# Reusable Component Library System Security Plan

# NIST SP 800-53 Revision 4 Privacy

## DM: Data Minimization and Retention

### DM-1: MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION

“The organization: a. Identifies the minimum personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection; b. Limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent; and c. Conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings [Assignment: organization-defined frequency, at least annually] to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.”

##### Privacy

Example Org does not collect or maintain PII and therefore does not directly address this control though it may address it indirectly. The data collected (email address, first and last name) is demonstrably a minimum.

### DM-2: DATA RETENTION AND DISPOSAL

“The organization: a. Retains each collection of personally identifiable information (PII) for [Assignment: organization-defined time period] to fulfill the purpose(s) identified in the notice or as required by law; b. Disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and c. Uses [Assignment: organization-defined techniques or methods] to ensure secure deletion or destruction of PII (including originals, copies, and archived records).”

##### Privacy

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

### DM-3: MINIMIZATION OF PII USED IN TESTING, TRAINING, AND RESEARCH

“The organization: a. Develops policies and procedures that minimize the use of personally identifiable information (PII) for testing, training, and research; and b. Implements controls to protect PII used for testing, training, and research.”

##### Privacy

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