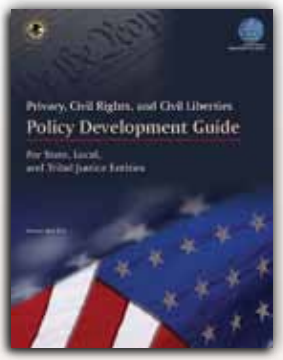
7 Steps to a Privacy, Civil Rights, and Civil Liberties Policy



Ethical and legal obligations compel professionals in the justice system, when sharing information, to protect privacy, civil rights, and civil liberties interests. The U.S. Department of Justice's Global Justice Information Sharing Initiative's (Global) *Privacy, Civil Rights, and Civil Liberties Policy Development Guide for State, Local, and Tribal Justice Entities* (or "Privacy Guide") is a practical resource that supports privacy protection requirements for physical and automated information sharing environments. Its purpose is to guide privacy policy development while supporting information sharing.

The following seven steps highlight the privacy policy development process, as recommended in the Privacy Guide, including preparation, drafting, and implementation. Privacy Guide section references are also included along with each step. The Privacy Guide is available at www.it.ojp.gov/privacy.

Step 1. Understanding Foundational Concepts (Section 4)

- Become familiar with applicable terms: privacy, civil rights, civil liberties, information quality, and security
- Learn how privacy issues arise and the purpose of a privacy policy

Step 2. Assembling the Project Team (Section 5)

- Designate the project champion or sponsor
- Secure support and justify resources
- Appoint the project team leader
- Build the project team and stakeholders
- Identify the roles within the entity (e.g., privacy and security officers)

Step 3. Establishing a Charter (Section 6)

- Draft components:
  - Vision, mission, and values statements
  - Goals and objectives for the creation of the privacy policy
- Write the charter

Step 4. Understanding Information Exchanges (Section 7)

- Identify information exchanges—what information is collected, used, maintained, and shared
- Examine privacy risks by performing a Privacy Impact Assessment

Step 5. Performing the Legal Analysis (Section 8)

- Identify legal authorities applicable to the entity's privacy protection efforts
- Address legal and technological gaps in the privacy policy

Step 6. Writing the Privacy Policy (Section 9 and Appendix C)

- Develop an outline and draft policy language to meet core privacy policy concepts. Include legal references identified in Step 5
- Perform a policy review to determine whether the draft policy adequately addresses current privacy standards and protection recommendations

Step 7. Implementing the Privacy Policy (Section 10)

- Obtain formal adoption of the policy
- Make the policy available to decision makers, practitioners, and the public
- Train personnel and authorized users
- Specify methods for auditing and compliance monitoring
- Incorporate revisions and updates identified through the monitoring process

Global Justice Information Sharing Initiative

United States Department of Justice

www.it.ojp.gov/privacy

Core Concepts Recommended in a Privacy Policy

The following core concepts should be addressed in a privacy policy, as recommended by the *Privacy, Civil Rights, and Civil Liberties Policy Development Template for State, Local, and Tribal Justice Entities* (or "SLT Policy Development Template"). These are discussed further in Section 9 of the Privacy Guide and in the Template located in Appendix C. Template sections are referenced along with each concept. The SLT Policy Development Template is available at www.it.ojp.gov/privacy.

Section A. Purpose Statement—What is the purpose of the privacy policy? Articulate the importance of privacy in the agency's integrated justice environment, and explain what the policy will accomplish.

Section B. Policy Applicability and Legal Compliance—To whom does the policy apply and under what authority does the entity operate? Articulate what laws, statutes, and regulations apply to the entity's conduct and to its operating policies.

Section C. Governance and Oversight—Who is responsible for oversight, development, implementation, and enforcement of the policy? Identify those charged with these tasks and their responsibilities.

Section D. Definitions—What key words or phrases are regularly used in the policy? Define terms that are not commonly known or have multiple meanings.

Section E. Information—What information does the policy apply to and how is it handled? Identify information that may or may not be sought, retained, shared, or disclosed and the processes for labeling and categorizing the information, including limitations of its use.

Section F. Acquiring and Receiving Information—What are the policies that require that information be obtained legally? State the agency's position that information acquired or received must comply with applicable law.

Section G. Information Quality Assurance—How is information quality addressed? State the process for ensuring the quality of collected, maintained, and disseminated information.

Section H. Collation and Analysis—What are the parameters for collation and analysis? State who is authorized, what information is analyzed, and for what purpose.

Section I. Merging Records—What are the parameters for merging records? State who is authorized, the criteria for merging, and the policy for partial matches.

Section J. Sharing and Dissemination—What are the conditions for sharing information inside and outside the agency? Identify levels of access, credentials, policies, and the public records process.

Section K. Redress—What is the process for disclosure and correction of information? State the conditions for disclosure to individuals and the procedures for corrections, appeals, and complaints.

Section L. Security Safeguards—How is information kept secure? Specify the administrative, technical, and physical mechanisms to secure information and breach notification procedures.

Section M. Information Retention and Destruction—How long is information retained? State the retention period and procedures for the review, purge, and destruction of information.

Section N. Accountability and Enforcement—How do you ensure transparency, accountability, and enforcement? Specify how the policy is provided to the public, the schedule for policy updates, the point of contact for inquiries and complaints, the process for reporting violations and evaluating compliance, and sanctions for noncompliance.

Section O. Training—What are the training requirements for the privacy policy? State who is required to receive privacy policy training and what is covered by the training.

rev. 9/6/11

BJA Bureau of Justice Assistance U.S. Department of Justice

This project was supported by Grant No. 2009-DB-BX-K105 awarded by the Bureau of Justice Assistance, Office of Justice Programs, in collaboration with the U.S. Department of Justice's Global Justice Information Sharing Initiative. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the U.S. Department of Justice.