CDL Information Technology Key Security Guidelines & Baseline Supporting Practices

Introduction

In order to fulfill its mission to support the University of California community's scholarship and to extend the University's public service mission, the California Digital Library (CDL) is committed to providing a secure information technology infrastructure that protects the integrity, confidentiality, and ownership of information while maintaining the fundamental accessibility to content and tools promised in our service descriptions and commitments.

Each member of the CDL community is responsible for the security and protection of electronic information resources over which he or she has control. Resources to be protected include networks, computers, software, and data. The physical and logical integrity of these resources must be protected against threats such as unauthorized intrusions, malicious misuse, or inadvertent compromise. Activities outsourced to external entities must comply with the same security requirements as in-house activities.

These guidelines, baseline supporting practices, and incident reporting practices together form CDL's commitment to meeting the UC Office of the President's security policy mandate that "UCOP departments should implement procedures and practices that ensure, to the extent possible, the confidentiality, integrity, and availability of the University's information assets, as well as the protection of sensitive data".
Except where otherwise noted these guidelines and practices apply to the CDL's Computing and Storage Resource Center (i.e. the server, storage, and network infrastructure used to develop, test, and deliver CDL services) and its staff desktop computing environment. For its constituencies the CDL may broker access to Internet sites, content and services that are outside of the CDL's administrative domain. The entities that own and operate those sites establish and publish security policies and practices which may vary from these guidelines and to which site users may be obligated to adhere.

1. Key Guidelines

1.1. Roles and Responsibilities

Responsibilities range in scope from administering security controls for a CDL program to the protection of one's own access password(s). A particular individual often has more than one role. Roles include:
1.1.1. Administrative Officials (individuals with administrative responsibility for CDL programs or units or individuals having functional ownership of data – nominally including members of the CDL Director's Cabinet, and CDL program Technical Leads) must:

- identify the electronic information resources within areas under their control;
- define the purpose and function of the resources and confirm that CDL's security guidelines and baseline practices provide adequate protection;
- identify and recommend any needed variance from CDL's security guidelines and baseline practices by assessing risk factors such as:
    - the criticality of the information resource or data to the continued operation of the program, the CDL, the University, or other stakeholders;
    - how negatively the operations of one or more units would be affected by unavailability or reduced availability of the resources,
    - how likely it is that a resource could be used as a platform for inappropriate acts towards other entities,
    - limits of available technology, programmatic needs, cost, and staff support;
- ensure that requisite security measures are implemented for the resources;

- ensure that requisite education and documentation are provided to their staff members as needed;
- for systems in support of CDL/University business administration, ensure compliance with relevant provisions of BFB IS-3 "Electronic Information Security".

1.1.2. Service staff (individuals who design, manage, and operate CDL electronic information resources, e.g. project managers, system designers, application programmers, or system administrators) must:

- become knowledgeable regarding relevant security requirements and guidelines;
- analyze potential threats and the feasibility of various security measures in order to provide recommendations to Administrative Officials;
- implement security measures that mitigate threats, consistent with the level of acceptable risk established by administrative officials;
- establish procedures to ensure that privileged accounts are kept to a minimum and that privileged users comply with privileged access agreements;
- for systems in support of University business administration, establish procedures to implement relevant provisions of BFB IS-3;
- communicate the purpose and appropriate use for the resources under their control.

1.1.3. Users (individuals who access and use CDL electronic information resources) must:

- become knowledgeable about relevant and explicit security requirements and guidelines upon which their use is conditional;
- protect the resources under their control, such as access passwords, computers, and data they download.

1.1.4. Departmental Security Officer (individual responsible for coordinating CDL departmental security guidelines and practices) shall be designated by the CDL Executive Director in consultation with the UCOP security officer.

1.1.5 Other entities with important CDL information resource security responsibilities include the UC Office of the President's Information Technology Services department (ITS) and the UC Information Security group; the UC Berkeley data center (which provides data center services for a portion of the CDL's IT infrastructure) and System and Network Security (SNS) Office; the AWS Security & Compliance team; and the electronic software and content vendors with whom the CDL does business on behalf of the University of California. Insufficient security measures at any level may cause resources to be damaged, stolen, or become a liability to the University. Therefore, preventive and responsive actions may be taken. Actions that may be taken, and the guidelines for them, are described below in "Baseline Supporting Practices" and "Incidence Response."

1.2. Key Security Elements

1.2.1. Logical Security

- Host systems, operating systems, and externally sourced applications software must have the most recently available and appropriate software security patches within the relevant software/OS distribution, commensurate with acceptable risk.
- Applications must be designed, implemented, and managed to minimize the risk from malicious or accidental misuse of the application and any associated data.
- Adequate authentication and authorization functions must be provided, commensurate with appropriate use and the acceptable level of risk. In general CDL follows a least privileges model, in which privileged users of a system are granted the least amount of privilege necessary to fulfill their responsibilities.
- Adequate electronic perimeter controls must be in place to control and manage the origins, targets, and allowable connections to CDL server and desktop systems.
- System monitoring must be designed to detect configuration changes and intrusions commensurate with acceptable risk. System logs must be kept and examined as required to detect unusual behavior and conduct forensics for incident analysis and reporting (following a principle of least privilege necessary for such detection and analysis).

1.2.2. Physical Security

- Appropriate controls must be employed to protect physical access to resources, commensurate with the identified level of acceptable risk. These may range in scope and complexity from extensive security installations to protect a room or facility where CDL servers and storage are located, to simple measures taken to protect a CDL staff member's laptop from theft.

1.2.3. Privacy and Confidentiality

- Applications must be designed and systems must be used so as to protect the privacy and confidentiality of the various types of electronic data they process, in accordance with applicable laws and the CDL's Privacy Policy.

1.2.4. Compliance with Law and Policy

- Security policies that apply to all University electronic information resources, including those of the CDL, include, but are not limited to the UC Electronic Communications Policy (http://www.ucop.edu/ucophome/policies/ec/). Electronic information resources used in support of University business administration must comply with the provisions of Business and Finance Bulletin IS-3 Electronic Information Security. Federal and state laws prohibit theft or abuse of computers and other electronic resources.
- The following activities are specifically prohibited under this Policy:
    - interfering with, tampering with, or disrupting resources;
    - intentionally transmitting any computer viruses, worms, or other malicious software;
    - attempting to access, accessing, or exploiting resources you are not authorized to access;
    - knowingly enabling inappropriate levels of access or exploitation of resources by others;
    - downloading sensitive or confidential electronic information/data to computers that are not adequately configured to protect it from unauthorized access;
    - disclosing any electronic information/data you do not have a right to disclose.
    - In addition to any possible legal sanctions, violators of this Policy may be subject to disciplinary action up to and including dismissal or expulsion, pursuant to UCOP policies, collective bargaining agreements, codes of conduct, or other instrument governing the individual's relationship with the University. Recourse to such actions shall be as provided for under the provisions of those instruments.

1.2.5. Contacts:

- Questions about this Policy or other campus electronic information resource policies may be directed to the CDL Executive Director.
- Report CDL security incidents to CDL Systems Administration.
- For information about UC campus-based computer security policies and procedures consult the Campus "Local IT Policies".

1.2.6. Changes to this policy:

- This policy may be reviewed and revised from time to time as required by legal or contextual changes affecting UC, UCOP, or the CDL. The current policy, with its effective date, is maintained and publicly available at http://www.cdlib.org/about/policies.html. The current policy and past versions of it are also available in hard copy upon request.

2. Baseline Supporting Practices

Adopted September 27, 2011; [revised January 22, 2016]

2.1 Security awareness and training

- Upon employment all CDL staff are required to read the CDL and UCOP security policies and guidelines and to complete the University of California Computer Security Basics Online Training (http://webtutorials.ucsd.edu/csecforOP/index.html).
- No less than twice per year security issues are discussed in staff meetings.
- Application security is a standing agenda item on the CDL's TechCouncil meetings.

- Staff development for CDL System administrators include system security training, staff development/training plans are reviewed and updated during annual staff reviews.

2.2 Logical Security

- OS security - CDL servers in all environments (development, stage, and production) are patched or upgraded twice yearly (following change management practices) and as critical security issues arise; critical security issues are monitored through subscription to vendor announcements, and SANS@Risk news.
- Database security – Database engines are patched or upgraded no less than once per year and as critical security issues arise; critical security issues are monitored through subscription to vendor announcement lists and regular attendance at user group and vendor-sponsored conferences.
- Application security – CDL's TechCouncil has a standing agenda item to discuss common application security issues. TechCouncil also identifies, and recommends training for, no fewer than 3 developers as "application security advisers" available to the entire CDL developer community. Each CDL program and application owner is responsible for monitoring critical security issues of application components.
- Authentication/authorization – Server login accounts are managed according to the CDL's System Access and Account Management Policy which dictates password strength, password encryption, sudo privileges, account removal upon termination, and provisioning of trusted external user accounts. CDL maintains global login accounts and sudo privileges via global account management strategies and tools. Account provisioning requires approval by an Administrative Official and is performed by a limited and controlled set of authorized system administrators whose membership is approved by the Manager, Infrastructure and Applications Support.
- Electronic perimeter control – all CDL IT environments are protected by a Firewall Services Module (FWSM). Firewall configuration is based upon a "least access necessary" principle – allowable traffic is specified and all other traffic is denied. Logins are permitted only through encryption (using SSH) and limited to known and trusted origin addresses, Non-UC origins addresses are established only through documented business needs (a list of such needs and addresses is maintained in CDL's "External User's Access Policy." To the fullest extent possible, when originating outside of the CDL network blocks, logins are allowed only through a hardened bastion server. Firewall configuration changes are performed by a limited and controlled list of authorized system administrators whose membership is approved by the Manager, Infrastructure and Applications Support (for dev and stage environments) or the Manager, Systems Engineering (for production environment).
- Encryption – Secure Shell (SSH) is used for all remote logins and Secure Sockets Layer (SSL) is implemented when data protection warrants it. All CDL laptops are secured through local disk encryption (as per policy from IR&C, which manages most desktop and laptop class computers). When necessary the CDL is prepared to encrypt data during transmission outside of firewall-protected zones or when copied onto backup media. [Note: The CDL does not generally acquire, generate, or manage "restricted data" as defined by Business and Finance Bulletin IS-3 Electronic Information Security. In a condition where it does acquire such data, or data that requires equivalent protection, encryption and encryption key management would be implemented as described in IS-3. Per the CDL's Privacy Policy, regular audits of data and data retention ensure the identification of data that would rise to this level of protection.
- System logging, monitoring, and vulnerability and intrusion detection – System messages and sudo activity are logged and scanned daily in all environments. Intrusion detection software is or will be used on all servers to monitor OS and critical file changes [note: IDS deployment is 50% complete as of adoption date]. Vulnerability assessments are or will be conducted annually on CDL servers following the Center for Internet Security benchmarks (http://www.cisecurity.org) [note: vulnerability assessment deployment is 50% complete as of adoption date]. Network-level intrusion detection and vulnerability scanning is provided continuously by network operations groups for all CDL environments.

- Data transfer – Transfer of data into and out of CDL systems (other than public read access) is actively managed in compliance within the logical security guidelines above, and by implementing the appropriate baseline practices herein, to ensure that the data transfer is monitored and logged, and the data transfer initiator, whether an individual or a process, is authenticated and authorized. Data is encrypted or not according to the nature of the data (whether it includes sensitive or restricted data), and business need.
- Disposition of equipment – CDL and UCOP asset management procedures inventory and track equipment locations and document equipment decommissioning. Equipment is decommissioned through UC's Corporate Equipment, Facilities, and Assets System (EFA); All magnetic media on decommissioned equipment is erased via degaussing before leaving the data center in which it resides.

2.3 Physical security

- The two data centers in which CDL servers and storage are located adhere to IS-3 level controls for limiting physical access to facilities housing restricted or essential resources and are implemented through the use of combination locks, key locks, badge readers, manual sign in/out logs, verification of identification, etc. The ability to track both ingress and egress of all individuals is maintained. Access privileges are granted by data center policies; CDL staff with such privileges is limited and approved by the Manager, Infrastructure and Applications Support. CDL desktops are located in a secure facility requiring keycard access.

3. Incident response

- The CDL follows the UCOP Security Incident Handling Process when a security breach within its Computing Storage and Resource Center is reported, suspected, or confirmed. See the UC Privacy and Data Security Incident Response Plan for an example of the process for responding to a security-related incident.