Standard Operating Procedure

Procedure Title: Acceptable Use Policy
Procedure #: IT.001
Revision #: 1

Unit Responsible: Divisional Office, Information Technology Services Division
Individual Responsible: Chief Information Officer

Effective Date: 08/17/2021

Initial Approval Date: 08/17/2021
Last Review/Update Date: 2/15/2023
Next Review Date: 08/17/2024

***Does this procedure support a Board Policy?** *Yes*
If yes, identify: 6.010 - Acceptable Use

Board policies can be found at: LCC Board of Trustees Policy Page

***Does this procedure support HLC criteria?** *Yes*
If yes, identify: *2A2, 3D4, 5B1*

HLC Criteria can be found at: HLC Accreditation Criteria

***Does this procedure support a State or Federal Regulation?** Yes
If yes, identify: FERPA – Family Educational Rights and Privacy Act, PCI DSS – Payment Card Industry Data Security Standard, GDPR -- EU's General Data Protection Regulation, HIPAA -- Health Insurance Portability and Accountability Act, GLBA -- Gramm–Leach–Bliley Act, FTC Red Flag Rule, and Michigan's Identity Theft Protection Act.

***Note: Standard Operating Procedures should be in furtherance of some LCC policy and/or accreditation criteria, even if the relationship is not direct. Assistance in determining this information can be obtained from the Academic Procedure Advisory Committee (APAC) and/or the Accreditation Liaison Officer.**

Acceptable Use Policy, BP 6.010

1. Purpose

This procedure describes guidelines for the use of the College's technology resources and College wide data. It addresses the monitoring, enforcement, and practices associated with the Acceptable Use policy.

2. Scope

This procedure applies to all Information Technology Services (ITS) Division employees involved in the monitoring of usage of the College's technology resources and the performance of authorized investigations into potential misuse of technology resources.

3. Prerequisites

N/A

4. Responsibilities

Employees throughout the ITS Division share the responsibility and play a role in the implementation of this procedure. Responsibility for the interpretation and administration of the Acceptable Use Policy and this procedure is delegated to the Chief Information Officer or his/her designee(s).

5. Procedure

A. Technology Use Monitoring
- The ITS Division utilizes a number of tools for the automated scanning and monitoring of systems and communications traffic in order to protect and secure the College's information assets.
  - These tools continuously scan email and internet traffic using College resources to identify and prevent spam, viruses, malware, and other types of attacks and intrusions that pose a threat to the College. When staff are alerted by these tools that something unusual has occurred, they will investigate to determine if the College is at risk and will respond accordingly.
  - A security tool is used to scan computers on a monthly basis to determine if data conforming to the format of Social Security or credit card numbers are present. When such patterns are found, an email is subsequently sent to the user of the computer requesting that the suspected data be reviewed and removed or flagged as a false positive. Guidelines are provided to the user outlining this process.
- Suspect emails and potential malware are occasionally reported to the ITS Division by the user community. ITS staff will respond to these reports, investigate them, and take appropriate action to mitigate any threat to the College.

B. Investigations
   - The ITS Division does not engage in any investigations without prior authorization except for those that may be triggered by alerts from our automated monitoring and scanning tools as noted above.
   - Required Authorizations
     - Employee Related Investigations: Executive Vice President or Executive Director of Human Resources
     - Student Related Investigations: Director of Student Compliance
     - FOIA/Legal Related Investigations: Director of Risk Management & Legal Services
     - Security Camera Related Investigations: Director of Public Safety
   - All requests for an investigation, the subject of an investigation, and the results of an investigation are to remain confidential.

C. Issuance of College Owned Mobile Devices
   - Mobile computing devices such as laptops, tablets, and smart phones are issued to employees at the request and approval of their respective Executive Leadership Team member.
   - Prior to the device being issued, the user is required to read and sign the "Employee Mobile Device User Agreement" to acknowledge they understand the College's expectations regarding the use and care of the device.

6. Reference

N/A

7. Definitions

N/A