



| | |
|----------------|-----------------------|
| Policy No. | 70001 |
| Effective Date | Feb. 23, 2009 |
| Revision Dates | 11/29/16 |
| Revision No. | 1 |
| Approved: | Cheryl Thompson-Stacy |
| Date: | January 11, 2017 |

INFORMATION TECHNOLOGY SECURITY POLICY

1.0 Purpose

Lord Fairfax Community College (LFCC) is part of the Virginia Community College System (VCCS) and, accordingly, is obliged to comply with the various VCCS and Commonwealth of Virginia (COV) policies, standards, regulations and guidelines. This policy is intended to ensure the College's full and on-going compliance with COV policies and procedures governing the proper implementation and management of information technology security policies.

2.0 Revision History

None: New policy

3.0 Applicability

This policy applies to all LFCC faculty, staff, administration, students, guests and visitors with network access other than the public wireless Internet network.

4.0 Policy

LFCC is fully committed to be in compliance with the various Information Technology (IT) security policies, standards, regulations and guidelines set forth by the VCCS.

5.0 Definitions

COV ITRM Standards ISO27000: Commonwealth of Virginia, Information Technology Resource Management, this is a security standard which defines the minimum acceptable level of IT security.

Commonwealth of Virginia (COV): This refers to the government of the Commonwealth of Virginia, and its agencies and departments.

Separation of Duties: This is an assignment of responsibilities such that no one individual or function has complete control of an entire process. Separation of duties is a technique for maintaining and monitoring accountability and responsibility for IT systems and data.

6.0 Responsibilities

All persons are responsible for knowing and adhering to this policy and its procedures.

It is a requirement of the VCCS IT Security Standard and the COV ITRM Standards ISO27000 that all employees and third-party contractors having access to network administrative systems be aware of best practices for “safe” computing activities. All employees and third-party contractors are to annually receive and be certified in the College security awareness training program. The College posts information regarding security awareness training on its website, and offers periodic informal training sessions.

All supervisors must ensure that all of their respective employees complete their annual security training. Initial hiring orientation processes will include information regarding the mandatory annual security awareness training requirement.

All supervisors must annually review their employees’ job descriptions to ensure that “separation of duties” is documented as mandated by the COV ITRM Standards ISO27000 Security Audit Standard.

7.0 Procedure

The College will continually review its internal business processes in order to meet the mandatory compliance statements of the latest revision or updates pertinent to the COV ITRM Standards ISO27000 and various VCCS IT security standards with no need for vetting these standards.

8.0 Sanctions

Failure to comply with the terms of this policy may result in disciplinary action by the appropriate College official.

9.0 Interpretation

Authority for interpretation of this policy rests with the vice president of financial and administrative services.

10.0 Authority/Reference

The Code of Virginia, Title 2.2-2827, "Restrictions on State employee access to information Infrastructure".

<http://law.lis.virginia.gov/vacode/title2.2/chapter28/section2.2-2827/>

The Code of Virginia, Title 2.2-2009, "Policies, procedures, and standards that address IT security audits".

<http://law.lis.virginia.gov/vacode/title2.2/chapter28/section2.2-2827/>

<http://law.lis.virginia.gov/vacode/title2.2/chapter20.1/section2.2-2009/>

The VCCS Information Technology 5.1 Security Program, revision 1, Sept. 1, 2016.

<https://buzz2.vccs.edu/teams/src/Information%20Security%20Program%202016/Forms/AllItems.aspx?RootFolder=%2Fteams%2Fsrc%2FInformation%20Security%20Program%202016%2FStandards%2F05%5FInformation%5FSecurity%5FProgram&FolderCTID=0x0120005F2B0D832AE25D4B9B2D66D2AA682E45&View=%7BCE300093%2D9AD7%2D4BE9%2D8DC1%2D6D089B027EDA%7D>