on a periodic basis for appropriateness.

REVIEW

This Policy will be reviewed by the Vice President for Information Technology Services on an annual basis or as deemed appropriate based on changes in technology and regulatory requirements.

APPROVAL SIGNATURES

Tom J. Lemke 10/8/2020

Board of Governors Chair **Date**

DocuSigned by:

Bonny B. Copenhagen

President **Date**

RELATED POLICIES, OTHER REFERENCES AND ADDITIONAL NOTES

ASSOCIATED FORMS

HISTORY		
REVISION DATE	DESCRIPTION OF CHANGE	VICE PRESIDENT APPROVAL
10/01/2020	New Policy	

New River Community and Technical College expects all faculty, staff and students to be familiar with and adhere to all applicable college policies.