Police Foundation

Sample Privacy Impact Assessment Matrix[1]

Template Section	PIA Questions	Suggested Respondent (s)	Answer (Yes/No/In-complete or N/A)	Assessment of Risk	Corrective Action/Re-mediation/ Location
A. Purpose Specification	1. Is there a written mission statement for the entity?	Entity Administrator			
	2. Is there a written purpose statement for collecting personally identifiable information (PII)? Include all types.	Entity Administrator/Data Privacy Officer/Legal Counsel			
	3. Does the entity's mission statement support the purpose for collecting PII?	Entity Administrator/Data Privacy Officer/Legal Counsel			
B. Policy Applicability and Legal Compliance	1. Does the entity have legal authority for collecting, creating, storing, accessing, receiving, and sharing or viewing data? If so, include citation(s), if applicable.	System Administrator OR Data Privacy Officer/Legal Counsel			
	2. Will all individuals with physical or logical access to the entity information be subject to the privacy policy?	System Administrator OR Data Privacy Officer/Legal Counsel			

[1] *Source of matrix: The Global Justice Information Sharing Initiative (2012). Guide to Conducting Privacy Impact Assessments for State, Local, and Tribal Justice Entities. Washington DC: U.S. Department of Justice, Bureau of Justice Assistance. The Police Foundation recreated the matrix in a fillable format for easy use. All credit is reserved for BJA and the Global Justice Information Sharing Initiative.*

	3. How does the entity plan to provide the privacy policy to personnel, participating users, and individual users (for example, in print, online)?	System Administrator			
	4. Will the entity require all individuals with physical or logical access to acknowledge receipt of the policy and agree to comply with the policy? (In writing or online?)	System Administrator			
	5. Will the entity require that individuals with physical or logical access and information-originating and user agencies be in compliance with all applicable constitutional and statutory laws protecting privacy, civil rights, and civil liberties in the gathering and collection, use, analysis, retention, destruction, sharing, disclosure, and dissemination or information? Note: These laws, statutes, and regulations will be cited in the privacy policy.	System Administrator OR Data Privacy Officer/Legal Counsel			
	6. Is a privacy notice required by law before data is collected, where appropriate (usually limited to health records)?	System Administrator OR Data Privacy Officer/Legal Counsel			
C. Governance and Oversight	1. Is primary responsibility for the entity's overall operation – including the information systems, information collection and retention procedures, coordination of personnel, and enforcement of the privacy policy – assigned to one or more individuals?	System Administrator OR Data Privacy Officer/Legal Counsel			
	2. Will the entity designate and train a privacy officer to handle reported errors and violations and oversee that implementation of privacy protections?	System Administrator			
	3. Will the entity assign responsibility for ensuring that enforcement procedures and sanctions for noncompliance with the privacy policy are adequate and enforced?	Entity Administrator			

D. Information	1. Has the entity identified the information it will seek, collect, retain, share, disclose, or disseminate?	System Administrator OR Data Privacy Officer/Legal Counsel			
	2. Does the entity apply labels to information based on legal or policy restrictions or information sensitivity to indicate to authorized users how to handle the information?	Entity Administrator OR Data Privacy Officer/Legal Counsel OR Technical Systems Security Staff			
	3. Does the entity categorize information based on its type (for example, tips and leads, suspicious activity reports, criminal history, intelligence information, case records, conditions of supervision, case progress), usability, and quality?	Entity Administrator OR Data Privacy Officer/Legal Counsel OR Technical Systems Security Staff			
	4. Does the entity require certain basic descriptive information to be associated with each record, data set, or system of records containing PII (for example, source, originating entity, collection date, and contact information)?	System Administrator OR Data Privacy Officer/Legal Counsel OR Technical Systems Security Staff			
	5. Is personal information obtained with the knowledge or consent of the data subject, if appropriate?	System Administrator			
E. Acquiring and Receiving Information	1. Are there applicable state and federal constitutional provisions and statutes that govern or specify the techniques and methods the entity may employ when seeking and receiving information? Note: These laws, statutes, and regulations will be cited in the privacy policy.	System Administrator OR Data Privacy Officer/Legal Counsel			
	2. Does the entity (if operational, conducting investigations) adhere to a policy regarding the investigative techniques to be followed when acquiring information (for example, an intrusion-level statement)?	System Administrator OR Data Privacy Officer/Legal Counsel			

	3. Do agencies that access your entity's information and/or share information with your entity ensure that they will adhere to applicable law and policy?	System Administrator OR Data Privacy Officer/Legal Counsel			
	4. Does the entity contract with commercial databases and, if so, does the entity ensure that the commercial database entity is in legal compliance in its information-gathering techniques?	System Administrator OR Data Privacy Officer/Legal Counsel			
F. Information Quality Assurance	1. Has the entity established procedures and processes to ensure the quality (for example, accurate, complete, current, verifiable, and reliable) of the information it collects and maintains, including procedures for responding to alleged or suspected errors or deficiencies (for example, correction or destruction)?	System Administrator OR Data Privacy Officer/Legal Counsel			
	2. Does the entity apply labels (or ensure that the originating agency has applied labels) to the information regarding its level of quality (for example, accurate, complete, current, verifiable, and reliable)?	System Administrator OR Data Privacy Officer/Legal Counsel OR Technical Systems Security Staff			
	3. Does the entity review the quality of information it originates to identify data that may be inaccurate or incomplete?	System Administrator OR Data Privacy Officer/Legal Counsel			
	4. When information that is received from or provided to another agency is determined to be inaccurate or incomplete, does the entity notify the originating or recipient agency?	System Administrator OR Data Privacy Officer/Legal Counsel			
G. Collation and Analysis	1. Is there a policy stating the purpose for which information is analyzed and specifying who is authorized (position/title, credentials, etc.) to analyze information?	System Administrator OR Data Privacy Officer/Legal Counsel			
	2. Has the entity defined what information can be analyzed?	System Administrator OR Data Privacy Officer/Legal Counsel			

H. Merging Records	1. Does the entity identify who is authorized (position/title, credentials, clearance level[s], etc.) to merge records?	System Administrator OR Data Privacy Officer/Legal Counsel OR Technical Systems Security Staff			
	2. Does the entity define matching criteria for merging information from multiple records allegedly about the same individual (e.g., sufficient identifying information beyond "name")?	System Administrator OR Data Privacy Officer/Legal Counsel OR Technical Systems Security Staff			
	3. If the criteria specified above are not met, does the entity have a procedure for partial matches? Note: If the agency or exchange does not merge records that have partial matches, the policy should state this.	System Administrator OR Data Privacy Officer/Legal Counsel OR Technical Systems Security Staff			
I. Sharing and Disclosure	1. Does the entity assign credentialed role-based levels of access for authorized users (for example, class of access and permission to view, add, change, delete, or print)?	System Administrator OR Data Privacy Officer/Legal Counsel OR Technical Systems Security Staff			
	2. Has the entity defined the conditions and credentials for access to and disclosure of records within the entity or in other governmental entities (for example, for law enforcement, public protection, public prosecution, public health or justice purposes)?	System Administrator OR Data Privacy Officer/Legal Counsel OR Technical Systems Security Staff			
	3. Are participating agencies that access information from your entity required to obtain approval from the originator of the information prior to further dissemination or to follow the disclosure laws applicable to the originating agency?	System Administrator OR Data Privacy Officer/Legal Counsel			

	4. Has the entity identified those laws or policies that specify when a record can be disclosed to a member of the public?	System Administrator OR Data Privacy Officer/Legal Counsel			
	5. Does the entity maintain an audit trail to document access to and disclosure of information retained by the entity (e.g., dissemination logs)?	System Administrator OR Data Privacy Officer/Legal Counsel OR Technical Systems Security Staff			
	6. If release of information can be made only under exigent circumstances, are those circumstances described?	System Administrator OR Data Privacy Officer/Legal Counsel			
	7. Does the entity adhere to laws or policies for confirming the existences or non-existence of information to persons or agencies that are not eligible to receive the information?	System Administrator OR Data Privacy Officer/Legal Counsel			
J. Redress **J.1. Disclosure**	**Disclosure** 1. If required by law or policy, has the entity established procedures for disclosing information to an individual about whom information has been gathered (for example, proof of identity, fingerprints)?	System Administrator OR Data Privacy Officer/Legal Counsel			
	2. Are there conditions under which an entity will not disclose information to an individual about whom information has been gathered? Note: The privacy policy will cite applicable legal authority for each stated basis for denial.	System Administrator OR Data Privacy Officer/Legal Counsel			
	3. If the entity did not originate the information and does not have the right to disclose it, are there circumstances in which the entity will either refer the individual to the agency originating the information or notify the originating agency of the request?	System Administrator OR Data Privacy Officer/Legal Counsel			

J. Redress J.2. Corrections	1. Has the entity established procedures for handling individuals' requests for correction involving information the entity has disclosed and can change because it originated the information?	System Administrator OR Data Privacy Officer/Legal Counsel			
J. Redress J.3. Appeals	1. If requests for disclosure or corrections are denied, does the entity have established procedures for appeal?	System Administrator OR Data Privacy Officer/Legal Counsel			
K. Security Safeguards	1. Does the agency or exchange have a designated security officer?	Entity Administrator OR Data Privacy Officer/Legal Counsel OR Technical Systems Security Staff			
	2. Does the entity have physical, procedural, and technical safeguards for ensuring the security of its data? Note: The privacy policy will describe how information will be protected from unauthorized access, modification, theft, or sabotage (whether internal or external) resulting from natural or human-caused disasters or intrusions with, for example, procedures, practices, system protocols, use of software, information technology tools, and physical security measures.	Entity Administrator OR Data Privacy Officer/Legal Counsel OR Technical Systems Security Staff			
	3. Is information stored in a secure format and a secure environment?	Entity Administrator OR Data Privacy Officer/Legal Counsel OR Technical Systems Security Staff			
	4. Does the entity utilize watch logs to maintain audit trails or requested and disseminated information, and do logs identify the user initiating the query?	Entity Administrator OR Data Privacy Officer/Legal Counsel OR Technical Systems Security Staff			

	5. Does the entity have established procedures for adhering to data breach notification laws or policies?	Entity Administrator OR Data Privacy Officer/Legal Counsel OR Technical Systems Security Staff			
L. Information Retention and Destruction	1. Does the entity have a records retention and destruction policy (including methods for removing or destroying information)?	System Administrator OR Data Privacy Officer/Legal Counsel			
	2. Does the entity have a review schedule for validating or purging information?	System Administrator OR Data Privacy Officer/Legal Counsel			
	3. Will there be a periodic review of collected data to make sure they are still needed? If so, include the review schedule	System Administrator			
M. Accountability and Enforcement M. 1 Information System Transparency	Information System Transparency 1. Does the entity have a point of contact (position/title) for handling inquiries or complaints?	System Administrator OR Data Privacy Officer/Legal Counsel			
	2. Will the privacy policy be available on the entity's public website?	System Administrator OR Data Privacy Officer/Legal Counsel			
M.2 Accountability	**Accountability** 1. Are there procedures and practices the entity follows to enable evaluation of user compliance with system requirements and applicable law, as well as its privacy policy, when established?	System Administrator OR Data Privacy Officer/Legal Counsel OR Technical Systems Security Staff			
	2. Is there an established mechanism for personnel to report errors and suspected or confirmed violations of policies related to protected information?	System Administrator OR Data Privacy Officer/Legal Counsel			

M. 3 Enforcement	**Enforcement** 1. Has the entity established procedures for enforcement (sanctions) if an agency or authorized user is suspected of being or has been found to be in noncompliance with the laws and policies, including the entity's privacy policy, when established?	System Administrator OR Data Privacy Officer/Legal Counsel			
N. Training	1. Will the entity require any individual having physical or logical access to entity information to participate in training programs regarding the implementation of and adherence to the privacy policy?	System Administrator OR Data Privacy Officer/Legal Counsel			
	2. Will the entity's privacy training program cover the purpose of the policy, substance and intent of the provisions of the policy, impact of infractions, and possible penalties for violations?				