Sacramento State User Access Review Procedure for Level 1 Systems

1.0 Background

ICSUAM Information Security Policy on Access Control requires an access review be conducted at least annually for information assets (systems/applications) containing protected data. The results of the review must be documented.

The following procedure is intended to comply with this CSU Access Control Policy.

2.0 Scope

All systems that contain protected university information assets classified as level 1/confidential/Personally Identifiable Information (PII). This includes all campus and auxiliaries cloud services, workstations, applications, servers, databases, etc., Sacramento State's Common Management Systems and OnBase imaging and workflow follow a separate process.

Administrative access includes any access assigned to users that are in addition to any self-service type of access. The responsible administrator conducting the review must not have Account Administrator permissions. See below for the types of roles and responsibility that may be assigned for users with administrative access.

Role	Responsibility
Account Holder	The individual or group which is assigned the Account. This could be a privileged or general account.
Privileged Account	An account that may have administration access to configure setup, security administration, interface configurations, development(coding), daily batch jobs, data extract, etc.,
Security Administrator	Those who support Accounts by adding, modifying, assigning passwords, or other account management actions.
System/Service Administrators	Those who are members of organizational units that support enterprise, division, or department level IT services. System/Service administrators within their area of responsibility facilitate end-user privilege management and implement operating procedures to conform to campus information security standards and guidelines.
System/Service Owner	The system owner is ultimately responsible for providing the system's service/functionality to the campus. Often the system owner is a manager/director, department chair, or dean.
Data Owner	The data owner is responsible for establishing procedures for granting and revoking access privileges. https://www.csus.edu/information-resources-technology/it-governance/data-security-governance.html

Reference - Sacramento State Data Classification Standard -
https://www.csus.edu/information-resources-technology/information-security/_internal/_documents/sac-data-classification-and-protection-standards-sacramento.pdf

3.0 Procedure

The steps below outline the procedure/process to coordinate the review from initial reports generation to the final step of certifying the overall process.

	Step	Responsible Staff	Task Details
3.1	Create list of roles/template	Security Administrator and/or system/service administrator	Create a list of roles and/or templates that are used to control access to the system/service.Example: administrative roles, user roles, privileged access roles. Role: a standard template created and assigned to user(s) based on operational need
3.2	Create access report	Security Administrator and/or system/service administrator	Generate a report of active users and the roles assigned for each user. Note: standard useraccounts that have access to their own data do not need to be included in the report.
3.3	Audit access report	Security Administrator and/or system/service administrator	Conduct a comprehensive review of the list of users and roles at a minimum: 1) Is this an active employee? 2) Has their job or responsibilities changed? 3) Do they have appropriate access (least privilege)? 4) Is the employee current with Data Security & Privacy Training? 5) Is this a shared account (i.e. does more than one person know the password)?
3.4	Mark action needed	Security Administrator and/or system/service administrator	Mark any users and/or privileged roles/templates that may need to be removed or changed inthe access report. Example: create an additional column for notes in the access report.
3.5	Review/Approve	System/Service Owner	Document the access review activity using the template provided in Adobe Sign. Route it forreview/signature to the Data Owner. It is the responsibility of the responsible administrator (MPP) to certify the access review. Include an appendix for additional descriptions and/or information that may not fit in thetemplate
3.6	Submit	Automatically done by Adobe Sign	Submit the completed review to the Information Security Office

4.0 Activity Timeline

The Information Security Office will use the application inventory database to identify all level 1 systems and assigned System Owners to coordinate the review, annually at a minimum.

Task	Timeline	Owner
1. Coordinate/setup check ins with System Owners in early October 2. Conduct workshop sessions to provide an overview of the access review process 3. Notify Systems Owners, Data Owners, Vice Presidents and Deans	October	Information Security Office, Data Owners
4. Work with the System Owners to document the access review template using the template in section 5.0 and route for approvals through Adobe Sign	November – December	Information Security Office
5. Review completed access review reports for accuracy 6. Inventory and update application inventory database to note date of review	January	Information Security Office
7. Summarize the review process and present to Data Owners for review/approval		
8. Present summary reports for review to Information Security Officer/Chief Information Officer 9. Certify the annual access review process with the Vice President/Chief Information Officer in February	February	Information Security Office

5.0 Access Review Template

ANNUAL ACCESS REVIEW FOR LEVEL 1 SYSTEMS

To: Information Security Office

In accordance with System wide Information Security Policy on Access Control 8060.0 and Sacramento State Level 1 Systems Access Review procedures, I/we have conducted a review of the level 1 systems that are under my purview.

Division Name	
System Owner	
Department Name	
Certification Date	
Review Dates	From:mm/dd/yyyy To mm/dd/yyyy
Service Description	

User (Name)	Title	Department	System Role	Description	Status
John Smith1	ITC	SA IT	Super User	Manage batch process, administer role templates	Approved
John Smith1	Analyst	SA IT	Super User	Manage batch process, administer role templates	Delete

Review Conducted By:_____ Date:

Responsible Administrator (MPP) Certification:_____Date:

Sacramento State User Access Review Procedure for Level 1 Systems

Review/Approval History

Review Date	Reviewed By	Action(Reviewed, Recommended or Approved)
12/8/2021	Document created	ISO Team
12/14/2021	ISO Team, VP/CIO	Reviewed
01/18/2022	ISO Team	Reviewed, Updated Section 2.0
02/03/2022	ISO Team	Reviewed, Updated Section 3.0, Template
02/10/2022	ISO Team	Reviewed, Updated Section 4.0
02/11/2022	ISO Team	Reviewed, Updated Section 4.0
02/15/2022	IT Advisory Board	Reviewed
03/09/2022	Data Owners Group	Reviewed/Approved