# Reusable Component Library System Security Plan

# NIST SP 800-53 Revision 4 Privacy

## TR: Transparency

### TR-1: PRIVACY NOTICE

“The organization: a. Provides effective notice to the public and to individuals regarding: (i) its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information (PII); (ii) authority for collecting PII; (iii) the choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and (iv) the ability to access and have PII amended or corrected if necessary; b. Describes: (i) the PII the organization collects and the purpose(s) for which it collects that information; (ii) how the organization uses PII internally; (iii) whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing; (iv) whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; (v) how individuals may obtain access to PII; and (vi) how the PII will be protected; and c. Revises its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change.”

##### Privacy

Example Org publishes a privacy policy in the footer of every page. Further, upon login, the user must accept a detailed Terms and Conditions of Use.

### TR-2: SYSTEM OF RECORDS NOTICES AND PRIVACY ACT STATEMENTS

“The organization: a. Publishes System of Records Notices (SORNs) in the Federal Register, subject to required oversight processes, for systems containing personally identifiable information (PII); b. Keeps SORNs current; and c. Includes Privacy Act Statements on its forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected.”

##### Privacy

Example Org does not collect or maintain PII and therefore does not publish a SORN.

### TR-3: DISSEMINATION OF PRIVACY PROGRAM INFORMATION

“The organization: a. Ensures that the public has access to information about its privacy activities and is able to communicate with its Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO); and b. Ensures that its privacy practices are publicly available through organizational websites or otherwise.”

##### Privacy

Example Org publishes a privacy policy in the footer of every page. Further, upon login, the user must accept a detailed Terms and Conditions of Use.