LFCC
Lord Fairfax Community College

Technology Standard

Personnel Security – Security Awareness and Training

Version 2.0
Status: Updated 7/29/09 12/29/12 4/28/13
Contact: Coordinator of IT Network Security of LFCC

PURPOSE

Lord Fairfax Community College (LFCC) will establish and maintain a information technology security awareness and training program for sensitive information systems to ensure that all computer/network users are aware of their security responsibilities in regards to College IT resources. All computer/network users shall receive an information technology security awareness training by utilizing an on-line service known as Securing The Human (STH) which is hosted by SANS.

SCOPE

As described in the VCCS Security Awareness and Training Program document, "In accordance with the ISO27002 Security Standard, a security awareness and training program must be implemented for all managers, administrators, and users to focus attention on security and produce relevant and needed security skills and competency. Further, the security awareness and training program must provide technical training for all VCCS employees involved in the management, administration, operation, development, or use of information systems."

APPLICABILITY

The Security Awareness and Training Standard is applicable to all LFCC employees, or anyone that may have access to the College's IT systems.

STANDARD

Overview
All Employees will receive Information security awareness training that is at a level commensurate with job responsibility, sensitivity of information handled, and expertise required to meet the information security needs of the college. These needs may be met either through general security training or may require more specialized training. Employee participation in security awareness and training is mandated by the ISO27002 Security Standard and must be documented and maintained on file.

At a minimum, the following IT security awareness training will be provided.

- All new employees must complete the Securing The Human (STH) IT security awareness training within 30 days of their hire date. Adjunct faculty and third-party contractors may acknowledge their IT security awareness training by signature on the Adjunct and Third Party IT Security Awareness document.

- All LFCC employees are required to annually complete a set of on-line video training modules using the STH curriculum. Adjunct faculty and third-party contractors may acknowledge their IT security awareness training by signature on the Adjunct and Third Party IT Security Awareness document.

- System Owners and Data Owners receive additional training targeting college and VCCS security awareness topics.

- Information Security Officers receive additional training that focuses on policy and practices that will help to maintain a secure information technology environment for the college.

- Technology Services staff are provided with technical training that will increase skills regarding college security policies, practices, and controls and how to effectively implement them.

- Specialized training is conducted for those users who have roles in college contingency and disaster plans such as COOP, DRP, ERT etc, to ensure that they can effectively implement their responsibilities.

Internal and web-based training is available to all employees with EWP's that support their job duties that handle sensitive data in the eVA, AIS, SIS, CIPPS, PMIS or CARS systems. The data owners in conjunction with external agencies such as DHRM, DOE, or VCCS will facilitate the proper training venues and timing to conduct various training sessions throughout the year. Data owners of these systems will schedule within the first 30 days of a new hire employee, the appropriate training in order for the new hire to complete their job duties.

Each data owner of a sensitive system will document and forward to the ISO on an annual basis the following training activity information that was provided to LFCC employees:

- Title of the training event
- A sample of the training materials for each event.
- Verification of attendees receiving the training materials.
- Title and name of the individual/entity providing the training.
- Procedures and/ Processes that were used that provide tracking and scheduling.

Management's responsibility shall include the following:

- The President of the college annually designates the Primary and Backup Security Officers who are responsible for the college Information Technology Security Program.
- The college ISO reports to the Vice Present of Financial and Administrative Services, who reports directly to the President. This provides the shortest practical reporting lines to the agency head.
- The college's Business Impact Analysis and Risk Assessment reports provide information to direct the training needs for this document.

- The college's Polices and Procedures, hard copy memos, and e-mail communiqués are used for facilitating the communication process between Technology Services and other areas of the college.

In compliance with periodic audit review, exceptions to security safeguards are not allowed and do not exist. The security officers of the college are the only personnel with the ability to override the access to any system. College security officers would only exercise this authority in the event of an emergency or as direct by appropriate college authority.

- **Application/System Training**

  Employee training for applications and/systems that provide access to confidential information will be provided by the respective data owner as identified in the college Business Analysis Impact report. Data owners are also responsible for monitoring the appropriate compliance certifications as well as annually providing verification of the training activities for themselves and the appropriate end-users for each their respective areas of responsibility..

  The College Information Security Officer is assigned the responsibility of developing, implementing, testing, training, monitoring compliance certifications, and periodically updating the college information security awareness and training program known as STH.

- IT Security Awareness Training (STH) will include but not limited to:

  - Information Security – Roles & Responsibilities, Electronic & Non-Electronic, Information Handling, Encryption, Information Security Best Practices

  - Internet Security – Internet Usage & Access, Malicious Software and Code, Internet Threats, Best Practices

  - E-mail & Viruses – E-mail Security, E-mail Threats, Viruses & Ad-ware, E-mail Best Practices

  - Social Hacking – Weakest Links, Social Engineering, Incident Reporting

  - Acceptable Use and Ethics Agreement

  - FERPA Guidelines

All documentation containing sensitive information about college network procedures and safeguards are maintained in a physically secured area of the college. All documentation containing sensitive information for college departmental procedures and safeguards are the responsibility of that department to house in a secured location.

Primary Security Officer
Doug Shrier
(540) 868-7199
dshrier@lfcc.edu

Secondary Security Officer
Chris Grabenstein
(540) 868-7246
cgrabenstein@lfcc.edu

Examples of Training Opportunities

College training of end-users may be delivered by means of but not limited to:

- Online security training
- In-house hosted workshops (group and one-on-one)
- Posters, brochures, electronic bulletin boards
- College sponsored Professional Development Opportunities (PDO)
- Subscriptions to technical magazines
- Informational email messages to users
- External Workshops and seminars
- Obtaining technical manuals, reference materials and/or other documentation related to applications and systems

- **New Employee Orientation**

  New employees are required to attend an orientation to the college. The Human Resources Office is responsible for conducting a majority of the new employee orientation. In addition IT security awareness training is provided within thirty days of employment to all new hires and subsequently on an annual basis for all employees.

  The data owners for eVA, AIS, PMIS, CIPPS, CARS and the SIS Security officer makes a determination and provides the appropriate training to end-users as it relates to their respective database applications. The AIS and eVA data owners conduct monthly discussions with the Business Office staff to review gaps in end-user training needs that can be resolved with scheduling future training workshops.

- **Professional Development Day**

  Professional development days provide an opportunity for college staff to update their skills by means of short courses on a variety of topics. These short courses include but are not limited to, administrative procedures, IT security topics, AIS/eVA updates, SIS business processes, and various technical support or special interest topics.

- **Forums**

  Each data owner has the option of delivering a portion of specialized training to the appropriate end-users by means of periodic short forums. An attendance log is kept for each training event. Some forums are mandatory based upon a person's job title and/or duties and other forums are optional to attend.

- **Help Desk Alerts and Reminders**

  The Technology Services Help Desk will use e-mail and web pages to alert, remind, and instruct users on computer security topics.

- **Departmental Newsletters**

  Each department of the college has the option to maintain an on-line newsletter. Updates are periodically posted on the college website to keep the public and end-users up-to-date with special announcements.