The California State University
SYSTEMWIDE HUMAN RESOURCES

Office of the Chancellor
401 Golden Shore, 4th Floor
Long Beach, CA 90802-4210
562-951-4411
email: hradmin@calstate.edu

Date: October 24, 2013

Code: **TECHNICAL LETTER HR/EHDB 2013-05**

To: Human Resources Officers

From: Evelyn Nazario
Associate Vice Chancellor
Human Resources Management & CO HR Services

William Perry
Chief Information Security Officer
Information Security

Subject: **Common Human Resources System (CHRS) Security Plan and Requirements - Policy Guidelines**

Overview

Audience: Human Resources Officers and/or HR Professionals, Security Administrators or designees responsible for campus security administration.

Action Item: Adhere to the policy guidelines for implementation of the CHRS Security Plan and Requirements.

Affected Employee Group(s)/Unit(s): Individuals responsible for supporting and administering campus security and those individuals involved in the various implementation aspects of CHRS.

Summary

This Technical Letter provides detailed information regarding the implementation of the CHRS Security Plan and Requirements.

HR Letter 2013-13 announced the release of the CHRS Security Plan and Requirements as required by the system owner, California State University (CSU) Systemwide HR. This Technical Letter includes an overview of the information contained in the CHRS Security Plan and Requirements for CHRS, which serves as official documentation. This information will establish secure protocols and uniformity for campuses and the Chancellor's Office. Information is provided based on the following sections:

Sections

Distribution:

CSU Chancellor
All Campus Vice Presidents
Associate Vice Presidents/Deans, Faculty Affairs
Human Resources Officers
Business Managers
Budget Officers
General Counsel
State Controller's Office (SCO)

6.0 CHRS Security Incident Management

7.0 CHRS Business Continuity and Disaster Recovery

8.0 CHRS Infrastructure

Questions regarding this technical letter may be directed to Human Resources Management at (562) 951-4411. This document is available on Human Resources Management's Web site at: http://www.calstate.edu/HRAdm/memos.shtml.

EN/th

The California State University
PROJECT MANAGEMENT OFFICE

CHRS Security Plan and Requirements

Last Revised: **10/18/2013**

FINAL

REVISION CONTROL

Document Title: CHRS Security Plan and Requirements
Author: Tammy Hines
File Reference: CHRS Security Plan and Requirements 20131018

Revision History

Revision Date	Revised By	Summary of Revisions	Section(s) Revised
07/05/13	T. Hines, A. Harwood, G. Mansoor	New Document	All
07/09/13	J. Whitney	Reviewed	All
07/16/13	T. Hines	Revised to remove reference to 'Central' Security Administrator	Section 1.3
08/19/13	T. Hines	Updates to indicate document is approved/final	All
10/18/13	T. Hines	Final edits for distribution	All

Review / Approval History

Review Date	Reviewed By	Action (Reviewed, Recommended or Approved)
07/05/13	Evelyn Nazario, Associate Vice Chancellor HRM and CO HR Services	Recommended for approval
07/08/13	William Perry, Chief Information Security Officer, CO Information Security	Recommended for approval
07/09/13	Jessie Lum, Chief Information System Officer, CO Information Systems	Recommended for approval
08/19/13	Gail Brooks, Vice Chancellor, Systemwide HR	Approved

Table of Contents

Page

1.0 Introduction

The Common Management Systems (CMS) currently supports California State University (CSU) campuses and the Chancellor's Office (CO) operational databases. Campuses have a minimum of seven test, development, and production databases for each application. A recent study of CMS recommended that the CSU consider consolidating applications to provide opportunities for cost savings to the CSU.

CMS goals are to achieve best business practices, reduce costs and improve performance. The CMS Executive Committee (EC) determined that CMS is not sustainable in its current state. The CMS EC proposed the Common Human Resources System (CHRS) initiative to achieve CMS's stated goals. A CHRS Advisory Group was then established to research the feasibility of adopting a common Human Resources (HR) system.

The major reasons to adopt a common HR system were to:

- Enable adoption of a system-wide HR model that facilitates the timely adoption of best business practices across all campuses.
- Allow all campuses to take full advantage of a feature rich system. Smaller campuses do not have the resources to maintain and enhance the system.
- Contain costs associated with managing CMS.
- Provide the CSU with a comprehensive reporting system via a system-wide HR reporting environment and Data Warehouse (DW).

The EC approved the CHRS Project which encompasses an enriched common HR application code and common configuration on a single platform, with an HR reporting solution.

1.1 Document Purpose

This document describes the CHRS Security Plan and Requirements as required by the system owner, CSU Systemwide HR. The protection measures described in this document were designed to ensure CHRS complies with CSU Systemwide HR Policies, CSU System-wide Information Security Standards and Policies governing information technology (including those with specific relevance to HR operations), information security and human resources as well as all pertinent state and federal regulatory requirements.

Security within CHRS will be addressed throughout the software development life cycle and within the environment supporting CHRS, including but not limited to the production and non-production network, operating system, and application levels.

1.2 Document Scope

This strategy was developed to ensure the confidentiality, integrity and availability of CHRS information assets. It outlines security controls that must be in place to reduce and mitigate CSU security risks with associated data from 23 campuses and the CO residing in one consolidated environment. The CHRS Security Plan and Requirements is not intended to be a campus procedural document or a campus operational guide; however, it

will include specific protocols that will govern the security of CHRS system-wide data. The CHRS Security team will develop and distribute additional documents to support the implementation of this plan.

1.3 Assumptions

A core security design will be developed for CHRS. This core design will include the following elements:

- Security Administrators will be assigned to CHRS to support the security management activities at the CO and campus offices. The Security Administrators will include the CO Information Security Officer (ISO) to ensure security within CHRS is managed by a subject matter expert and complies with CSU System-wide Information Security Standards and Policies governing information security.
- CHRS users will be permitted to view data applicable to their job duties only.
- Campus Distributed Security Administrators (DSAs) and other designated employees may be permitted to access system-wide data to support development within a specific CHRS project, for a specified time, with appropriate approvals from Systemwide HR.
- Authentication controls will be managed similar to the Common Financial System (CFS) through System-wide Identity Access Management (IAM) infrastructure.
- Access to the CHRS system-wide data will be based on the principles of "need-to-know" and least privileges.
- Campuses will comply with all CSU policies governing information security including the CSU's Segregation of Duties policy (SoD).

2.0 Systemwide HR Requirements

Each campus is its own appointing authority. As such, all campus information must be secured at the campus level both in production and non-production database instances. Applicable CSU Systemwide HR and Security Policies must be followed. Refer to the Appendix section for a listing of applicable CSU Systemwide HR and security policies/laws. Where specific approvals have been granted, an employee may be granted access to data at another campus when working on a specific CHRS system-wide project for a specified duration. In those instances, a "Confidentiality Agreement" must be signed by the employee and approvals to grant such access must be obtained from Systemwide HR. Quarterly audits of changes made to permissions and security roles must be performed to ensure the access assigned was authorized, appropriate and applicable to the functions being performed. The details around these processes will be documented in the CHRS Security/Operational Guide.

In all other situations, all security strategies must be administered in such a way that campus employees are able to only access information needed to perform their job duties. All regulatory laws and CSU policies must be adhered to, including those specified in HR 2005-16 which states:

> The California State University (CSU) has a responsibility to protect sensitive personal data and maintain confidentiality of that data under the Information Practices Act (IPA) and Title 5. In light of rapidly changing technology and increased Internet use, this memorandum is written to highlight the importance of the CSU's responsibility. The Information Practices Act, California Civil Code §1798, et seq., requires

the Chancellor's Office and campuses to collect, use, maintain, and disseminate information relating to individuals in accordance with its provisions. Additionally, §42396 through §42396.5 of Title 5 of the California Code of Regulations address privacy and the principles of personnel information management. (Refer to Appendix)

The CSU also complies with the Family Educational Rights and Privacy Act (FERPA), which prohibits the release of education records without student permission (Refer to Appendix). Each campus is responsible for campus record-keeping and procedures relating to student and employee personal information. In addition, each campus is required to maintain appropriate access, disclosure, and confidentiality of student and employee personal information.

1. Each campus must ensure that all employees with access to confidential personal information have a legitimate CSU need to have such access. These employees must understand the responsibility they have under the Information Practices Act and Title 5 to protect sensitive personal data.

2. Confidential personal information should not be transmitted outside the CSU unless it is for legitimate CSU purposes. Recipients must be informed that the information provided is confidential and is provided for the sole purpose of the specific business need. Also, recipients must be informed that they are responsible for the protection of the information and the destruction of all files after the intended use is satisfied.

2.1 System Applications/Specific Processes

The following system application security requirements, in addition to the information outlined above, must be adhered to for CHRS. These operational security requirements apply to production and non-production CHRS database instances.

2.1.1 Employment information

Employee information must be secured at the campus and department levels and only accessible to employees based upon a "need-to-know" basis to perform their assigned job duties.

Employment information includes but is not limited to information identified as Level 1 and/or Level 2 data. Refer to the CHRS Data Classification section 2.1.8 below for specific details.

2.1.2 Campus Conversion Validation

The approach used for campus validation of converted data for CHRS must adhere to the security requirements outlined previously to ensure all data is secured by the campus. Access must be provided in a manner that enables campus designated employees to validate data at their respective campus by specific job function(s).

2.1.3 Development

CHRS development will be handled by the central CO staff. Campus-specific modifications to CHRS are not allowed. Therefore, campus development access will not be authorized, unless it is granted to support a specific CHRS project. Refer to Section 2.0 for additional details.

2.1.4 HR/CS Split

Oracle has advised that although the application is physically splitting, certain HR employment and pay information is necessary and must be kept in sync to support CS operational business needs, e.g. Work Study. The specific tables and values that will remain in sync will be defined by the CHRS Data Governance team. Nonetheless, each campus must secure their campus CS system to ensure that only CS menu options, pages and functions are available within CS. The campus must comply with the Systemwide HR policy (to be defined) to remove access to HR menu options, pages and functions as these are no longer applicable and will not be maintained. Quarterly audits will be governed by CO Security to ensure campus compliance; details of these audits and controls will be included in the CHRS Security Guide. (A delivered solution will be pursued with Oracle.)

2.1.5 Person Data[1] (Demographic) /Searches

HR Person Data may be viewed by campus employees on a "need-to-know" basis to perform their job. Certain Person Data elements may also be viewed to preclude duplicate records from being added to the system, e. g. Search Match functionality. Data available for online viewing and searches include information contained in the existing CSU ID Search Modification.

Search Criteria	• **Search Results**
• Name	• Name
• SSN (full)	• SSN – last 4 digits
• Employee ID/Record Number	• Empl ID/Record Number
	• Job Code and Description
	• HR Status (Active/Inactive)
	• Department ID and Description
	• Date of Birth (Month and Date)
	• Organization Relationship
	• Employee Class
	• POI Type
	• Business Unit

2.1.6 Person Data and CS

- HR Person Data **may** be shared between the campus HR and **respective CS** instance.
- HR Person Data **may not** be shared or used to update a **non-respective campus CS** instance.

Systemwide HR is the data owner of Person Data and a designated delegate will work with respective campus representative(s) to manage demographic related data discrepancies. Operational processes that govern how personal information will be updated within CHRS and the Higher Education Constituent Hub (HECH) will be defined by the CHRS Data Governance team.

[1] Refer to the data standards defined as part of the CHRS Systemwide HR Data Standardization project for a complete listing of Person Data elements (Phase I).

2.1.7 CHRS Non-Production Sensitive Data

Specific development functions must be performed in the CHRS non-production environments where data may not be fully secured by the campus. As part of the CHRS development/implementation efforts, campus employees may be given access to system-wide data to assist with specific project development. In these instances, sensitive data contained within the CHRS development (non-production environments) must be masked and/or scrambled to minimize the possibility that personally identifiable information cannot be associated with actual employees. To protect information in this category, the following data elements, at a minimum are considered sensitive and must be protected as noted above:

1. **Name**
2. **SSN – National ID**
3. **Date of Birth (DOB)**

2.1.8 CHRS Data Classification

The following data items are classified as Level 1 and 2 by Systemwide HR as they relate to an employee's CSU employment history and applicant record (name and qualifications, education, physical description-including photo, and background investigations) and thereby must be protected/secured (this information is typically stored in Oracle within multiple modules, e.g., Workforce Administration, Benefits Administration, Time & Labor/Payroll, Absence Management, etc.). Employees may be granted access to these data items only as it is relevant and necessary to perform their job duties.

- Level 1 Data Items:
    - Social Security Numbers (with name)
        - Taxpayer ID
        - National ID
    - International Identification (such as passport, visa-with name)
    - Date of Birth (with partial SSN and Name)
    - Benefits Records
    - Medical Information
    - Driver's License (with name)
    - Citizenship/Visa Status
    - Personal Telephone Numbers, Email Address
    - Address (Home and Mailing)
    - Race and Ethnicity
    - Family Member Names (Mother's Maiden Name)
    - Gender
    - Marital Status

- Level 2 Data Items:
    - Date of Birth (partial or full with name)
    - Employee Applicant Record
    - Net Salary
    - Time and Labor

- Payment Information
- Employee Evaluations
- Veteran Status
- Disability/Reasonable Accommodation
- Age (Date of Birth)

2.1.9 Oracle Reporting/Queries

Access to Oracle query and reporting capabilities will use delivered Oracle application security controls and row level security.

Oracle online reporting and query is the primary reporting tool for CHRS. Direct SQL access is not intended for reporting and is provided for technical support and integration purposes.

2.1.10 Database SQL Access

Access to the CHRS production database for technical support and service accounts, e.g. integration point, will be allowed using Oracle accounts. The default and standard CSU_SELECT role as outlined in the *Validating Oracle Users and Roles* document will not include any tables that contain employee related data. The CSU_UPDATE role will not exist within the CHRS environment.

- Only a limited number of campus based employees may be granted (direct database) access for their respective campus to view and/or query information containing sensitive data.
- Level 1 and 2 data will be segregated by campus using campus specific Oracle views/roles which must be requested via the modification governance process.
- A few predefined tables that include employee related data will be secured by campus and provided as a baseline.
- Access to the campus-specific Oracle views will be provided by way of campus specific Oracle roles.

2.1.11 Roles and Permissions

Security Roles and Permissions lists for CHRS will be defined and maintained by the CHRS Security Team. A system-wide set of security roles and permission lists will be defined to support the Systemwide HR approved job functions required to implement the CHRS business practices defined by Systemwide HR.

Campuses will have the ability to assign roles to users based upon their job function(s).

Campuses may submit a request to the Central Security office for an updated, or a new role/permission list to be defined to support a specific business need/function. The request will be reviewed by the CHRS Security Team, and approved by the Systemwide HR Data Steward for inclusion in CHRS.

3.0 CHRS Governance Structure

The CHRS governance structure defines the functions, relationships, responsibilities, and authorities of committees and individuals that support CHRS.

3.1 System-wide Roles and Responsibilities

3.1.1 Systemwide Human Resources

The data owner for CHRS will be the Associate Vice Chancellor of Human Resources Management and CO HR Services, Systemwide HR. The data delegate will be the Sr. Manager, CMS-Systemwide HR. The Vice Chancellor for Systemwide HR is primarily responsible for reviewing and approving the CHRS Security Plan and Requirements.

3.1.2 CHRS Data Governance

Updates made to an employee's Person Data record within CHRS may be permitted but will be governed by rules defined by the CHRS Data Governance Team. The system update rules will be applicable to CHRS, the HECH and other internal and/or external applications and integrations that rely on Person Data, e.g. HR/CS Split environment, Identity Management Systems etc.

3.1.3 CHRS Security Campus Action Team (CHRS Security CAT)

A review team, comprised of personnel from campuses and CMS Central, will be created to support CHRS information security requirements and initiatives. This team will be responsible for developing a set of roles and permission lists approved for CHRS for which security administrators will use to associate with campus based users. A security matrix that describes what access each end-user needs, based on the Systemwide HR Policies and requirements and security guidelines and delivered roles from CHRS Central team will be available to campuses. If campuses identify a needed change or new role or permission list, they will submit that request as described in the section on Roles and Permissions lists. The CHRS Security CAT will review the requests and recommend approval.

3.1.4 Central Security Administrator

The Central Security Administrator (CSA) will work with the CO, campus staff, and CHRS CAT, to validate the security design and provide post-implementation support. The CSA's duties include but are not limited to the following:

- Consultation with campus and CO staff to meet operational security needs.
- Consultation with the project team to ensure CHRS compliance with CSU System-wide Information Security Standards and Policies.
- Evaluation of user security requests and consultation with the CHRS Security CAT to ensure requests comply with CHRS security policies and audit guidelines.
- Providing support to campuses and CMS during audits.
- Initial creation of DSA User Accounts:
  - On-going responsibility will be performed by Central Security Maintenance rather than Administration.

- Monthly, quarterly, and annual review of CHRS security to ensure compliance with SoD policies.

3.1.5 CMS Technical Services and Application Development Team

CMS Technical Services will manage the production infrastructure associated with the application and web tiers, supporting the CHRS environment with direction from the Central Security Administrator. This includes all tasks associated with application server setup, configuration and management, process scheduler setup, configuration and management, and web server setup configuration and management. CMS Technical Services is responsible for ensuring appropriate resources at the web and application tier and include responsibilities for capacity planning, tuning, and installation.

CMS Technical Services along with CMS Application Development Teams will support the campus non-production environments as this now requires central security control and coordination.

3.2 Campus Roles and Responsibilities

3.2.1 Distributed Security Administrators

To highlight the shared responsibilities of CHRS, campus security administrators will be referred to as Distributed Security Administrators (DSA's). The DSA's will be managed using Oracle's delivered Distributed User Profiles functionality. They will be given the capability of assigning roles restricted to those in their Role Grant domain. DSA's will provide security support for operational activities at the campus within the limitations of the access provided to them. Other duties of the DSA's include but are not limited to the following:

- Evaluate and act upon user access requests for their respective campuses.
- Establish and maintain user profiles in CHRS for their respective campuses.
- Process user requests by assigning privileges to user accounts based on approval from Campus Application Owners.
- Maintain documentation related to users requests for their respective campus.
- Accept and review user requests to access non-campus based security objects. Such requests are forwarded to the Central Security Administrator based on approval from Campus Application Owner.
- Participate in audits of user accounts in accordance with CSU Information Security Policies.
- De-provision accounts when the user has separated from the university by locking them.
- Limited (Security Maintenance only) monthly, quarterly and annual reviews of SoD reports for compliance.

DSA's and their backups can grant any level of access or responsibility within the roles granted to them for the CHRS Oracle Application. This responsibility includes delegating limited administrative capabilities to Application Leads. This special role provides the ability to administer the rights to any menu, component, page or tool within CHRS, again delineated by the role granted through the Role Grant functionality, and therefore should be deployed sparingly.

4.0 CHRS Security Training

Efforts are underway to develop a system-wide campus CHRS implementation support program that will include training for the CHRS security model.

CMS expects campuses to take the requisite security awareness and training. CHRS will require existing security experience and reinforce security awareness as part of the implementation support program, as outlined in CSU System-wide Information Security Policy.

5.0 Authentication and Access Control

CHRS will implement a custom authentication process. CHRS Oracle system will be front-ended by a combination of the CSYou Employee Portal and Shibboleth for general authentication. Users that are successfully logged into CSYou or other system-wide authentication services will be able to access resources based on their roles that are defined and granted within CHRS.

The following approach provides an example of this model:

1. A user attempts to access the main page of CSYou.
2. The user is redirected to their local campus Identity Provider (IAM infrastructure) to enter their campus managed credentials.
3. Once authenticated, the user will be redirected back to CSYou where they will find a link to access CHRS.
4. This link executes custom code that works in conjunction with the Oracle Sign-In Code.
5. If the user has been provided access, they will now be able to perform any functions granted to them through the roles that have been assigned to them.

5.1 Password Management

Oracle Password Management feature will NOT be used in CHRS. Since campuses are responsible for managing their campus user's password policy they are encouraged to require strong passwords and follow the password management guidelines in the California State University System-wide Information Security Standard**.**

Significant changes that are to be implemented in the shared CHRS will be appropriately reviewed and approved by the CHRS Security CAT. Significant changes made to the CHRS Security model will be appropriately reviewed and approved by the designated change control authority.

Any approved changes will be migrated into CHRS production per the CHRS Release Management Guide. This documents the migration process and describes the delineation of responsibilities in compliance with SoD policies.

6.0 CHRS Security Incident Management

CHRS will comply with the Information Security Incident Management Polices as defined in the California State University System-wide Information Security Policy.

7.0 CHRS Business Continuity and Disaster Recovery

Campus and CO users and administrators access the CHRS at the Unisys data center. Disaster recovery for all of CMS, including the CHRS, is managed and coordinated within the purview of the Unisys data center contract.

8.0 CHRS Infrastructure

This section describes differences to the CMS security infrastructure made to support the CHRS application environment. All current CMS security practices, policies and procedures will be in place for CHRS. This includes all current security components such as VPN, IDS, and Firewalls that are in place for the CMS environment. This section covers only areas where CHRS is different from current CMS HRSA environments.

8.1 Oracle Database User Accounts Password Management

The oracle account's password controls will comply with CSU Policy 8050.0 Access Control and Standard 8060.S01 Access Control.

9.0 Appendix

California State University. (2012, June 5). *Access Control 8060.S01* Retrieved August 18, 2013, from http://www.calstate.edu/icsuam/sections/8000/8060-Access_Control_Standard.pdf

California State University. (2010, April 19). *Configuration Management Policy 8050.0.* Retrieved 08 19, 2013, from ICSUAM CSU Policy: http://www.calstate.edu/icsuam/sections/8000/8050.0.shtml

California State University. (2011, June 22). *HIPPA Regulations as Amended by the HITECH Act- Update of Privacy and Security* . Retrieved 2013, from CSU Human Resources Management: http://www.calstate.edu/HrAdm/pdf2011/HR2011-07.pdf

California State University. (2010, April 19). *Information Asset Management Policy 8065.0.* Retrieved 08 19, 2013, from ICSUAM CSU Policy: http://www.calstate.edu/icsuam/sections/8000/8065.0.shtml

California State University. (2011, September 23). *Information Security Data Classification 8065.S02.* Retrieved August 18, 2013, from http://www.calstate.edu/icsuam/sections/8000/8065_FINAL_DRAFT_Data_Classification_CW_V4.pdf

California State University. (2005, April 8). *Requirements for Protecting Confidential Personal Data: Updated to Include Information Practices Act Web Site and Security Breach.* Retrieved August 18, 2013, from CSU Human Resources Management: http://www.calstate.edu/HrAdm/pdf2005/HR2005-16.pdf

US Department of Education. (n.d.). *Family Rights and Privacy Act (FERPA).* Retrieved August 18, 2013, from US Department of Education: http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html