

# Manage Security and Privacy through Reusable Processes

Our digital services have to protect sensitive information and keep systems secure. This is typically a process of continuous review and improvement which should be built into the development and maintenance of the service. At the start of designing a new service or feature, the team lead should engage the appropriate privacy, security, and legal officer(s) to discuss the type of information collected, how it should be secured, how long it is kept, and how it may be used and shared. The sustained engagement of a privacy specialist helps ensure that personal data is properly managed. In addition, a key process to building a secure service is comprehensively testing and certifying the components in each layer of the technology stack for security vulnerabilities, and then to re-use these same pre-certified components for multiple services.

The following checklist provides a starting point, but teams should work closely with their privacy specialist and security engineer to meet the needs of the specific service.

## Key Questions

1. Does the service collect personal information from the user? How is the user notified of this collection?
2. Does it collect more information than necessary? Could the data be used in ways an average user wouldn't expect?
3. How does a user access, correct, delete, or remove personal information?
4. Will any of the personal information stored in the system be shared with other services, people, or partners?
5. How and how often is the service tested for security vulnerabilities?
6. How can someone from the public report a security issue?

## Checklist

Contact the appropriate privacy or legal officer of the department or agency to determine whether a System of Records Notice (SORN), Privacy Impact Assessment, or other review should be conducted

Determine, in consultation with a records officer, what data is collected and why, how it is used or shared, how it is stored and secured, and how long it is kept

Determine, in consultation with a privacy specialist, whether and how users are notified about how personal information is collected and used, including whether a privacy policy is needed and where it should appear, and how users will be notified in the event of a security breach

Consider whether the user should be able to access, delete, or remove their information from the service

“Pre-certify” the hosting infrastructure used for the project using FedRAMP

Use deployment scripts to ensure configuration of production environment remains consistent and controllable

---

Revision #1

Created 26 February 2024 16:20:56 by Tom O'Malley

Updated 26 February 2024 16:21:34 by Tom O'Malley