LFCC Information Technology Security Plan

The College has adopted the policies, models, standards and guidelines set forth by the VCCS. These, along with College supporting documentation (policies, procedures, executive summaries, application profiles, etc.) constitute the College's security plan.

The following describes the major parts of the security planning process and provides current information for those documents that must be updated as part of the security planning.

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. The College has chosen the Intranet to be the communication vehicle for faculty and staff. All LFCC information security policies are available at: http://www.lfcc.edu/about-the-college/office-of-financial-and-administrative-services/technology-services-475/computer-security-information/index.html

This includes legal, regulatory, and contractual requirements; security awareness training; and business continuity management.

Security Roles and Responsibilities

Information technology security roles are assigned to individuals to ensure accountability and compliance among the information technology processes. The role or working title and assignment of personnel for each security role may differ at each college however it is critical that each function be identified and the individuals assigned have the appropriate skill sets. Individuals may be assigned multiple roles, as long as the multiple role assignments provide adequate separation of duties, provide adequate protection against the possibility of fraud, and do not lead to a conflict of interests.

Dr. Cheryl Thompson-Stacey, President has designated the following employees as Information Security Officers for the College:

Mr. Douglas M. Shrier, Primary Information Security Officer
Mr. Christopher Grabenstein, Secondary Information Security Officer

Updated forms are sent to the VCCS Security Officer as needed and at least annually.

F:\ISO27002\Additional\ISO Designation	Updated and sent to the VCCS Security Officer January 2013.
F:\ISO Designation - Presidential Approval Letter	Personnel change sent to the VCCS Security Officer January 2013.

Security roles are assigned during the completion of the Business Impact Analysis processes. The EWP Addendum completed annually denotes the security roles.

The College IT Security Plan Committee

The Security Plan Committee is led by the College's Information Security Officer (ISO). Other committee members include the Information Technology Strategist, the Network Administrator/backup Information Security Officer. Other employees may be temporary members of the committee depending on the topic and expertise required. Additionally, all college-wide information technology security policies are reviewed and approved during the President's Advisory Team (PAT) meeting prior to being placed on the College's Intranet.

Business Impact Analysis

The Business Impact Analysis (BIA) is a key step in the contingency management process. The BIA enables the Contingency Planning Coordinator to characterize fully the system requirements, processes, and interdependencies and use this information to determine contingency requirements and priorities.

F:\ISO27002\7.2 Information Classification\2012 BIA Surveys	Business Impact Analysis Completed December 14, 2012 (Data uploaded to VCCS: UT21/VCCSBusiness server

Risk Assessment

The Risk Assessment (RA) process is conducted to identify the potential threat to an IT system, determine the likelihood a potential threat will occur, identify and evaluate vulnerabilities, and determine the loss impact if one or more vulnerabilities are exploited by a potential threat. The output of this process aids in identifying appropriate controls for reducing or eliminating risk.

This document reports on the risks identified through the business impact analysis process, questionnaires, and interviews.

F:\ISO27002\7.2 Information classification\LFCC Risk Assessment Summary 12-26-12	Completed December 2012. Data uploaded to the VCCS: UT21/VCCSBusiness server.

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, un-willful 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:

- Risk Assessment and Treatment
- Security Policy
- Organization of Information Security
- Asset Management
- Human Resource Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Information Systems Acquisitions Development and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance
- PCI

Continuity of Operations Planning

Continuity of Operations Planning (COOP) includes developing plans necessary to provide continuity of essential College IT systems and data in accordance with the Virginia Department of Emergency Management (VDEM).

Mr. Chris Boies has been designated as Continuity of Operations (COOP) Coordinator for the College. Updated plans are approved by the College President and submitted to VDEM and are maintained on a restricted shared network folder. Paper copies are securely housed off-site as required.

\\LF.....\..\LFCC Continuity Plan April 2013a	Updated March 2013

Disaster Recovery Planning

IT Contingency Planning includes developing plans to minimize the disruptions of critical functions and the capability to recover critical IT systems in accordance with ISO/IEC 27002:2005(E). *The outcome may contribute to various plans that properly organize the response, recovery, and continuity activities for disruptions affecting the relationship between IT systems and business processes supported by the IT systems.*

The IT Disaster Recovery Plan is updated in accordance with ISO/IEC 27002:2005(E). Copies are securely housed off-site as required.

F:\ISO27002\10.5 Backup\Disaster Recovery Planning\LFCC Cont & DRP April 2013	Updated April 2013

The IT Disaster Recovery Plan will be updated based on any defaults discovered during the testing.

F:\ISO27002\10.5 Backup\Annual DR Plans\Annual DR Test Elec Outage report 6/10/11	June 10, 2011
F:\ISO27002\10.5 Backup\Annual DR Plans\Annual DR Test Network Outlage report 7/12/12	July 12, 2012

Review and Report

All processes will be reviewed as needed when the development, installation and/or changes occur to the College environment. The college's ISO and the IT Security Plan Committee will review the security plan periodically. A complete review will be completed every three years.

Summary

The College is moving in positive directions to neutralize or minimize all known vulnerabilities identified via the risk assessment of information technology recourses 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 be determining funding sources during planning to rectify where applicable any discrepancies of non-compliance with ISO/IEC 27002:2005(E), as identified from conducting the Business Impact Analysis and the Risk Assessment for Information Technology Infrastructure.