JULY 2024

Information Security Guideline

Pension Plan Administrators

Draft for Consultation

BCFSA

Contents

Introduction

BC Financial Services Authority ("BCFSA") Guidelines establish principles that regulated entities are expected to implement and follow and provide best practices on how to meet the objectives of the Guideline.

Potential consequences of information security ("IS") breaches constitute a concern for BCFSA pension plan members, and pension plan administrators ("PPA"). As a result of these concerns, BCFSA has produced this IS guideline that outlines expectations to mitigate IS risks.

This guideline does not replace or substitute other applicable rules, guidance or law and does not require regulated entities or PPAs to act in a way that is incompatible with any legal or regulatory requirements.

Scope

IS risks include unauthorized, illegal, or accidental use, disclosure, access to, modifications or destruction of data, or impairment of network systems (collectively referred to as information security incidents), which can cause serious harm to pension plan members. The risk of unauthorized or illegal access to sensitive information or systems can come from employees, consultants, or external threat actors.

A distinction is made between data privacy and data and system protection (i.e., information security). Data privacy is concerned with issues related to authorized collection, use and disclosure of information. Data and system protection focus on securing against unauthorized or accidental loss or misuse of data or information systems.

Data can be generated by the PPA or provided by third parties to the PPA. Data collection, storage and processing can be in any format (for example; paper, electronic, or video) or location (for example; onsite, offsite, or cloud service). Information systems include people, machines, methods of organization, and procedures which provide input, storage, processing, communications, output, and control functions in relation to information and data.

BCFSA's expectations for outsourcing information system management services to third parties is addressed through a separate Outsourcing Guideline. Where information management services are outsourced, BCFSA expects PPAs to ensure that all service providers comply with all applicable legislation, regulations, and/or rules, as well as this guideline in their treatment of the PPA's information.

This guideline applies to B.C. registered pension plan administrators and replaces the BCFSA Information Security Guideline released October 2021.

Approach

This guideline sets out both high level principles and specific BCFSA expectations.

Principles form the foundation for good governance expected by BCFSA. Principles communicate the spirit of BCFSA's expectation without prescribing the form by which the principle is achieved. BCFSA expects principles to be implemented across all PPAs.

For each principle, specific BCFSA expectations are used for further illustration and clarity. Specific BCFSA expectations are the procedures and practices[1] that achieve the objective of each principle.

The implementation of the guideline will be applied in a risk-based and proportionate manner and will vary given differences in the nature, scope, complexity, and risk profile of the PPA. Principles and expectation outlined in this guideline reflect minimum provisions. When reviewing pension plans, BCFSA may determine that additional specific expectations will be applicable for a particular plan. Additional pension plan related expectations will only be applied following discussions between BCFSA and the pension plan administrator.

Governance

The PPA's governing body is ultimately responsible for overseeing the prudent management of IS risks.

For the purposes of this guideline, the governing body would be the administrator established under the plan documents.

PPAs will need to demonstrate that they have familiarized themselves with industry accepted practices for plan governance, including the Canadian Association of Pension Supervisory Authorities ("CAPSA") Guideline on Pension Plan Governance, and other CAPSA guidelines as applicable.

For PPAs the following expectations apply.

Administrators should:

- Ensure the written governance policy recognizes information security as a material risk and:
    - Identifies all participants who have authority to make decisions in respect of those structures, processes and controls and describes the roles, responsibilities, and accountabilities of those participants; and
    - Establishes an ongoing process to identify the educational requirements and skills necessary for the administrator to perform his or her duties in relation to information security.

[1] Procedures operationalize policies. Practices are detailed instructions.

Information Security Risk Management Program

A PPA is expected to establish and document an effective IS risk management program. This program should focus on security measures to mitigate IS risks.

A PPA should design and document an IS Risk Management Program that includes the following:

- Procedures and systems to identify and protect against IS threats and monitor IS incidents;
- A plan that clearly sets out strategies for responding to and recovering from material IS incidents; and
- Internal controls to ensure compliance with established IS risk management policies and procedures.

Identify

A PPA is expected to develop an understanding of IS risk to systems, people, assets, data, and capabilities.

A PPA should:

- Identify the data, personnel, devices, systems, software platforms, and applications and facilities that enable the organization to achieve business objectives;
- Perform a risk assessment to understand the IS threats and risks; and
- Identify IS risk pertaining to third parties, such as suppliers and third-party partners.

Protect

A PPA is expected to protect its data and systems in a reasonable and appropriate manner based on the sensitivity, value and/or criticality that the data and information system have to the PPA and legislative requirements. A PPA should develop and implement preventative physical and logical security measures against identified IS risks to ensure data and information system protection and delivery of critical services.

A PPA should:

- Establish appropriate physical and logical security measures to protect sensitive data of the organization as well as the network systems;

- Document and implement policies, practices, and procedures to manage access rights to information assets and their supporting networks on a need-to-know basis;
- Document and institute controls over privileged system access by strictly limiting and closely supervising staff with elevated information system access entitlements; and
- Implement Information Technology ("IT") system updates from infrastructure and software providers in a timely manner.

Detect

A PPA is expected to establish monitoring processes to rapidly detect IS incidents and periodically evaluate the effectiveness of identified controls, including through network monitoring, testing, audits, and reporting.

A PPA should:

- Establish appropriate capabilities for detecting physical or digital intrusion as well as breaches of confidentiality, integrity, and availability of the information assets used; and
- Maintain and test detection processes and procedures to ensure timely and adequate awareness of IS incidents.

Respond

A PPA is expected to develop and implement appropriate actions in response to IS incidents.

A PPA should:

- Establish appropriate processes to ensure monitoring, handling, and follow-up of IS incidents;
- Execute response procedures and practices to contain the incident, maintain critical functions, and mitigate losses in the event of a material incident[2];
- Establish procedures for reporting IS incidents, as appropriate;
- Inform plan beneficiaries and members about any material incident that has an impact on their benefits, financial or personal interests; and
- Ensure that the measures being taken to mitigate the impact of material incidents are communicated to affected plan beneficiaries.

[2] See Appendix 1 for definition of "material incident."

Recover

A PPA is expected to develop and implement appropriate activities to maintain plans for resilience, restore capabilities or services and comply with applicable legislation.

A PPA should:

- Develop an IS incident recovery plan; and
- Execute a recovery plan during or after an IS incident.

Communication With the Regulator

A PPA is expected to be in communication with BCFSA in the event of a material incident.

- In the event of a material incident, the PPA should contact BCFSA within 24 hours of determining that an IS incident is material. Thereafter, as soon as possible but within 72 hours of a material incident, the PPA should provide BCFSA with a written incident report. See Appendix 1 for guidance on how to determine if an incident is material.
- The initial contact with BCFSA can be in the form of a phone call and may include only a preliminary description of the IS incident and contain fewer details than outlined in the incident report, since some information regarding the incident may not be available at the time. See Appendix 2 for reporting details.
- These are the steps for submitting an incident report:

  Step 1. Notification of intent to submit an incident report:

  - Notify the office of the superintendent of pensions of your intent to submit an incident report by sending an email to pensions@bcfsa.ca. Please include the name of the pension plan and/or the plan number in the notification email.
  - Do not send the incident report or include any sensitive information about the incident in your notification email.

  Step 2. Receive secure link to submit an incident:

  - Once BCFSA receives the notification in email, you will receive a secure SharePoint link to upload the incident report and other correspondence pertaining to the incident.

Appendix 1: Determining If an Information Security Incident Is Material

An IS incident should be of a certain degree of severity for it to be reported to BCFSA. The determination of the severity of an event is made by the PPA and should relate to the impact that the incident will have on the pension plan's members.

For PPAs, indicators that a material incident has occurred could include but are not limited to the following:

If the incident:

- Disrupts the operations of the pension plan to an extent that the plan can no longer be effectively administered;
- Is likely to negatively affect other entities or individuals regulated by BCFSA, or is an incident that is likely to reoccur with other entities or individuals regulated by BCFSA;
- Compromises confidential plan member data; or
- Impacts the ability of the administrator to pay benefits, receive remittances or manage investments.

Appendix 2: Information Security Incident Reporting Information

PPAs should notify BCFSA in the event of a material incident as soon as possible. The initial contact with BCFSA can be in the form of a phone call and may include only a preliminary description of the information security incident and contain fewer details than outlined in the incident report, since some information regarding the incident may not be available at the time.

Thereafter, as soon as possible but within 72 hours after a material incident has occurred, PPAs should provide BCFSA with a written incident report. Where specific details are unavailable the PPA should indicate “information not yet available.” In such cases, the PPA should provide best known estimates and all other details available at the time.

Details to report should include the following:

- Date and time the incident was assessed to be material;
- Date and time/period in which the incident took place;
- Incident type (for example, internal breach, malware, data breach, extortion, etc.);
- Incident description, including:
    - Known direct/indirect impacts (quantifiable and non-quantifiable) including privacy and financial,
    - Whether the incident originated at a third party or has an impact on third party services, and
    - Number of members impacted;
- Primary method used to identify the incident;
- Current status of incident;
- Date for internal incident escalation to pension plan administrator;
- Mitigation actions taken or planned;
- Known or suspected root cause; and
- Name and contact information for the PPA incident lead and liaison with the BCFSA.

Note: No personally identifiable information regarding plan members should be included in the report.

SUBSEQUENT REPORTING REQUIREMENTS

PPAs should provide BCFSA with regular updates as new information becomes available, and until all material details about the incident have been provided. The method and frequency of these updates should be established through discussions with BCFSA considering the severity, impact, and velocity of the incident.

Until the incident is contained/resolved, PPAs should provide BCFSA with situation updates, including any short-term and long-term remediation actions and plans.

Following incident containment, recovery, and closure, the PPA should report to BCFSA on its post incident review and lessons learned.

BC Financial Services Authority

600-750 West Pender Street
Vancouver, BC V6C 2T8

604 660 3555
Toll free 866 206 3030
info@bcfsa.ca