August 2013

INFORMATION SECURITY STANDARD

Version 1.0

CALIFORNIA COMMUNITY COLLEGES

Effective Date: 9/1/2013

Last Revision Date: 8/23/2013

Contents

CONTENTS 2

1 INTRODUCTION 4

2 SCOPE 4

3 INFORMATION SECURITY RISK MANAGEMENT 5

3.1 Information Security Risk Assessment 5

3.2 Information Security Risk Mitigation 6

3.3 Information Security Risk Transference 6

3.4 Information Security Risk Acceptance 6

3.5 Information Security Risk Monitoring 7

4 PRIVACY OF PERSONAL INFORMATION 7

4.1 Collection of Personal Information 7

4.2 Access to Personal Information 8

4.3 Access to Electronic Data Containing Personal Information 8

5 INFORMATION SECURITY AWARENESS AND TRAINING 9

5.1 Information Security Awareness 9

5.2 Information Security Training 9

6 MANAGING THIRD PARTIES 10

6.1 Granting Access to Third Parties 10

7 INFORMATION TECHNOLOGY SECURITY 10

7.1 Protections Against Malicious Software Programs 10

7.2 Network Security 10

7.3 Mobile Devices 11

7.4 Information Asset Monitoring 11

8 CHANGE CONTROL 12

8.1 Emergency Changes 12

9 ACCESS CONTROL 12

9.1 Need-to-know 13

9.2 Separation of Duties 13

9.3 Password Management 13

9.4 Access Review 14

9.5 Modifying Access 14

10 ASSET MANAGEMENT 14

11 POLICY ENFORCEMENT 14

1 Introduction

The California Community Colleges are creating a standard of best information security practices for protecting the confidentiality, integrity and availability of LONG BEACH COMMUNITY COLLEGE DISTRICT (LBCCD) information assets. Unauthorized modification, deletion, or disclosure of information assets can compromise the mission of the LBCCD, violate individual privacy rights, and possibly constitute a criminal act.

It is the collective responsibility of all users to ensure:

- Confidentiality of information which the LBCCD must protect from unauthorized access.
- Integrity and availability of information stored on or processed by LBCCD information systems.
- Compliance with applicable laws, regulations, and LBCCD policies governing information security and privacy protection.

The LBCCD Information Security Standards are not intended to prevent, prohibit, or inhibit the sanctioned use of information assets as required to meet the LBCCD's core mission and LBCCD academic and administrative goals. But to ensure that these goals are achieved while meeting the COLLEGE'S/DISTRICT'S obligation to protect and safeguard information.

2 Scope

The California Community Colleges Information Security Standard is a set of best information security practices that would apply to the following:

- Central and departmentally-managed LBCCD information assets.
- All users employed by LBCCD or any other person with access to LBCCD information assets.
- All categories of information, regardless of the medium in which the information asset is held or transmitted (e.g. physical or electronic).
- Information technology facilities, applications, hardware systems, and network resources owned or managed by the LBCCD.

The purpose is to provide a continuous up-to-date information security standard that LBCCD may adopt once through passage of a LBCCD Information Security Policy that refers to this standard.

Auxiliaries, external businesses and organizations that use LBCCD information assets must operate those assets in conformity with the LBCCD's Information Security Policy based on this standard.

This standard was created by the CCC Systemwide Architecture Committee with input from the CCC Information Security Advisory Committee. This standard will be updated from time to time, as will be reflected in the revision number. Once adopted, LBCCD's Information Security Policy should always refer to the current version of the standard. LBCCD's Police Departments that access the FBI's Criminal Justice Information Services (CJIS) will have more Information Security requirements that are addressed in CJIS Security Policy, see http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center.

3 Information Security Risk Management

Risk management involves the identification and evaluation of risks to information security assets (risk assessment) and the ongoing collection of information about the risk (risk monitoring). Once a risk has been identified, the LBCCD will develop and implement strategies to reduce the risk to acceptable levels (risk mitigation), share or shift the risk to another party (risk transference), or assume the identified risk (risk acceptance).

The LBCCD will develop risk management processes that identify, assess, and monitor risks to information assets containing level 1 Confidential and level 2 Internal Use data as defined in the LBCCD Data Classification Standard. This data may be referred to as "Protected Data". Identified risks to these information assets must be actively managed by data owners and/or appropriate administrators in order to prioritize resources and remediation efforts.

3.1 Information Security Risk Assessment

Risk assessments are part of an ongoing risk management process. Risk assessments provide the basis for prioritization and selection of remediation activities and can be used to monitor the effectiveness of LBCCD controls.

The LBCCD shall document the scope and frequency of the risk assessment; risk assessment methodology; result of the risk assessment; and, mitigation strategies designed to address identified risks.

3.2 Information Security Risk Mitigation

Risk mitigation involves prioritizing, evaluating, and implementing appropriate risk-reducing activities recommended as a result of the risk assessment process. Since the elimination of all risk is impossible, LBCCD leadership shall balance the cost and effectiveness of the proposed risk-reducing activities against the risk being addressed.

The LBCCD shall select appropriate mechanisms to safeguard the confidentiality, integrity, and availability of information assets containing protected data. LBCCD mitigation strategies shall be commensurate with risks identified by risk assessments. For those risks where the mitigation strategy involves the use of controls, those controls shall ensure that risks are reduced to an acceptable level, taking into account:

- Legal and regulatory requirements and compliance.
- Cost of implementation, maintenance, and operation.
- LBCCD operation and policy requirements and constraints.

Each LBCCD shall develop and maintain a process for documenting and tracking decisions related to risk mitigation activities.

3.3 Information Security Risk Transference

Whenever possible, a risk may be managed by sharing or completely transferring it to another entity. The LBCCD may transfer risks if the required actions of the receiving entity are deemed to result in an acceptable outcome should the risk be exploited and damage occurs. Risks associated with potential failure to comply with applicable laws, statutes, or regulations can only be transferred if the results will support compliance. External entities must meet or exceed the level of security that the LBCCD protects its information assets with. The LBCCD shall develop and maintain a process for documenting and tracking decisions related to risk transference activities.

3.4 Information Security Risk Acceptance

Risk acceptance occurs when potential risk-reduction activities cannot be found or those identified are determined not to be cost effective (e.g. the protection measures cost more than the potential loss). In the case where resources for the best mitigation strategy are not available, the risk must be addressed to the extent possible using available resources. Identified acceptable risks shall be recorded in a central LBCCD risk register. The LBCCD shall develop a process for documenting, reviewing and approving accepted risks. Accepted risks

identified in the risk registry shall undergo periodic review and approval by appropriate administrators.

3.5 Information Security Risk Monitoring

Sometimes, when a risk is identified, there may be insufficient or conflicting information regarding its likelihood of occurrence or potential impact. The LBCCD shall monitor risks of this nature and develop a plan to gather sufficient information to judge whether the risk shall be mitigated, transferred, or accepted. If the risk is accepted, it shall be added to the LBCCD'S risk registry.

4 Privacy of Personal Information

All users of LBCCD information systems or network resources are advised to consider the open nature of information disseminated electronically and must not assume any degree of privacy or restricted access to information they create or store on LBCCD systems. The LBCCD is a public college system, and information stored on LBCCD information systems may be subject to disclosure under state law. No LBCCD information system or network resource can absolutely ensure that unauthorized persons will not gain access to information or activities. However, the LBCCD acknowledges its obligation to respect and protect private information about individuals stored on LBCCD information systems and network resources. Should personally identifiable information (identified in California law Civil Code 1798.29) be compromised accidentally or maliciously the COLLEG/DISTRICT is required to inform the effected parties. If more than 500 California residents are effected, then a copy of the notification must be provided to the California Attorney General. To protect the privacy of the COLLEG/DISTRICTS data all staff (including part time and student workers) that have access to Level 1 Confidential data shall have a DOJ Live Scan background check.

4.1 Collection of Personal Information

To comply with state and federal laws and regulations, the LBCCD shall not collect personally identifiable information unless the need for it has been clearly established.

Where such information is collected:

- The LBCCD shall use reasonable efforts to ensure that personally identifiable information is adequately protected from unauthorized disclosure.
- The LBCCD shall store personally identifiable information only when it is appropriate and relevant to the purpose for which it has been collected.

4.2 Access to Personal Information

Except as noted elsewhere in LBCCD policy, information about individuals stored on LBCCD information systems shall only be accessed by:

- The individual to whom the stored information applies or his/her designated representative(s).
- Authorized LBCCD employees with a valid LBCCD-related business need to access, modify, or disclose that information.
- Appropriate legal authorities.

When appropriate, authorized LBCCD personnel following established LBCCD procedures may access, modify, and/or disclose information about individuals stored on LBCCD information systems or a user's activities on LBCCD information systems or network resources without consent from the individual. For example, a LBCCD may take such actions for any of the following reasons:

- To comply with applicable laws or regulations.
- To comply with or enforce applicable LBCCD policy.
- To ensure the confidentiality, integrity or availability of LBCCD information.
- To respond to valid legal requests or demands for access to LBCCD information.

If LBCCD personnel accesses, modifies, and/or discloses information about an individual and/or his/her activities on LBCCD information systems or network resources, staff will make every reasonable effort to respect information and communications that are privileged or otherwise protected from disclosure by LBCCD policy or applicable laws.

4.3 Access to Electronic Data Containing Personal Information

Individuals who access or store protected data must use due diligence to prevent unauthorized access and disclosure of such assets.

Browsing, altering, or accessing electronic messages or stored files in another user's account, computer, or storage device is prohibited, even when such accounts or files are not password protected, unless specifically authorized by the user for LBCCD business reasons. This prohibition does not affect:

- Authorized access to shared files and/or resources based on assigned roles and responsibilities.
- Authorized access by a network administrator, computer support technician, or departmental manager where such access is within the scope of that individual's job duties.

- Access to implicitly publicly accessible resources such as LBCCD websites.
- LBCCD response to subpoenas or other court orders.
- LBCCD response to a request pursuant to public record disclosure laws.

5 Information Security Awareness and Training

LBCCD shall implement a program for providing appropriate information security awareness and training to employees appropriate to their access to LBCCD information assets. The LBCCD ***information security awareness*** program shall promote strategies for protecting information assets containing protected data.

All employees with access to protected data and information assets shall participate in appropriate information security awareness training. When appropriate, *information security training* shall be provided to individuals whose job functions require specialized skill or knowledge in information security.

5.1 Information Security Awareness

The security awareness program shall provide an overview of LBCCD information security policies, and help individuals recognize and appropriately respond to threats to LBCCD information assets containing “Protected Data” as defined in the LBCCD Data Classification Standard.

The program shall promote awareness of:

- LBCCD information security policies, standards, procedures, and guidelines.
- Potential threats against LBCCD protected data and information assets.
- Appropriate controls and procedures to protect the confidentiality, integrity, and availability of protected data and information assets.
- LBCCD notification procedures in the event protected data is compromised.

After receiving initial security awareness training, employees shall receive regular updates in policies, standards, procedures and guidelines. The updates shall be relevant to the employee’s job function, duties and responsibilities. All staff that has access to Level 1 Confidential data shall undergo information security awareness training.

5.2 Information Security Training

When necessary, the LBCCD information security program shall provide or coordinate training for individuals whose job functions require special knowledge

of security threats, vulnerabilities, and safeguards. This training shall focus on expanding knowledge, skills, and abilities for individuals who are assigned information security responsibilities.

6 Managing Third Parties

Third parties who access LBCCD information assets shall be required to adhere to appropriate LBCCD information security policies and standards. As appropriate, a risk assessment shall be conducted to determine the specific implications and control requirements for the service provided, and be reassessed periodically.

6.1 Granting Access to Third Parties

Third party service providers may be granted access to LBCCD information assets containing protected data as defined in the LBCCD Data Classification Standard only when they have a need for specific access in order to accomplish an authorized task. This access shall be authorized by a designated LBCCD official and based on the principles of need-to-know and least privilege.

Third party service providers shall not be granted access to LBCCD “Protected Data” as defined in the LBCCD Data Classification Standard until the access has been authorized, appropriate security controls have been implemented, and a contract/agreement has been signed defining the terms for access.

7 Information Technology Security

LBCCD shall develop and implement appropriate technical controls to minimize risks to their information technology infrastructure. LBCCD shall take reasonable steps to protect the confidentiality, integrity, and availability of its critical assets and protected data from threats.

7.1 Protections Against Malicious Software Programs

LBCCD shall have plans in place to detect, prevent, and report malicious software effectively. Electronic data received from untrusted sources shall be checked for malicious software prior to being placed on a non-quarantined location on a LBCCD network or information system.

7.2 Network Security

LBCCD shall appropriately design their networks—based on risk, data classification, and access—in order to ensure the confidentiality, integrity and availability of their information assets. LBCCD shall implement and regularly

review a documented process for transmitting data over the LBCCD network. This process shall include the identification of critical information systems and protected data that is transmitted through the LBCCD network or is stored on LBCCD computers. LBCCD processes for transmitting or storing critical assets and protected data shall ensure confidentiality, integrity, and availability.

7.3 Mobile Devices

LBCCD shall develop and implement controls for securing protected data stored on mobile devices. Protected data shall not be stored on mobile devices unless effective security controls have been implemented to protect the data. LBCCD shall use encryption, or equally effective measures, on all mobile devices that store level 1 Confidential data as defined in the LBCCD Data Classification Standard. Alternatives to encryption must be reviewed on a case-by-case basis and approved in writing by a designated LBCCD official. Other effective measures include physical protection that ensures only authorized access to protected data.

7.4 Information Asset Monitoring

LBCCD shall implement appropriate controls on the monitoring of information systems and network resources to ensure that monitoring is limited to approved activities. Monitoring shall not be conducted for the purpose of gaining unauthorized access, “snooping”, or for other activities that violate their LBCCD Acceptable Use Policy. Records created by monitoring controls (e.g. logging) shall be protected from unauthorized access and reviewed regularly. LBCCD shall ensure that only individuals who have a “need-to-know” are granted access to data generated from monitoring controls.

Data generated by monitoring shall be retained for a period of time that is consistent with effective use, LBCCD records retention schedules, regulatory, and legal requirements such as compliance with litigation holds.

At a minimum, server administrators shall regularly scan, remediate, and report un-remediated vulnerabilities on critical systems or systems that store protected information within a prescribed timeframe. The risk level of a system determines the frequency at which logs shall be reviewed. Risk factors to consider are:

- Criticality of business process.
- Information classification associated with the system.
- Past experience or understanding of system vulnerabilities.
- System exposure (e.g., services offered to the Internet).

8 Change Control

Changes to information technology systems, network resources, and applications shall be appropriately managed to minimize the risk of introducing unexpected vulnerabilities and ensure that existing security protections are not adversely impacted. LBCCD shall establish and document a process to manage changes to LBCCD information assets containing “Protected Data”, as defined in the LBCCD Data Classification Standard.

LBCCD shall evaluate the information security impact of changes by taking a risk-based approach to change control.

Changes to information assets which store protected data will likely require a more rigorous review than changes to non-critical assets and shall be made in accordance with a formal, documented change control process. Changes that may impact the security of these information assets shall be identified along with the level of control necessary to manage the change.

LBCCD shall define and communicate the scope of significant changes to “Protected Data” in order to be sure that all affected parties have adequate information to determine if a proposed change is subject to the change management approval process.

8.1 Emergency Changes

Only authorized persons shall make an emergency change to LBCCD information assets containing “Protected Data” as defined in the LBCCD Data Classification Standard. Emergency changes are defined as changes which, due to urgency or criticality, need to occur outside of the LBCCD formal change management process.

Such emergency changes shall be appropriately documented and promptly submitted, after the change, to the LBCCD normal change management process.

9 Access Control

On-campus or remote access to information assets containing “Protected Data” as defined in the LBCCD Data Classification Standard shall be based on operational and security requirements. Appropriate controls shall be in place to prevent unauthorized access to protected information assets. This includes not only the primary operational copy of the protected information assets, but also data extracts and backup copies. LBCCD shall have a documented process for provisioning approved additions, changes, and terminations of access rights and

reviewing access of existing account holders. Access to LBCCD protected information assets shall be denied until specifically authorized.

Access to public and shared resources shall be excluded from this requirement. LBCCD shall identify and document public or shared resources that are excluded from this requirement. Authorized users and their access privileges shall be specified by the data owner, unless otherwise defined by LBCCD policy.

9.1 Need-to-know

Access to LBCCD information assets containing protected data as defined in the LBCCD Data Classification Standard shall be provided only to those having a need for specific access in order to accomplish an authorized task. Access shall be based on the principles of need-to-know and least privilege.

Authentication controls for access to LBCCD protected data must be unique to each individual and shall not be shared unless authorized by appropriate LBCCD management. Where approval is granted for shared authentication, the requesting organization shall be informed of the risks of such access and the shared account shall be assigned a designated owner. Shared authentication privileges shall be regularly reviewed and re-approved at least annually.

9.2 Separation of Duties

Separation of duties principles shall be followed when assigning job responsibilities relating to restricted or essential resources. LBCCD shall maintain an appropriate level of separation of duties when issuing credentials to individuals who have access to information assets containing protected data. LBCCD shall avoid issuing credentials that allow a user greater access or more authority over information assets than is required by the employee's job duties.

9.3 Password Management

The LBCCD must identify and communicate acceptable password criteria. The criteria may vary by system or application at the campus' discretion based upon a risk assessment.

The LBCCD must identify and communicate a password change schedule. The schedule may vary by system or application at the LBCCD's discretion based upon a risk assessment. A sample schedule follows:

- Passwords with administrative access to "Protected Data" must be changed every 90 days.

- Passwords with ability to create application transactions (e.g., create purchase requisitions, approve purchase requisitions, create general ledger transactions) must be changed every 180 days.
- Password reuse must be restricted to no more than once every four (4) uses.
- Accounts shall be locked for a duration of 20 minutes upon 5 wrong password attempts.
- First-time passwords (e.g., passwords assigned by IT administrators upon account creation or during password resets) must be set to a unique value per user and changed immediately after first use. Campus information systems and network resources must not display, transmit, or store passwords in clear text.

9.4 Access Review

LBCCD shall develop procedures to detect unauthorized access and privileges assigned to authorized users that exceed the required access rights needed to perform their job functions. Appropriate LBCCD managers and data owners shall review, at least annually, user access rights to information assets containing protected data. The results of the review shall be documented.

9.5 Modifying Access

Modifications to user access privileges shall be tracked and logged. Users experiencing a change in employment status (e.g., termination or position change) shall have their logical access rights reviewed, and if necessary, modified or revoked.

10 Asset Management

The LBCCD must provide for the integrity and security of its information assets by identifying ownership responsibility, as defined with respect to the following:

- Owners of the information within the LBCCD.
- Custodians of the information.
- Users of the information.
- Classification of information to ensure that each information asset is identified as to its information class in accordance with law and administrative policy.

11 Policy Enforcement

The LBCCD respects the rights of its employees and students. In support of the LBCCD Information Security Policy, the LBCCD shall establish procedures that

ensure investigations involving employees and students suspected of violating the LBCCD Information Security Policy are conducted in compliance with appropriate laws, regulations, collective bargaining agreements, and LBCCD policies. Additionally, LBCCD shall develop procedures for reporting violations of this policy.

The LBCCD reserves the right to temporarily or permanently suspend, block, or restrict access to information assets, independent of such procedures, when it reasonably appears necessary to do so in order to protect the confidentiality, integrity, availability, or functionality of LBCCD resources or to protect the LBCCD from liability.

Allegations against employees that are sustained shall result in disciplinary action. Such actions shall be administered in a manner consistent with the terms of the applicable collective bargaining agreements and the California Education code. Student infractions of the LBCCD Information Security Policy shall be handled in accordance with the established student conduct process. Auxiliary employees who violate the requirements of the policy shall be subject to appropriate disciplinary actions as defined by their organization's policies. Third party service providers who do not comply with this policy will be subject to appropriate actions as defined in contractual agreements and other legal remedies available to the LBCCD.

The LBCCD may also refer suspected violations to appropriate law enforcement agencies.

REVISION HISTORY

RESOURCES AND REFERENCE MATERIALS

Useful Guidelines:

Related Principles:

Sound Business Practices:

Laws, State Codes, Regulations and Mandates:

- California Civil Code 1798.29, 1798.82, and 1798.84
- Family Education Rights and Privacy Act (FERPA)