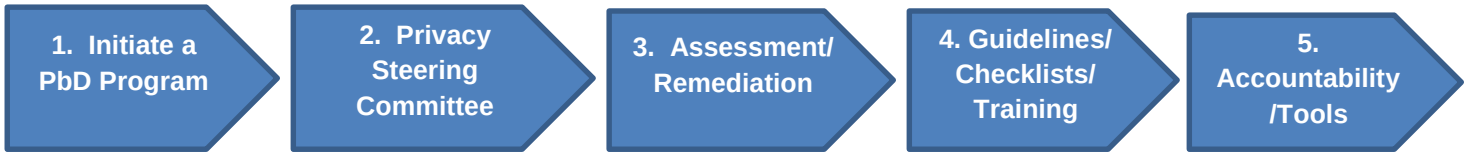
Job Aid

Integrating Pbd With Rim - A Reference Guide

'Privacy' is often defined as the ability of individuals to exercise control over the disclosure and subsequent use of their personal information. "Privacy by Design" is an approach to protecting privacy by embedding it into the design of products, services and business practices. That means building in privacy right up front – right into the design of new systems and processes.

Five Steps for Integrating to Privacy by Design with a Corporate Records Program



1. Initiate a PdD program
   - ☐ Team with the Chief Privacy Officer
   - ☐ If in a regulated sector (e.g. health, finance, government)
     - Privacy controls are mandated by law
   - ☐ If in a non-regulated sector, look for:
     - Privacy incident in a peer organization (or your own)
     - Privacy evangelist
     - Board or C-Level sponsor
   - ☐ Include RIM in the privacy gap analysis

2. Privacy Steering Committee
   - ☐ Include the Records Manager part of the Privacy Steering Committee
   - ☐ Identify roles and responsibilities for Privacy Coordinators and Records Managers
   - ☐ Privacy Training (possible IAPP Certification Training)[1] for the committee members
   - ☐ Formalize the relationship between the Privacy and RIM functions

3. Assessment/Remediation
   - ☐ Merge assessment activities where possible
     - E.g. Merge privacy and records assessments of systems and vendor practices
   - ☐ Update retention schedule to include a privacy classification

4. Guidelines/Checklists/Training
   - ☐ Build alliances with IT, Information Security, Audit, Legal – and include records retention in their checklists
   - ☐ Ensure that RIM is built into every phase of the Systems Development Lifecycle (SDLC)
   - ☐ Cross-reference/integrate records retention in corporate privacy training
   - ☐ Cross-reference/integrate privacy requirements in corporate records retention training

[1] International Institute for Privacy Professionals (IAPP) – http://www.privacyassociation.org

5. Accountability/Tools
   - During Annual Review include review of privacy requirements in retention schedule
   - Verify that any database containing personal information is managed per the retention schedule
   - Work with IT to ensure that expired content with personal information can be disposed without affecting database integrity

Privacy by Design – Seven Elements of Design[2]

The following principles of Privacy by Design (*PbD*) are considered best practice in the development of any type of system containing personal information and can be incorporated into the five steps to *PbD* above. *PbD* extends to (1) IT systems, (2) accountable business practice and (3) physical design and networked infrastructure. Its objectives are to ensure privacy and gaining personal control over an organization's information.

1. ***Proactive*** not Reactive; ***Preventative*** not Remedial
   Aim to prevent privacy invasive events; comes before the fact, not after

2. Privacy as the ***Default Setting***
   Ensure that all personal information (PI) is automatically protected in any given IT system or business practice.

3. Privacy ***Embedded*** into Design
   Design the handling of privacy in the design and architecture of IT systems and business practices; not "bolted-on" after the fact

4. Full Functionality – ***Positive-Sum***, not Zero-Sum
   Accommodate all legitimate interests and objectives in a "win-win" manner

5. End-to-End Security – ***Full Lifecycle Protection***
   Strong security measures are implemented end-to-end, for the data or records throughout the information lifecycle. Ensure that data is securely retained, and securely destroyed at the end of the process, in a timely fashion (per the retention / disposition schedule)

6. ***Visibility*** and ***Transparency*** – Keep it ***Open***
   Assure all stakeholders that the business practices and technology are operating according to stated promises and objectives, subject to independent verification. Trust but verify.

7. ***Respect*** for User Privacy – Keep it ***User-Centric***
   Keep the interests of the individual uppermost in mind by offering such measures as strong privacy defaults, appropriate notice and user-friendly options.

[2] http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf - Developed by Anne Cavoukian, PhD, Information & Privacy Commissioner, Ontario, Canada