# Reusable Component Library System Security Plan

# NIST SP 800-53 Revision 4 Privacy

## AR: Accountability, Audit, and Risk Management

### AR-1: GOVERNANCE AND PRIVACY PROGRAM

"The organization:  
 a. Appoints a Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer  
 (CPO) accountable for developing, implementing, and maintaining an organization-wide  
 governance and privacy program to ensure compliance with all applicable  
laws and  
 regulations regarding the collection, use, maintenance, sharing, and disposal  
 of personally identifiable information (PII) by programs and information  
systems;  
 b. Monitors federal privacy laws and policy for changes that affect the privacy  
 program;  
 c. Allocates [Assignment: organization-defined allocation of budget and staffing]  
 sufficient resources to implement and operate the organization-wide privacy  
program;  
 d. Develops a strategic organizational privacy plan for implementing applicable  
 privacy controls, policies, and procedures;  
 e. Develops, disseminates, and implements operational privacy policies and  
 procedures that govern the appropriate privacy and security controls for  
programs,  
 information systems, or technologies involving PII; and  
 f. Updates privacy plan, policies, and procedures [Assignment: organization-defined  
 frequency, at least biennially]."

##### Privacy

Project does not collect or maintain PII and therefore does not directly address this control though it may address it indirectly.

### AR-2: PRIVACY IMPACT AND RISK ASSESSMENT

"The organization:  
 a. Documents and implements a privacy risk management process that assesses  
privacy risk to  
 individuals resulting from the collection, sharing, storing, transmitting,  
use, and disposal of  
 personally identifiable information (PII); and  
 b. Conducts Privacy Impact Assessments (PIAs) for information systems,  
programs, or other  
 activities that pose a privacy risk in accordance with applicable law,  
OMB policy, or any  
 existing organizational policies and procedures."

##### Privacy

Project does not collect or maintain PII and therefore does not directly address this control though it may address it indirectly.

### AR-3: PRIVACY REQUIREMENTS FOR CONTRACTORS AND SERVICE PROVIDERS

"The organization:  
 a. Establishes privacy roles, responsibilities, and access requirements for contractors and service  
 providers; and  
 b. Includes privacy requirements in contracts and other acquisition-related documents."

##### Privacy

Project does not collect or maintain PII and therefore does not directly address this control though it may address it indirectly.

### AR-4: PRIVACY MONITORING AND AUDITING

"The organization monitors and audits privacy controls and internal privacy policy  
 [Assignment: organization-defined frequency] to ensure effective implementation."

##### Privacy

Project does not collect or maintain PII and therefore does not directly address this control though it may address it indirectly.

### AR-5: PRIVACY AWARENESS AND TRAINING

"The organization:  
 a. Develops, implements, and updates a comprehensive training and awareness  
strategy aimed at  
 ensuring that personnel understand privacy responsibilities and procedures;  
 b. Administers basic privacy training [Assignment: organization-defined  
frequency, at least  
 annually] and targeted, role-based privacy training for personnel having  
responsibility for  
 personally identifiable information (PII) or for activities that involve  
PII [Assignment:  
 organization-defined frequency, at least annually]; and  
 c. Ensures that personnel certify (manually or electronically) acceptance  
of responsibilities for  
 privacy requirements [Assignment: organization-defined frequency, at  
least annually]."

##### Privacy

Project does not collect or maintain PII and therefore does not directly address this control though it may address it indirectly.

### AR-6: PRIVACY REPORTING

The organization develops, disseminates, and updates reports to the Office of  
 Management and Budget (OMB), Congress, and other oversight bodies, as appropriate,  
to  
 demonstrate accountability with specific statutory and regulatory privacy  
program mandates, and  
 to senior management and other personnel with responsibility for monitoring  
privacy program  
 progress and compliance."

##### Privacy

Project does not collect or maintain PII and therefore does not directly address this control though it may address it indirectly.

### AR-7: PRIVACY-ENHANCED SYSTEM DESIGN AND DEVELOPMENT

Control:The organization designs information systems to support privacy by automating privacy controls.

##### Privacy

Project does not collect or maintain PII and therefore does not directly address this control though it may address it indirectly.

### AR-8: ACCOUNTING OF DISCLOSURES

"The organization:  
 a. Keeps an accurate accounting of disclosures of information held in each  
system of records  
 under its control, including:  
 (1) Date, nature, and purpose of each disclosure of a record; and  
 (2) Name and address of the person or agency to which the disclosure  
was made;  
 b. Retains the accounting of disclosures for the life of the record or  
five years after the  
 disclosure is made, whichever is longer; and  
 c. Makes the accounting of disclosures available to the person named in  
the record upon request."

##### Privacy

Project does not collect or maintain PII and therefore does not directly address this control though it may address it indirectly.