
**INFORMATION SECURITY OFFICE**

# Information Systems Security Requirements for Projects (ISO/SR1)

**Version 3.5**

**October 2007**

## Revision History

| Doc No. / Rev No. | Revision Date | Revised By | Description of Revision / Change |
|---|---|---|---|
| S19 / R1.5 | 1/10/2007 | A. Lancashire CDHS | Reformatting changes |
| SR1 / R1.0 | 9/12/2007 | M. Serapio DHCS, B. Kelsey CDPH | Updated to address new best practices (previous version had dependencies to best practices from pre-SOA), fill existing regulatory gaps, remove vendor dependencies, reword language to make applicable to COTS/MOTS applications, and re-designated document number and name. |
| SR1/v1.5 | 9/14/2007 | I. Sanford DHCS | Various grammatical and definition changes. Clarification of terms and responsibilities. |
| SR1/v2.0 | 9/21/2007 | I. Sanford DHCS | Post team review updates |
| SR1/v2.1 | 10/17/2007 | J. Cleveland CDPH | 2nd team review comments/changes |
| SR1/V2.2 | 10/21/2007 | J. Cleveland CDPH | Added Admin User ID and password section from Ian Sanford and Data Query section from Brett Kelsey. |
| SR1/V2.3 | 10/22/2007 | J. Cleveland CDPH | Modifications to Admin User ID and password section and Data Query section. |
| SR1/V3.0 | 10/25/2007 | J. Cleveland CDPH | Minor grammatical changes, removal of dynamic web links, and added COTS language in C.8. |
| SR1/V3.5 | 10/26/2007 | J. Cleveland CDPH | Addition of Sections A.13, A.14, B.12, B.13, B.14, B.15, and B.16 for the purpose of covering Privacy, when used in conjunction with BAAs. |

| | |
|---|---|
| *Type:* **ISO Requirements** | |
| *Issued:* **October 26, 2007** | *Doc Number:* **SR 1/v3.5** |
| *Revised:* | |
| *Title:* **Information Systems Security Requirements for Projects** | |

## I. Purpose

This document provides the minimum security requirements, mandated by the Information Security Office (ISO) from projects governed and/or subject to the policies and standards of the California Department of Public Health (CDPH). Projects that intend to deploy systems/applications into the Department's system infrastructure or will consume Department information system services are also subject to these minimum security requirements.

This document is intended to assist the Department and its service consumers in understanding the criteria the Department will use when evaluating and certifying the system design and security features and protocols used by project solutions consuming Department services. The security requirements herewith will also be used in conjunction with the Department ISO's compliance review program of its information system services consumers.

This document will serve as a universal set of requirements which must be met regardless of physical hosting location or entities providing operations and maintenance responsibility. These requirements do not serve any specific project nor do they prescribe any specific implementation technology.

## II. Scope of Requirements

The information security requirements herein are organized in five categories (sections) and address at a minimum:

- Administrative/Management Safeguards
- Technical and Operational Safeguards
- Solution Architecture
- Documentation of Solution
- ISO Notifications

## III. Contact

Chief Information Security Officer
California Department of Public Health
Information Security Office
1615 Capital Avenue
Sacramento, Ca 95814

## IV. Information Systems Security Requirements

### A. Administrative / Management Safeguards

#### 1. Workforce Confidentiality Statement

All persons working with Department information must sign a confidentiality statement. The statement must include at a minimum; General Use, Security and Privacy safeguards, Unacceptable Use, Audit, and Enforcement policies. (Contact the ISO for the current version of the Security & Confidentiality form in use.)

The statement must be signed by the project member prior to being granted access to the Department's information. The statement must be renewed annually.

#### 2. Access Authorization

Project/Program must implement and document clear rules and processes for vetting and granting authorizations; and procedures for the supervision of workforce members who work with Department information or in locations where it might be accessed.

#### 3. Access Authorization Maintenance

On at least a semi-annual basis, Project/Program will review and remove all authorizations for individuals who have left the department, transferred to another unit, or assumed new job duties within the department.

#### 4. Information System Activity Review

Project/Program must implement and document procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

#### 5. Periodic System Security Review

All systems shall allow for periodic system security reviews that provide assurance that management, operations, personnel, and technical controls are functioning effectively and providing adequate levels of protection.

The reviews may include technical tools and security procedures such as virus scanners, vulnerability assessment products (which look for known security problems, configuration errors, and the installation of the latest hardware/software "patches"), and penetration testing.

## 6. Periodic System Log Review

All systems processing and/or storing Department information shall have a method or procedure in place to create and review system logs for unauthorized access. Logs may be stored within the system or on a centralized logging server or service, and shall be maintained for a minimum of three years.

## 7. Business Impact Analysis

Project/Program will conduct annually a Business Impact Analysis of the application to determine the Maximum Acceptable Outage (MAO), cost of lost functionality, system component dependencies, business function dependencies, and business partner dependencies.

## 8. Change Control

All systems processing and/or storing Department information must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity, and availability of information.

For those systems running within the Department's environment and/or are consuming Department services, those systems shall comply with DTS and Department standards for change control process and procedures.

## 9. Incident Response

Establish procedures for responding to an emergency or other occurrence (e.g., fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

The emergency response procedures shall be added to the existing Operational Recovery Plan (ORP). The ORP shall address what to do if a computer system and/or the information files are violated, lost, damaged, or inaccessible.

## 10. Disaster Recovery

Establish procedures that allow facility access in support of restoration of lost information under the ORP and emergency mode operations plan in the event of an emergency.

The restoration/recovery support procedures shall be added to the existing Operational Recovery Plan (ORP) to restore any loss of information and assure continuity of computing operations for support of the application and information.

Recovery procedures shall be developed using Appendix "J" Template from the Department's ORP.

### 11. Emergency Mode Operation Plan

Establish an Emergency Mode Operation Plan to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode. This plan shall be added to the existing ORP.

### 12. Periodic System Recovery Testing

All systems, as part of a new or existing project, shall allow for periodic system recovery testing. The period between tests should be defined as part of the project and be consistent with relevant department disaster recovery standards. Such testing should provide assurances that plans (Incident Response, Disaster Recovery, Emergency Mode Operation, and Data Backup) and controls (management, operations, personnel, and technical) are functioning effectively and providing adequate levels of protection during an incident, disaster, or breach.

### 13. Supervision of Data

Public Health Information (PHI) in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk, or office. Unattended means that information is not being observed by an employee authorized to access the information. Department PHI in paper form shall not be left unattended at any time in vehicles or planes and shall not be contained in checked-in baggage on commercial airplanes.

### 14. Escorting Visitors

Visitors to areas where Department PHI is contained shall be escorted and Department PHI shall be kept out of sight while visitors are in the area.

## B. Technical and Operational Safeguards

### 1. System Security Compliance

All project systems shall comply with applicable department security policies and requirements, as specified in the State Administrative Manual, Health Administrative Manual, HIPAA, Privacy Act, and any other applicable state or federal regulation. All security safeguards and precautions shall be subject to the approval of the Department ISO.

### 2. Virus Protection

All systems shall install and actively use comprehensive third-party anti-virus and virus protection software, and routinely update such software when updates are Released. All security safeguards and precautions shall be subject to the approval of the Department ISO.

### 3. Patch Management

All systems shall install and actively use comprehensive third-party patch management program and routinely update system and application software when updates are released. All security safeguards and precautions shall be subject to the approval of the Department ISO.

### 4. Encrypted Electronic Transmissions

All information transmissions that contain confidential information must be encrypted end-to-end using an industry-recognized encryption standard. The electronic transport must utilize Secure Socket Layer (SSL) and Department information and confidential information shall be encrypted at the minimum of 128 bit AES or 3DES (Triple DES) if AES is unavailable. Equivalent or stronger algorithms may be used upon approval of the Department ISO.

### 5. Encrypted Data Storage

All confidential information must be encrypted when stored using a department approved encryption standard. Confidential information shall be encrypted at the minimum of 128 bit AES or 3DES (Triple DES) if AES is unavailable. Equivalent or stronger algorithms may be used upon approval of the Department ISO.

### 6. Workstation / Laptop Encryption

All workstations and laptops that process and/or store Department information must be encrypted with a Department approved solution or a solution using a vendor product specified on the California Strategic Sourced Initiative (CSSI) located at the following link: www.pd.dgs.ca.gov/masters/EncryptionSoftware.html

### 7. Removable Media Encryption

All electronic files that contain Department information must be encrypted when stored on any removable media type device (i.e. USB thumb drives, floppies, CD/DVD, tape backup, etc.) with a Department approved solution or a solution using a vendor product specified on the California Strategic Sourced Initiative (CSSI) located at the following link: www.pd.dgs.ca.gov/masters/EncryptionSoftware.html

### 8. Secure Connectivity

All transmission and data-links between the information and application/system and DBMS and the DTS WAN shall be secure between transmission systems as required by regulation, policy or standard and as prescribed for the given application/system.

## 9. Intrusion Detection and Prevention

All systems that are accessible via the Internet, are critical, or contain ePHI shall install and actively use a Department approved comprehensive third-party real-time host based intrusion detection and prevention program that reports security events directly to the Department ISO. All security safeguards and precautions shall be subject to the approval of Department ISO.

## 10. Minimum Data Downloads

In accordance with the principle of need-to-know, only the minimum amount of information required to perform necessary business functions should be copied or downloaded.

## 11. Data Destruction

All Department information must be wiped from systems when the information is no longer necessary. The wipe method must conform to Department of Defense and Department standards for information destruction. Once information has been destroyed, the Department contract manager must be notified. If an agency or other entity is unable to destroy media in accordance with Department standards and provide notification, the media must be returned to the Department after usage for destruction in an approved manner.

## 12. Confidential Destruction

Department PHI in paper form must be disposed of through confidential means, such as cross cut shredding and pulverizing.

## 13. Removal of Data

Department PHI in either electronic or paper form shall not be removed from Department premises or from the premises of an authorized vendor or contractor without the written permission of the Department ISO.

## 14. Faxing of Confidential Information

Facsimile transmissions containing PHI shall not be left unattended and fax machines shall be in secure areas. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them. Fax numbers must be verified before sending.

## 15. Mailing of Confidential Information

Department PHI shall only be mailed using secure methods. Large volume mailings of Department PHI must be by a secure, bonded courier with signature required on receipt. Disks and other transportable media sent through the mail must be

encrypted with a Department approved solution or a solution using a vendor product specified on the CSSI.

## C. Solution Architecture

### 1. System Security Compliance

The system shall comply with all applicable Department security policies and requirements, as well as those specified in the State Administrative Manual, Health Administrative Manual, HIPAA, Privacy Act, and any other applicable state or federal regulation. All security safeguards and precautions shall be subject to the approval of the Department ISO.

### 2. Access Point Warning Banner

All systems containing Department information shall display a warning banner stating that information is confidential, activity is logged, and system use is for business purposes only. User shall be directed to log off the system if they do not agree with these requirements.

The following warning banner shall be used for all access points (e.g., desktops, laptops, web applications, mainframe applications, servers and network devices):

***WARNING: This is a State of California computer system that is for official use by authorized users and is subject to being monitored and/or restricted at any time. Unauthorized or improper use of this system may result in administrative disciplinary action and/or civil and criminal penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use.***

***LOG OFF IMMEDIATELY, if you do not agree to the conditions stated in this warning.***

### 3. Layered Application Design

Application must be able to be segmented into a layered application design separating at a minimum the Presentation, Application/Business Logic, and Data Access Logic, and Data Persistence/Database layers.

### 4. Separation of Layers

The Presentation, Application/Business Logic, and Data Access Logic layer must be separated physically by a firewall regardless of physical implementation.

Vendor-provided commercial off-the-shelf (COTS) packages or components where physical separation of layers is not possible requires ISO approval.

## 5. Business Logic Layer Communication

Any system request made to the Business logic layer must be authenticated.

## 6. Data Access Logic Layer Design

The Data Access Logic Layer may take the form of stored procedures, database API, Data Access Objects/Components, Data Access Middleware, Shared Data Services, or Secure Web Service.

## 7. Data Access Logic Layer Communication

Any system request made to the Data Access logic layer must be authenticated and authorized.

## 8. Data Persistence/Database Layer Isolation

No direct access to the Data Persistence/Database layer will be permitted, except through the Data Access logic layer.

All calls to the Data Persistence/Database layer will be made through the Data Access logic layer as a trusted sub-system that utilizes a single database access account to all transactions.

Vendor-provided commercial off-the-shelf (COTS) packages or components where physical separation of Data Access Logic layer from Data Persistence/Database layer is not possible require ISO approval.

## 9. User Input Validation

All user input must be validated. The system must manage client input controls from server side to the extent possible. All third-party client side input controls must be documented and approved by the Department ISO.

## 10. Data Input Validation

All user information input must be validated before being committed to the database or other application information repository.

## 11. Data Queries

All Data queries (including In-line SQL calls) will not be allowed from the Presentation or the Business Logic layers unless validated for appropriate use of query language and validated for appropriate quantity/quality of data input. All data queries solution must be approved by department CISO.

Database table names and column names must not be exposed. Applications must use an alias for every table and column.

Dynamic SQL will not be permitted from the Presentation Layer without prior approval from the department ISO.

## 12. Username/Password Based Authentication

When usernames and passwords are going to be used as the method for system authentication the following for each must be met:

- Username requirements:
  - Usernames are unique and are traceable to an individual worker.
  - Usernames are NOT to be shared and never hard-coded into system logic.
- Password requirements:
  - Are not to be shared.
  - Must be 8 characters or more in length.
  - Must NOT be a word found in the dictionary, regardless of language.
  - Password must NOT be stored in clear text.
  - Must be changed at least every 60 days.
  - Must be changed immediately if revealed or compromised.
  - Passwords must be encrypted using irreversible industry-accepted strong encryption.
  - Accounts must be locked after 3 failed logon attempts.
  - Account lock-out reset timers must be set for a minimum of 15 minutes.
  - Must be composed of characters from at least three of the following four groups from the standard keyboard:
    - Upper case letters (A-Z);
    - Lower case letters (a-z);
    - Arabic numerals (0 through 9); and
    - Non-alphanumeric characters (punctuation symbols).

## 13. Administrator Username/Password Based Authentication

- Username requirements:
  - Must be unique and are traceable to an individual person.
  - Must NOT be shared.
  - Must never be hard-coded into system logic.
  - Must NOT be the same across different zones (e.g. Web Zone, Internal network, and Test Labs / Environments).
  - The default built-in Administrator account must be renamed and disabled.
  - The naming convention for administrator usernames must not make it obvious that usernames belong to administrator accounts.
  - If a generic Administrator account is created:
    - It must only be used in an Emergency.
    - It is NOT to be used for routine maintenance.
    - The password storage and management process for generic administrator accounts must be approved by the Department ISO.
- Password requirements:
  - Must not be the same as any of the previous 10 passwords.

- Must not to be shared.
- Must NOT be the same across different zones (e.g. Web Zone, Internal network, and Test Labs / Environments).
- Must be 12 characters or more in length.
- Must NOT be a word found in the dictionary, regardless of language.
- Password must NOT be stored in clear text.
- Must be changed at least every 60 days.
- Must be changed immediately if revealed, or compromised.
- Must be changed immediately upon the termination or transfer of an employee with knowledge of the password.
- Passwords must be encrypted using industry accepted, irreversible strong encryption.
- Accounts must be locked after 3 failed logon attempts.
- Account lock-out timers must be set for at least 60 minutes.
- Must be comprised of characters from at least three of the following four groups from the standard keyboard:
    - Upper case letters (A-Z);
    - Lower case letters (a-z);
    - Arabic numerals (0 through 9);
    - Non-alphanumeric characters (punctuation symbols).

## 14. Role - Based Access

Any system deployed during, or as a result of a project, shall provide secure role-based access for authorization utilizing the principle of least privilege at all layers/tiers.

## 15. User / Entity Authentication Logging

System must log success and failures of user authentication at all layers as well as log all user transactions at the database layer as required by regulation, policy or standard and as prescribed for the given application/system. This logging shall be included for all user privilege levels including but not limited to systems administrators. This requirement applies to systems that process, store, and/or interface with PII and/or confidential information.

## 16. Automatic System Session Expiration

The system must provide an automatic timeout of user sessions after 20 minutes of inactivity.

## 17. Automatic System Lock-out and Reporting

The system must provide an automatic lock-out of users and a means to audit a minimum of 3 failed log-in attempts. The means of providing audit information must be approved by the departmental ISO.

## 18. Role-based Access to Audit Functions and Data

All systems/applications will implement role-based access to auditing functions and audit trail information utilizing the principle of least privilege

## 19. Secure Online Access to Audit Functions

All systems / applications will implement a secure online interface to Audit Capabilities and Reporting by way of application programming interface (API) or network service (or Web Service); to allow Department ISO to view logs, auditing procedures, and audit reporting.

## 20. Audit Trails

This requirement delineates the (minimum) log information that audit trails should record for any system that contains or is involved in the transmission of confidential information. The information listed below should be available on every system running a production environment. Not only will this information assist with problem resolution efforts and system restore operations, it will also be invaluable to system penetration attack investigations, fraud investigations, and the like.

The system must record (at minimum) the following events and any other events deemed appropriate by the Department ISO:

Transaction Types

- Any and all administrative changes to the system (i.e.: administrative password changes (forgotten password resets), system variables, network configuration changes, disk subsystem modifications, etc).
- Logon failures.
- Logons during non-business hours.
- Program or file access denial.
- Addition, deletion, or modification of users or program access privileges.
- Changes in file access restrictions.
- Database addition, deletion, or modification.
- Copy of files before and after read and write changes.
- Transaction issued.

Individual audit trail records shall contain the information needed to associate each query transaction to its initiator and relevant business purpose. Individual audit trail records should capture at a minimum the following:

Minimum Audit Trail Record Content

- Date and Time Stamp.
- Unique Username of Transaction Initiator.
- Transaction Recorded.
- Success or Failure of Transaction Recorded.
- Relevant business process or application component involved.
- Data captured (if any).

Audit Trail logs shall be maintained at minimum for three years after the occurrence or a set period of time determined by the Program's ISO that would not hinder a detailed forensic investigation of the occurrence. The Department ISO has final approval authority.

## D. Documentation of Solution

### 1. System Configuration

As part of each project, assigned staff will document and maintain a full inventory of the major hardware, software, and communications platforms in use; system configurations; all applications/components with descriptions encompassing the solution; and a description of the solution's security design features and user access control mechanisms. Project will ensure a custodian(s) is assigned to each application/component.

### 2. Data In Use Classifications

Project will document and maintain information classification matrix of all information elements accessed and/or processed by solution.

The matrix should identify at a minimum:

- information element.
- information classification/sensitivity.
- relevant function/process or where is it used.
- system and database or where is it stored.

### 3. System Roles and Relationships

Project will document the organizational structure and relationships between systems managers, systems security personnel, and users, including an estimate of the number of users that will have access to Department information within the system solution and an explanation of their job descriptions.

### 4. Audit Method Documentation

Project will document the solution's auditing features and provide samples of audit reporting.

### 5. Retention of Documentation

The system/application maintainers will retain documentation, including audit and activity logs, for a minimum of three years (up to seven years) from the date of its creation or the date it was last in effect, whichever is later.

## E. ISO Notifications

### 1. Security Compliance Notification

As part of each project, assigned staff will document how proposed solution meets or addresses the requirements specified in this document and must be submitted to the Department ISO prior to taking custody of Department owned information.

### 2. Notification of Changes to Solution

Once a project is approved as final by the ISO, no changes will be made to the project scope, documentation, systems or components without a change approval by the ISO.

### 3. Notification of Breach or Compromise

The system/application maintainers shall immediately and in writing report to the ISO on any and all breaches or compromises of system and/or information security, and shall take such remedial steps as may be necessary to restore security and repair damage, if any.

In the event of a breach or compromise of system and/or information security, the ISO may require a system/application security audit. The ISO shall review the recommendations from the security audit, and make final decisions on the steps necessary to restore security and repair damage.

The system/application maintainers shall properly implement any and all recommendations of the security audit, as approved by the ISO.