INFORMATION TECHNOLOGY SECURITY PLAN

The SSC has adopted the policies, models, standards, and guidelines set forth by the Virginia Community College System (VCCS) Information Security Program. This, along with supporting documentation, constitutes the SSC'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.

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 SSC'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 SSC 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:

- 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

INFORMATION TECHNOLOGY SECURITY PLAN

- 19 - Public Cloud Services

Summary

The SSC 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 SSC 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 Information Security Officer (Rick Friesen, help@ssc.vccs.edu) for further information or questions on the SSC's Information Technology Security Plan.