

Privacy Program Strategic Plan, 2021-25 One-page Summary

CURRENT STATE		PLAN		FUTURE STATE
Program Area	Score*	Initiatives	Priority/Term	Key Success Indicators
<b>I. PROGRAM GOVERNANCE</b>  1. Program Accountability and Authority 1.1 Internal 1.2 Service Providers 2. Policies and Procedures 3. Communication, Training and Awareness	2	[1] Delegation Order Revision	High / Short-Term	<ul style="list-style-type: none"><li>• Number of incidents of faulty action or decision-making due to redundant or unclear roles.</li><li>• FOIP Coordinator and City compliance actions and decision-making meet identified standards.</li></ul>
	3	[2] Service Provider Contract Revision	Medium / Short-term	<ul style="list-style-type: none"><li>• Number of service provider services and contracts impacting privacy are identified and include requirements clauses.</li><li>• Number of service providers meeting or exceeding audit assessment standards.</li></ul>
	3	[3] Standalone Privacy Policy and Procedure	High / Short-term	<ul style="list-style-type: none"><li>• Number of adverse privacy incidents due to lack of understanding or knowledge of standards.</li><li>• Number of staff demonstrating an adequate understanding or knowledge of policies and standards.</li><li>• Degree to which policies and standards cover required privacy policy areas.</li></ul>
	3	[4] Communication, Training and Awareness Development	Medium / Mid to Long-Term	<ul style="list-style-type: none"><li>• Effective knowledge of key privacy concepts, requirements and processes across City.</li><li>• Number of communications resources published and distributed.</li><li>• Percentage of targeted staff trained.</li></ul>
	3	[5] Performance Metrics Development	Medium / Mid-Term	<ul style="list-style-type: none"><li>• Coverage of performance indicators across privacy program areas.</li><li>• Increased number of business units establishing indicators, targets, baseline data and annual data.</li><li>• Degree to which business unit initiatives and indicators are integrated into existing performance programs.</li></ul>
<b>II. PERSONAL INFORMATION COLLECTION, USE AND DISCLOSURE</b>  1. Limiting Collection 2. Notification - Identifying Purpose 3. Use and Disclosure 4. Consent 5. Employee Information 6. Authorized Representatives 7. Research 8. Performance Metrics	2	[1] PIA Follow-up and Auditing	Medium / Mid-Term	<ul style="list-style-type: none"><li>• Degree to which audit framework is integrated into existing project management.</li><li>• Number of deficiencies rectified as compared to deficiencies outstanding.</li><li>• Number of PIA follow up audits completed, based on identified targets</li></ul>
	2	[2] Track and Assess Personal Information Collected	Medium /Long - term	<ul style="list-style-type: none"><li>• Number and percentage of PIBs and personal information collection assessments completed and re-evaluated by departments annually.</li><li>• Number of unauthorized collection flows.</li><li>• Number of opportunities to de-identify and anonymize personal information implemented.</li></ul>
	2	[3] Inventory and Review Collection Notices	Medium / Mid-Term	<ul style="list-style-type: none"><li>• Number and percentage of collection notices identified, evaluated, and revised as required.</li><li>• Collection notices clearly provide the collection authority, purpose and resource for further information.</li></ul>
	4	[4] Mandatory Privacy Training for all City Staff	High / Short and Mid-term	<ul style="list-style-type: none"><li>• Number and percentage of identified staff trained at assigned level.</li><li>• Number of adverse privacy incidents due to lack of understanding or knowledge of policies and standards.</li><li>• Degree to which privacy and security are integrated into operational decision-making.</li></ul>
	2			
<b>III. RIGHT OF ACCESS AND CORRECTION</b>  1. Access and Correction Process 2. Proactive Dissemination/ Routine Disclosure 3. Performance metrics	4	[1] Access and Privacy Website Development	Medium / Short-term	<ul style="list-style-type: none"><li>• Efficiency and timeliness of access and correction requests and responses.</li><li>• Number of requests resolved by reference to the website and other highlighted options.</li></ul>
	3	2] Departmental Access and Sharing Standard and Registry	Medium /Long-Term	<ul style="list-style-type: none"><li>• Number of requests resolved by reference to disclosure registry.</li><li>• Number of formal access requests.</li><li>• Efficiency and timeliness of departmental responses to requests for information.</li></ul>
	3			
<b>IV. SECURITY AND INFORMATION MANAGEMENT</b>  1. Policies, Procedures, and Guidelines 2. Information Management and Retention 3. Personal Information Banks 4. PI Systems and Privacy Impact Assessments (PIAs) 5. Performance Metrics	3	[1] Review Information Management and Security Policy	Medium / Mid-Term	<ul style="list-style-type: none"><li>• Number of adverse security incidents due to lack of understanding or knowledge standards.</li><li>• Number of staff demonstrating an adequate understanding or knowledge of policies and standards.</li><li>• Degree to which policies and standards cover required security policy area</li></ul>
	4	[2] Personal Information Registry (PIR)	Medium / Long-term	<ul style="list-style-type: none"><li>• Number of PIBs identified.</li><li>• Degree to which PI location, information flows, authorities, security and retention are effectively tracked.</li><li>• Efficiency and timeliness of PIR capture.</li></ul>
	2	[3] PIA Follow-up Process	Medium / Mid-Term	<ul style="list-style-type: none"><li>• Degree to which follow-up framework is integrated into existing project management.</li><li>• Number of deficiencies rectified as compared to deficiencies outstanding.</li><li>• Number of PIA follow ups completed, based on identified targets</li></ul>
	3	[4] PIA Education and Training	High /Mid-term	<ul style="list-style-type: none"><li>• Number and percentage of identified staff trained at assigned level.</li><li>• Number of non-compliant projects and systems due to lack of assessment.</li><li>• Degree to which privacy and security are integrated into system development and operational decision-making.</li></ul>
	2			

**\*IM Maturity Level Scale**

