OSFI Technology and Cyber Incident Report

1. Incident & Contact Information	**Incident Name or Identifier:**	
	Date and Time Discovered/Detected:	**Date and Time Occurred**:
	Name of your Institution:	
	Key Contact's Name	Key Contact's Position
	Key Contact's Email	Key Contact's Phone Number
	Incident Lead's Name	Incident Lead's Position
2.Site Location and Lines of Business Affected	Name of Business Line Affected	
	Technologies Affected	
	Site/Location Affected	
3. Description of Risk & Incident	Provide the type of incident that occurred (e.g. Ransomware, Phishing, DDoS, etc.).	Provide description of sensitive information compromised or at risk.
	Provide details on the tools, techniques and processes involved in the incident.	Provide the indicators of compromise.
4. Incident Level or Priority	Select an incident level or priority from the drop-down list.	
5. Current State	**Please provide additional details below including: current state, actions completed and pending, with estimated timelines to address the remediation of the incident. Also include root cause or known causes of the incident.**	
	Internal and External Notifications	
	Has senior management been notified?	Date and time senior management was notified (if applicable).
	Have other regulators or supervisory agencies been notified?	Date and time regulatory or supervisory agencies were notified (if applicable).
	Provide names of other notified regulatory or supervisory agencies.	
	Have any law enforcement authorities been notified?	Name of notified law enforcement authorities.
	Have any cyber insurance providers been notified?	Name of notified cyber insurance providers and date of notification.
	Has a cyber and/or an insurance policy claim been initiated?	Have external forensics firms been engaged?
	Has the breach coach been engaged?	Has internal or external legal counsel been engaged?