



WYTHEVILLE COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

The College has adopted 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 a protected network location as the communication vehicle for faculty and staff. College-specific information technology security documents are available at: P:\IT Documentation\Security Documents

Security Controls

The purpose of security controls is to perform the tasks in the management, planning, technical, and operational safeguards and security measures to ensure the College's confidential and sensitive information is secure, that data remains intact, and that College services remain available to our patrons. These resources are vulnerable to being rendered unusable or crippled due to sabotage, human error and natural disasters. To preserve the integrity of information technology resources, all areas of the College must contribute to the appropriate level of protection of these mission critical resources. The primary areas of focus for security controls which significantly reduce threats are:

- | | |
|---|---|
| 4 – Information Security Risk Management | 12 – Operations Security |
| 5 – Information Security Management Program | 13 – Communications Security |
| 6 – Organization of Information Security | 14 – System Acquisition, Development & Maintenance |
| 7 – Human Resource Security | 15 – Supplier Relationships |
| 8 – Asset Management | 16 – Information Security Incident Management |
| 9 – Access Control | 17 – Information Security Aspects of Business Continuity Management |
| 10 – Cryptography | 18 – Compliance |
| 11 – Physical and Environmental Security | 19 – Cloud Services |

Summary

The College constantly works 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 [Information Security Officer](#) for further information or questions on the college Information Technology Security Plan.