Technology and Cyber Incident Report
Federally Regulated Private Pension Plans [Draft]

This completed form should be sent to OSFI within 24 hours of discovering a technology or cyber security incident; our email is pensions@osfi-bsif.gc.ca

Refer to the OSFI [draft] advisory: Technology and Cyber Security Incident Reporting for Federally Regulated Private Pension Plans (FRPPs) for more information about OSFI's expectations.

Incident & contact information	
Date and Time Discovered: (YYYY-MM-DD) & (00:00 – 23:59)	
Date and Time Occurred: (YYYY-MM-DD) & (00:00 – 23:59)	
FRPP Name:	
OSFI Registration Number:	
Contact Name(s):	
Contact Phone Number(s):	
Contact Email(s):	
Description of risk & incident	
Incident Category: ☐ Technology ☐ Cyber ☐ Other (please specify): _____ _____ _____ _____ _____	Where did the incident occur? ☐ Employer and / or Board of Trustees ☐ FRPP administrator ☐ Third party provider ☐ Other (please specify): _____ _____ _____ _____

Provide the incident type(s):

☐ Technology asset[1] outage	☐ DDoS	☐ Ransomware
☐ Technology asset degradation/delay	☐ Insider Threat	☐ Unauthorized access
☐ Account take-over	☐ Malware – Other	☐ Loss/theft of equipment
☐ Cyber Crime	☐ Malware Campaign	☐ Other (please specify): _____
☐ Data breach/leak	☐ Online Extortion	_____
	☐ Phishing	

Impact on the FRPP and its members and beneficiaries	
Number of plan members and beneficiaries impacted:	
Amount of benefit payments not made:	
Amount of contributions not remitted:	
Amount of pension investments impacted:	
Provide description of sensitive information compromised or at risk. If no sensitive information is at risk, indicate N/A	

[1] A "technology asset" can be something tangible (e.g., hardware, infrastructure) or intangible (e.g., software/application, data, information) that needs protection and supports the provision of technology services.

Internal and external notifications	
Which of the following stakeholders have been notified?	Date and time of notification: (YYYY-MM-DD) & (00:00 – 23:59)
☐ Plan Administrator	
☐ Other regulators, supervisory agencies or government departments (please specify)	
☐ Service providers such as third-party administrators, custodians, actuaries, pension fund auditors and legal counsel (please specify)	
☐ Law enforcement authorities	
☐ Cyber insurance providers	
☐ Plan members and beneficiaries	
☐ Other (please specify): _____	