

Contact Information

Full Name:

Email Address:

CMSM/DSSAB:

Please Select Auto populated. Please Keep Intact!

Algoma District Services Adm	North Program Office 1 (Northern)
District of Sault Ste Marie Ser	North Program Office 1 (Northern)
District of Thunder Bay Servic	North Program Office 1 (Northern)
Kenora District Services Boar	North Program Office 1 (Northern)
Rainy River District Social Ser	North Program Office 1 (Northern)
City of Greater Sudbury	North Program Office 2 (North East)
District Municipality of Musks	North Program Office 2 (North East)
District of Cochrane Social Se	North Program Office 2 (North East)
District of Nipissing Social Ser	North Program Office 2 (North East)
District of Parry Sound Social	North Program Office 2 (North East)
District of Timiskaming Social	North Program Office 2 (North East)
County of Wellington	Central Program Office 1 (Central East)
County of Dufferin	Central Program Office 1 (Central East)
County of Simcoe	Central Program Office 1 (Central East)
Regional Municipality of York	Central Program Office 1 (Central East)
Regional Municipality of Hal	Central Program Office 2 (Central West)
Regional Municipality of Peel	Central Program Office 2 (Central West)
Regional Municipality of Wat	Central Program Office 2 (Central West)
City of Cornwall	East Program Office 1 (Eastern)
County of Lanark	East Program Office 1 (Eastern)
United Counties of Leeds & G	East Program Office 1 (Eastern)
County of Renfrew	East Program Office 1 (Eastern)
City of Ottawa	East Program Office 1 (Eastern)
United Counties of Prescott &	East Program Office 1 (Eastern)
City of Kawartha Lakes	East Program Office 2 (South East)
City of Peterborough	East Program Office 2 (South East)
County of Northumberland	East Program Office 2 (South East)
Regional Municipality of Dur	East Program Office 2 (South East)
City of Kingston	East Program Office 2 (South East)
County of Hastings	East Program Office 2 (South East)
County of Lennox and Addin	East Program Office 2 (South East)
City of London	West Program Office 1 (South West)
City of St Thomas	West Program Office 1 (South West)
City of Stratford	West Program Office 1 (South West)
City of Windsor	West Program Office 1 (South West)
County of Bruce	West Program Office 1 (South West)
County of Grey	West Program Office 1 (South West)
County of Lambton	West Program Office 1 (South West)
Municipality of Chatham-Ken	West Program Office 1 (South West)
County of Huron	West Program Office 1 (South West)
City of Brantford	West Program Office 2 (Hamilton Niagara)
City of Hamilton	West Program Office 2 (Hamilton Niagara)
Norfolk County	West Program Office 2 (Hamilton Niagara)
Regional Municipality of Niag	West Program Office 2 (Hamilton Niagara)
County of Oxford	West Program Office 2 (Hamilton Niagara)
City of Toronto	Toronto

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Ontario Works Privacy Risk Assessment												
2													
3	<ul style="list-style-type: none"> The objective of the Ontario Works Privacy Risk Assessment Template is to provide Social Assistance (SA) service delivery sites with a systematic approach through consistent structures and processes for proactively managing privacy risks. 												
4													
5	<ul style="list-style-type: none"> Ensuring that SA delivery sites and the ministry have a clear understanding and line of sight on privacy risks across social assistance programs will enable stronger privacy risk management across the social assistance sector. 												
6													
7	<ul style="list-style-type: none"> This template is to be used by SA delivery sites to identify, assess, document and mitigate privacy risks and to report high risks and mitigations to the ministry. 												
8													
9	The Privacy Risk Management Process												
10													
11	Service Planning				Review and Analysis				Monitoring				
12	1. Ministry provides template via TPON.				The Ministry:				1. Ministry develops and provides sites with questions to be used for testing high risk mitigation strategies.				
13	2. SA delivery site completes template as per Instructions tab.				1. Receives completed templates from service delivery sites.				2. SA delivery sites test mitigation strategies to ensure they are working and submit results to ministry.				
14	3. SA delivery site leverages and includes high risks in the service planning Logic Model.				2. Consolidates and analyzes data.				3. Ministry summarizes results and shares with SA delivery sites for future reference/best practices.				
15	4. SA delivery site uploads completed template to TPON along with rest of service contract package.				3. Identifies areas for privacy risk testing.				4. As needed, ministry works with SA delivery sites to discuss and agree on a plan of action or next steps.				
16													
17													
18													
19													
20													
21													
22													
23	Refer to the "0. Instructions" tab for step-by-step instructions on completing tabs 1 and 2												

Risk Assessment Tab	
Columns	Prepopulated Risk Descriptions
A	List of Core Privacy Principles based on CSA and GAPP principles.
B	List of Objectives for each of the Core Privacy Principles.
C	The Risk Tracking Number for each of the Risk Descriptions.
D	List of Risk Descriptions associated with each Core Privacy Principle Objective.
Columns	Instructions
A+B+C+D	Review the prepopulated privacy principles, objectives and risk descriptions.
E	Use the drop down menu to select and assign a value from 1 to 5 for the 'Likelihood' of each risk occurring.
F	Use the drop down menu to select and assign a value from 1 to 5 for the possible 'Impact' if the risk occurred.
G	The template will automatically calculate the risk 'Priority Rating' and colour code it as Low, Medium, Medium-High or High.
H	The template will automatically calculate the 'Inherent Risk Level' to indicate if it is Low, Medium, Medium-High or High.
Mitigation for High Risks Tab	
Columns	Instructions
A	The Risk Tracking Numbers for each of the Risk Descriptions are prepopulated.
B	The list of Risk Descriptions associated with each of the Core Privacy Principle Objectives are prepopulated.
C	The template will automatically carry over the 'Inherent Risk Level' calculated from the Risk Assessment tab, but it will only colour code the "High" risks to make them easy to distinguish.
D	Only for the risks ranked 'High', enter the name of the "Risk Owner", the person assigned to determine how to mitigate a specific risk, take appropriate action and monitor the risk.
E	Only for the risks ranked 'High', document if there are existing controls and processes in place to mitigate the risk.
F	If there are no existing controls or if the current controls are not sufficient, the risk owner develops and enters mitigation strategies only for the risks ranked 'High'. Mitigation strategies should be SMART (Specific, Measurable, Achievable, Realistic, and Time-bound) and at a high level, detail how they will reduce the likelihood and impact of the risk.

Assessment Criteria within tab 3 provide the OPS Risk Assessment Methodology Placemat

Inherent Privacy Risk Assessment

(Assess the natural level of privacy risk built-into the system, process or activity)

A	B	C	D	E	F	G	H	
(Based on CSA and GAPP principles)	Each privacy principle has a set of established objectives.	Risk tracking number	Risk descriptions have been pre-populated for consistency.	Risk Likelihood: 1. Rare 2. Unlikely 3. Possibly 4. Likely 5. Almost certain	Risk Impact: 1. Insignificant 2. Minor 3. Moderate 4. Major 5. Critical	Risk Rating = Likelihood x Impact		
						Level	Score	How the Risk Should be Managed
						High	20+	Significant management attention required.
						Medium-High	11 to 19	Ongoing management review and discussion is necessary.
						Medium	5 to 10	Limited management review required.
Low	1 to 4	Risk can be managed through existing oversight/routine procedures.						
Core Privacy Principles	Privacy Principle Objectives	Risk Numbers	Risk Descriptions	Likelihood (1 to 5)	Impact (1 to 5)	Priority Rating (Likelihood x Impact)	Inherent Risk Level	
Accountability and Privacy Management	1.1 The organization defines and documents its privacy policies with respect to notice; choice and consent; collection; use, retention and disposal; access; disclosure to third parties; security for privacy; quality; and monitoring and enforcement.	1.1.1	Social Assistance privacy practices not being defined and documented.	1	4	4	Low	
		1.1.2	SA staff not understanding privacy practices.	1	3	3	Low	
		1.1.3	SA staff not adhering to privacy practices.	1	4	4	Low	
		1.1.4	SA management not monitoring and enforcing privacy practices.	1	4	4	Low	
	1.2 Privacy policies and the consequences of noncompliance with such policies are communicated at least annually to the organization's internal personnel responsible for collecting, using, retaining, and disclosing personal information. Changes in privacy policies are communicated to such personnel shortly after the changes are approved.	1.2.1	SA staff are not aware of consequences of noncompliance to privacy policies.	1	5	5	Medium	
		1.2.2	Changes to privacy policies not being communicated in a timely manner.	1	1	1	Low	
		1.2.3	Changes to privacy policies not being understood by SA staff.	1	1	1	Low	
	1.3 Privacy policies, procedures and changes are reviewed and approved by management.	1.3.1	Unclear accountability for updating privacy policies.	1	1	1	Low	
		1.3.2	Changes made to privacy policies and procedures are not aligned with SA delivery expectations.	1	1	1	Low	
		1.3.3	Inaccurate changes are made to privacy policies and procedures.	1	1	1	Low	
	1.4 Policies and procedures are reviewed and compared to the requirements of applicable laws and regulations at least annually and whenever there are changes to such laws and regulations. Privacy policies and procedures are revised to conform to the requirements of applicable laws and regulations.	1.4.1	Privacy policies become outdated and not being consistent with applicable laws and regulations.	1	1	1	Low	
	1.5 A privacy risk assessment process is established to identify new or changed risks to personal information and to outline the proposed remediation activities to address this risk.	1.5.1	Unawareness of new/emerging risks to personal information.	1	3	3	Low	
		1.5.2	Unawareness of severity of new/changed risks to personal information to determine whether action is needed.	1	3	3	Low	
	Notice / Consent	2.1 Notice is provided to the client about the organizations' privacy policies and procedures: • At or before the time personal information is collected, or as soon as practical thereafter. If personal information is collected from sources other than the client, such sources are described in the notice. • At or before the organization changes its privacy policies and procedures, or as soon as practical thereafter. • Before personal information is used for new purposes not previously identified.	2.1.1	SA staff not obtaining consent when required.	1	4	4	Low
			2.1.2	SA clients are not informed on what personal information and how it will be used.	1	4	4	Low
2.1.3			SA clients are not informed in advance (timely) of the use of their personal information.	1	4	4	Low	
2.2 Clients are informed: • About the choices available to them with respect to the collection, use and disclosure of personal information. • That implicit or explicit consent is required to collect, use, and disclose personal information, unless a law or regulation specifically requires otherwise.		2.2.1	SA clients not being provided with the choices available to them regarding their personal information.	4	1	4	Low	
3.1 The organization's privacy policies address the collection of personal information.	3.1.1	SA clients not being aware of how personal information is collected.	1	1	1	Low		

Collection	3.2 The collection of personal information is limited to that necessary for the purposes identified in the notice.	3.2.1	SA client personal information beyond what is required was collected in error.	2	1	2	Low
	3.3 Methods of collecting personal information are reviewed by management before they are implemented to confirm that personal information is obtained (a) fairly, without intimidation or deception, and (b) lawfully, adhering to all relevant rules of law, whether derived from statute or common law, relating to the collection of personal information.	3.3.1	SA client personal information was collected in a manner unsupported by related laws.	1	4	4	Low
		3.3.2	Unfairly collecting personal information.	1	4	4	Low
Use, Retention and Disposal	4.1 The organization limits the use of personal information to the purposes identified in the notice and for which the client has provided implicit or explicit consent. The organization retains personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.	4.1.1	Use of personal information for purposes other than what SA client consented.	1	4	4	Low
	4.2 Clients are informed that personal information is used only for the purposes identified in the notice and only if the client has provided implicit or explicit consent, unless a law or regulation specifically requires otherwise.	4.2.1	SA clients not being aware of the purposes for which their personal information is being used.	1	4	4	Low
	4.3 Personal information is retained for no longer than necessary to fulfill the stated purposes, or for a period specifically required by law or regulation.	4.3.1	SA client personal information continues to be retained for longer than necessary.	1	1	1	Low
	4.4 Personal information is disposed of in a manner that prevents loss, theft, misuse or unauthorized access.	4.4.1	Personal information to be disposed continues to be accessible by staff.	1	1	1	Low
		4.4.2	Personal information to be disposed accessed by unauthorized individuals within and/or external to the organization.	3	1	3	Low
Access	5.1 Clients are able to determine whether the organization maintains personal information about them and, upon request, may obtain access to their personal information.	5.1.1	SA clients not being able to request access to their personal information.	1	2	2	Low
	5.2 Clients are able to update or correct personal information held by the organization. If practical and economically feasible to do so, the organization provides such updated or corrected information to third parties that previously were provided with the client's personal information.	5.2.1	SA clients not being able to update and correct their personal information.	1	4	4	Low
Third Party Disclosure	6.1 The organization discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the client.	6.1.1	SA staff disclose client personal information to third parties without consent.	1	5	5	Medium
	6.2 Personal information is disclosed only to third parties who have agreements with the organization to protect personal information in a manner consistent with the relevant aspects of the organizations's privacy policies or other specific instructions or requirements. The organization has procedures in place to evaluate that the third parties have effective controls to meet the terms of the agreement, instructions, or requirements.	6.2.1	Sharing of client personal information with third parties which may not have appropriate processes to maintain privacy controls/safeguards over the personal information.	1	5	5	Medium
Security	7.1 The organization protects personal information against physical unauthorized access.	7.1.1	SA client personal information in physical form access by unauthorized individuals.	1	1	1	Low
	7.2 Logical access to personal information is restricted by procedures that address the following matters: a. Authorizing and registering internal personnel and clients b. Identifying and authenticating internal personnel and clients c. Making changes and updating access profiles d. Granting system access privileges and permissions e. Preventing clients from accessing other than their own personal or sensitive information f. Limiting access to personal information to only authorized internal personnel based upon their assigned roles and	7.2.1	SA client personal information in any form access by unauthorized individuals.	1	5	5	Medium

	responsibilities g. Distributing output only to authorized internal personnel h. Restricting logical access to offline storage, backup data, systems, and media i. Restricting access to system configurations, super-user functionality, master passwords, powerful utilities, and security devices (for example, firewalls) j. Preventing the introduction of viruses, malicious code, and unauthorized software.	7.2.2	SA staff saving client personal information on drives /external devices that can easily be subject to unauthorized access.	1	1	1	Low
Quality Management	8.1 The organization maintains accurate, complete, and relevant personal information for the purposes identified in the notice.	8.1.1	SA client information maintained is not accurate and/or complete.	1	4	4	Low
	8.2 Compliance with privacy policies, procedures, commitments, applicable laws, regulations, service level agreements and other contracts is reviewed, documented and the results of such reviews are reported to management. If problems are identified, remediation plans are developed and implemented.	8.2.1	Noncompliance with privacy policy documents is not identified in a timely manner.	1	1	1	Low
		8.2.2	Noncompliance with privacy policy documents not being remedied in a timely manner.	1	1	1	Low
Privacy Incident and Breach Management	9.1 A documented privacy incident and breach management program has been implemented that includes, but is not limited to, the following: • Procedures for the identification, management, and resolution of privacy incidents and breaches • Defined responsibilities • A process to identify incident severity and determine required actions and escalation procedures • A process for complying with breach laws and regulations, including stakeholders breach notification, if required • An accountability process for employees or third parties responsible for incidents or breaches with remediation, penalties, or discipline as appropriate • A process for periodic review (at least on an annual basis) of actual incidents to identify necessary program updates based on the following: - Incident patterns and root cause - Changes in the internal control environment or external requirements (regulation or legislation) • Periodic testing or walkthrough process (at least on an annual basis) and associated program remediation as needed	9.1.1	Privacy incidents and breaches occur undetected.	1	5	5	Medium
		9.1.2	Privacy incidents and breaches that are detected are not documented.	1	5	5	Medium
		9.1.3	Causes for privacy incidents and breaches are not explored and understood.	1	1	1	Low
		9.1.4	Lack of awareness of severity and frequency of privacy incidents and privacy.	1	1	1	Low
Privacy Training and Awareness	10.1 A privacy awareness program about the organization's privacy policies and related matters, and specific training for selected personnel depending on their roles and responsibilities, are provided.	10.1.1	SA delivery staff not knowing their obligations towards handling personal information.	1	5	5	Medium

Highest Inherent Risks

Develop Mitigation Strategies for 'High' risks from the Risk Assessment (Tab 1)

A	B	C	D	E	F
Risk Numbers	Risk Descriptions	Inherent Risk Level (Tab 1)	Risk Owner	Description of Controls/Processes Already in Place or None ?	If nothing in place, develop a mitigation plan and provide details including dates:
1.1.1	Social Assistance privacy practices not being defined and documented.	Low			
1.1.2	SA staff not understanding privacy practices.	Low			
1.1.3	SA staff not adhering to privacy practices.	Low			
1.1.4	SA management not monitoring and enforcing privacy practices.	Low			
1.2.1	SA staff are not aware of consequences of noncompliance to privacy policies.	Medium	Management	We feel staff are aware of consequences, it's just that if it happens, the impact is serious so happening even once a year is too often. We review privacy policy with staff annually, we complete a privacy audit annually. We review during orientation and onboarding with staff.	
1.2.2	Changes to privacy policies not being communicated in a timely manner.	Low			
1.2.3	Changes to privacy policies not being understood by SA staff.	Low			
1.3.1	Unclear accountability for updating privacy policies.	Low			
1.3.2	Changes made to privacy policies and procedures are not aligned with SA delivery expectations.	Low			
1.3.3	Inaccurate changes are made to privacy policies and procedures.	Low			
1.4.1	Privacy policies become outdated and not being consistent with applicable laws and regulations.	Low			
1.5.1	Unawareness of new/emerging risks to personal information.	Low			
1.5.2	Unawareness of severity of new/changed risks to personal information to determine whether action is needed.	Low			
2.1.1	SA staff not obtaining consent when required.	Low			
2.1.2	SA clients are not informed on what personal information and how it will be used.	Low			
2.1.3	SA clients are not informed in advance (timely) of the use of their personal information.	Low			
2.2.1	SA clients not being provided with the choices available to them regarding their personal information.	Low			
3.1.1	SA clients not being aware of how personal information is collected.	Low			
3.2.1	SA client personal information beyond what is required was collected in error.	Low			
3.3.1	SA client personal information was collected in a manner unsupported by related laws.	Low			
3.3.2	Unfairly collecting personal information.	Low			
4.1.1	Use of personal information for purposes other than what SA client consented.	Low			
4.2.1	SA clients not being aware of the purposes for which their personal information is being used.	Low			
4.3.1	SA client personal information continues to be retained for longer than necessary.	Low			
4.4.1	Personal information to be disposed continues to be accessible by staff.	Low			
4.4.2	Personal information to be disposed accessed by unauthorized individuals within and/or external to the organization.	Low			
5.1.1	SA clients not being able to request access to their personal information.	Low			
5.2.1	SA clients not being able to update and correct their personal information.	Low			
6.1.1	SA staff disclose client personal information to third parties without consent.	Medium	Management	If this happens, it is serious so impact is rated high. We have policies and procedures and have an intake job aid to ensure consent has been provided. These policies and procedures include any legal authorities and they must go through our Clerk's department. We work closely with the City's Clerks Department	
6.2.1	Sharing of client personal information with third parties which may not have appropriate processes to maintain privacy controls/safeguards over the personal information.	Medium	Management	This has not happened however if it did, the impact would be serious. All above controls would apply in addition to requirement attestation from third party about controls and safeguards for personal information.	
7.1.1	SA client personal information in physical form access by unauthorized individuals.	Low			

7.2.1	SA client personal information in any form access by unauthorized individuals.	Medium	Management	This would be high impact if it happens. We do complete audits on this and will also make requests to the province to review staff access. We are strict and clear about access and no sharing of passwords. We review these requirements annually and have staff sign forms to confirm they abide by these principles. We have processes to follow up with staff for any breach of any kind - this would include reporting to the province and to our Clerk's department - who may in turn report breaches to the privacy commission.
7.2.2	SA staff saving client personal information on drives /external devices that can easily be subject to unauthorized access.	Low		
8.1.1	SA client information maintained is not accurate and/or complete.	Low		
8.2.1	Noncompliance with privacy policy documents is not identified in a timely manner.	Low		
8.2.2	Noncompliance with privacy policy documents not being remedied in a timely manner.	Low		
9.1.1	Privacy incidents and breaches occur undetected.	Medium	Management	If this happens, it would have high impact. We review SAMS reports, AD-Hoc Ministry reports, complete audits on all third party accessed information on all staff who has access to this information. After receiving provincial notification for an incident back in 2017, we are diligent in our monitoring of third party access. We restrict access and keep logs and have one management supervisor who monitors third party information monthly.
9.1.2	Privacy incidents and breaches that are detected are not documented.	Medium	Management	If this happened, it would be serious. We do report all breaches to both the province and the City's Clerk's office and follow and implement any direction. If the breach is with an individual, we would follow up with a performance meeting with that staff member, working with our Human Resources Department
9.1.3	Causes for privacy incidents and breaches are not explored and understood.	Low		
9.1.4	Lack of awareness of severity and frequency of privacy incidents and privacy.	Low		
10.1.1	SA delivery staff not knowing their obligations towards handling personal information.	Medium	Management	If this were to occur it would have serious impact. We are confident our staff are fully aware of the obligations toward handling personal information and have all policies and procedures listed above to ensure this would not be the case

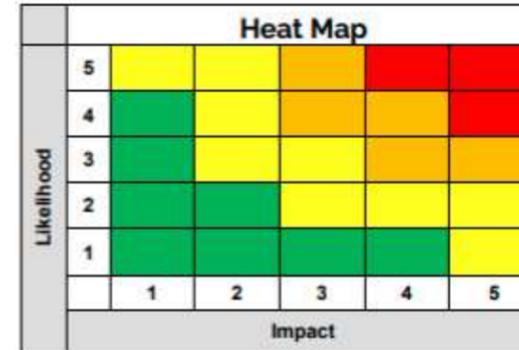
What is a risk?

Risk is the effect of uncertainty on objectives. It can be characterized as either a potential negative (threat) or positive (opportunity) consequence or event that deviates from an expected outcome.

Likelihood*			
Assessment	Level	Description	Probability
Rare	1	Risk event is very unlikely to occur in most circumstances.	<10%
Unlikely	2	Risk event is unlikely to occur in normal circumstances.	11% - 30%
Possible	3	Risk event may occur in certain circumstances.	31% - 50%
Likely	4	Risk event is likely to occur in most circumstances.	51% - 90%
Almost Certain	5	Risk event will occur in normal circumstances.	>91%

** Likelihood should consider the appropriate timeframe for the objectives and related products.*

Impact		
Assessment	Level	Description
Insignificant	1	A risk event that, if it occurs, will have a little or no impact on achieving outcome objectives.
Minor	2	A risk event that, if it occurs, will have negligible/inconsequential impact on achieving desired results, to the extent that one or more stated outcome objectives will fall below goals but well above minimum acceptable levels.
Moderate	3	A risk event that, if it occurs, will have limited impact on achieving desired results, to the extent that one or more stated outcome objectives will fall well below goals but above minimum acceptable levels.
Major	4	A risk event that, if it occurs, will have an extensive impact on achieving desired results, to the extent that one or more stated outcome objectives will fall below acceptable levels.
Critical	5	A risk event that, if it occurs, will have an excessive impact on achieving desired results, to the extent that one or more stated outcome objectives will not be achieved.



Risk Rating = Likelihood x Impact		
Level	Score	Recommended Response
High	20-25	Risk management requires significant senior executive/board decision makers attention. Mitigating actions should be tracked and monitored frequently and reported to senior leadership.
Medium - High	11-19	Risk management requires ministry senior leadership attention. Mitigating actions should be tracked, monitored and reported to senior leadership.
Medium	5-10	Risk can be managed by risk owner(s). Controls should be reviewed to determine whether additional action should be taken.
Low	1-4	Risk can be managed using controls already in place. No mitigation efforts required.

 Risks levels above are rated on a **residual basis** (i.e. factoring in all existing controls already in place).