

NEW RIVER Community College

New River Community College Information Technology Security Plan

Note: Links are restricted to employees - requires VCCS credentials.

New River Community College adheres to the policies, models, standards, and guidelines set forth by the Virginia Community College System (VCCS) Information Security Program. This, along with College-specific supporting documentation, constitutes the College's Information Technology Security Plan.

Governance

VCCS governance considers it essential to communicate its information security requirements throughout the organization to all users in a form that is relevant, accessible, current, and understandable to any reader. Standards are applicable to all organizations that comprise the Virginia Community College System (VCCS) including the System Office, the Shared Services Center, and all Community Colleges and to all persons directly or indirectly employed by the VCCS including student employees, faculty, adjunct faculty, staff, and contract personnel.

The College has chosen the Intranet as the communication vehicle for faculty and staff.

- [04 - Risk Management](#)
- [05 - Information Security Program](#)
- [06 - Organization of Information Security](#)
- [07 - Personnel Information Security](#)
- [08 - Asset Management](#)
- [09 - Access Control](#)
- [10 - Cryptography](#)
- [11 - Physical and Environmental Security](#)
- [12 - Operations Security](#)
- [13 - Communications Security](#)
- [14 - System Acquisition Development and Maintenance](#)
- [15 - External Party Relationships](#)
- [16 - Incident Management](#)
- [17 - Business Continuity Management](#)

- [18 - Compliance](#)
- [19 - Public Cloud Services](#)
- [20 – Office 365](#)

Summary

New River Community College works constantly to neutralize, or minimize, all known vulnerabilities identified via the risk assessment of information technology resources and environment. While conducting business there remains inevitable risks that exist, therefore, it must be recognized that we function in this environment yet strive to provide services while instituting reasonable protective measures. The College will determine funding sources during planning to rectify, where applicable, any discrepancies of non-compliance with ISO/IEC 27002:2013(E), as identified from conducting the Business Impact Analysis and the Risk Assessment for Information Technology Infrastructure.

Contact the college's Information Security Officer (wcressell@nr.edu) for further information or with questions on the college Information Technology Security Plan.