OCTOBER 2021

Information Security Guideline

BC Credit Unions, Insurance and Trust Companies, and Pension Plan Administrators

BCFSA

Contents

Production of this document included environmentally friendly best practices.
Please reduce, reuse and recycle.

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, consumers, pension plan members, provincially incorporated financial institutions ("FIs")[1] and pension plan administrators. In this Guideline, financial institutions and pension plan administrators will be referred to collectively as "PRFIs"[2]. As a result of these concerns, BCFSA has produced this IS Guideline that outlines expectations to mitigate IS risks.

Scope

IS risks include unauthorized, illegal, or accidental use, disclosure, access to, modifications or destruction of data, or impairment of network systems (information security incidents), which can cause serious harm to pension plan members and other financial services consumers, and significant financial and reputational damage to PRFIs. The risk of unauthorized or illegal access to sensitive information or systems can come from employees, consultants, and others within the regulated entity or external threat actors.

Data can be generated by the PRFI or provided by third parties to the PRFI. 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 PRFIs 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 PRFI's information.

A distinction is made between data privacy and data and system protection (i.e., IS). 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.

This Guideline applies to PRFIs – B.C. financial institutions and pension plan administrators. 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, systemic importance, and risk profile of the PRFI.

[1] In this guideline the term financial institutions includes; (i) BC credit unions and (ii) insurance and trust companies incorporated or licensed to do business in BC (excluding extra provincial companies)
[2] PRFIs for the purposes of this guideline include financial institution and administrators of BC registered pension plans.

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 PRFIs.

For each principle, specific BCFSA expectations are used for further illustration and clarity. Specific BCFSA expectations are the procedures and practices[3] that achieve the objective of each principle. For financial institutions, BCFSA may recommend additional IS actions be implemented consistent with a risk-based and proportionate supervisory approach.

Given the differences between institutional structures and legislation applicable to financial institutions and pension plans, the specific expectations associated with each principle will not be applied to pension plan administrators, unless pension plan specific expectations are identified in this Guideline. However, BCFSA will, as with FIs, apply the proportionality principle when reviewing pension plans and 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 PRFI's governing body is ultimately responsible for overseeing the prudent management of IS risks.

For the purposes of this Guideline, the governing body for financial institutions is the Board of Directors. The term "Board of Directors" also includes any group or individual who would hold a comparative position in a financial institution.

For pension plans, the governing body would be the administrator established under the plan documents.

For financial institutions, the following specific expectations apply.

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

The Board of Directors should[4]:

- Identify the governing body accountable for overseeing IS (for example, the Audit Committee of the Board);
- Approve the appropriateness of the IS risk management program relative to the nature, scope, complexity, and risk profile of the organization;
- Possess current and relevant knowledge of IS, or recognize when it needs additional expertise or third-party advice to meet its oversight responsibilities; and
- Assess the competencies, skills, and experience of senior management pertaining to IS.

Senior management should:

- Define and document roles and responsibilities for personnel implementing, managing, and overseeing the effectiveness of the IS strategy to ensure accountability;
- Develop, document, implement, and monitor an IS risk management program including, policies, procedures, and practices for the effective management of the institution's IS risks;
- Periodically review the effectiveness of the IS risk management program and plans for dealing with incidents; and
- Allocate sufficient resources to effectively conduct IS functions.

For pension plans the following expectations apply.

Administrators should:

- Ensure the written governance policy recognizes information security as a material risk and;
    - Sets out the structures, processes, and controls for overseeing, managing, and administering information security;
    - Explains what those structures, processes and controls are intended to achieve;
    - 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.

[4] Reference to the word "should" throughout this guideline means it is recommended that PRFIs adhere to that section.

Information Security Risk Management Program[5]

A PRFI is expected to establish and document an effective IS risk management program, which should be approved by the governing body and, for financial institutions, be reviewed at least once a year by senior management. This program should focus on security measures to mitigate IS risks and should be fully integrated into the PRFI's overall risk management processes.

An FI should design and document an IS Risk Management Program that includes the following:

- IS policies and procedures that align with the organization's risk exposure;
- 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 with roles and escalation processes clearly defined to facilitate timely response management;
- Procedures for testing IS measures to ensure that critical functions, processes, systems, transactions, and interdependencies are effective. The actions should support the objectives of protecting and, if necessary, re-establishing the integrity and availability of operations and the confidentiality of information assets; and,
- Internal controls to ensure compliance with established IS risk management policies and procedures.

Identify

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

An FI 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 as well as their implications on the organization's operations, assets, and individuals (including an analysis of the organization's exposure to severe business disruptions and an assessment of their potential impact);
- Identify IS risk pertaining to third parties, such as suppliers and third-party partners;
- Coordinate and align IS roles and responsibilities with external partners; and

[5] A IS Risk Management Program comprises a complete set of organizational resources including policies, staff, processes, practices, and technologies used to assess, mitigate and respond to IS risks. The contents of an IS Program may be contained in one or more documents and some aspects may be contained in other documents such as ERMs, BCPs, governance policies, etc.

- Collect IS threat information from internal and external sources to inform risk assessments.

Protect

A PRFI 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 PRFI and legislative requirements. A PRFI 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.

An FI should:

- Establish appropriate physical and logical security measures to protect sensitive data of the organization as well as the network systems;
- Document and maintain security policies, practices, and procedures used to manage protection of information whether at rest, in transit, or in use;
- Provide periodic training and awareness on IS to all personnel. The level of training will be commensurate with the individual's access to sensitive data and 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. Controls such as roles-based access, logging and reviewing of privileged users' network activities, strong authentication, and monitoring for anomalies should be implemented;
- Establish, document, and implement multi-layered controls covering people, processes, and technology, with each layer serving as a safety net for preceding layers. 'Multi-layered' should be understood as having more than one control covering the same risk (for example, implementing two-factor authentication for users accessing the network);
- Establish and implement a testing process that validates the robustness and effectiveness of the security measures and ensures that the testing framework is adapted to consider new threats and vulnerabilities identified through risk-monitoring activities;
- Ensure that tests are conducted in the event of changes to infrastructure, processes, or procedures and if changes are made in response to material security incidents;
- Exchange information with external stakeholders to achieve broader IS situational awareness;
- Establish processes to receive, analyze, and respond to vulnerabilities and flaws disclosed to the organization from internal and external sources; and
- Implement Information Technology ("IT") system updates from infrastructure and software providers in a timely manner.

Detect

A PRFI 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.

An FI should:

- Establish appropriate capabilities for detecting physical or digital intrusion as well as breaches of confidentiality, integrity, and availability of the information assets used;
- Monitor information system and assets to identify IS incidents covering relevant internal and external factors, including business and information system administrative functions; and
- Maintain and test detection processes and procedures to ensure timely and adequate awareness of IS incidents.

Respond

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

An FI should:

- Establish appropriate processes to ensure consistent and integrated 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[6];
- Establish procedures for reporting IS incidents, as appropriate; and
- Ensure effective crisis communication measures are in place during a disruption or emergency so that all relevant internal and external stakeholders, including external service providers, are informed in a timely and appropriate manner.

[6] See Appendix 1 for definition of “material incident”

Recover

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

An FI should:

- Develop an IS incident recovery plan, which should:
    - Focus on the impact on the operation of critical functions, processes, systems, transactions, and interdependencies,
    - Be documented and made available to the business and support units and readily accessible in case of emergency, and
    - Be updated in line with lessons learned from the tests, new risks identified, threats, and changed recovery objectives and priorities;
- Execute a recovery plan during or after an IS incident;
- Analyze IS incidents that have been identified or have occurred within and/or outside the organization, consider key lessons learned from these analyses, and update the risk management strategy accordingly;
- Conduct response and recovery planning and testing including with suppliers and third-party providers when applicable; and
- Develop and implement, for the purpose of ensuring the restoration of systems with minimum downtime and limited disruption, a backup policy specifying recovery methods, the scope of the data that is subject to the backup, and the minimum frequency of the backup based on the criticality of information or the sensitivity of the data.

Communication With The Regulator

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

The following expectation applies to PRFIs: In the event of a material incident, the PRFI should inform[7] BCFSA as soon as possible (see Appendix 1). Thereafter, as soon as possible but within 72 hours of a material incident, the PRFI should provide BCFSA with an incident report as described in Appendix 2.

[7] The initial contact with the BCFSA can be in the form of a phone call or email, and may include only a preliminary description of the information security incident and contain fewer details than outlined in the incident report (Appendix 2), since some information regarding the incident may not be available at the time.

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 PRFI and should relate to the impact that the incident will have on the PRFIs members, users, consumers, or the general public. In assessing the severity of a specific incident, the PRFI may want to consider the following factors, among others.

Is this an incident that:

a) Has been reported, or is reasonably expected to be reported, to the press or to the PRFI's members, users, or participating organizations with potential for a negative reputational impact?

b) Results in significant operational impacts to key/critical information systems or data?

c) Materially affects a PRFI's operational or customer data, including confidentiality, integrity, or availability of such data?

d) Has a significant operational impact on internal users that is material to clients or business operations?

e) Causes significant levels of system/service disruptions to critical business systems?

f) Is affecting a significant or growing number of customers[8]?

g) Will have a material impact on critical deadlines/obligations in financial market settlement or payment systems (e.g., financial market infrastructure, retiree payments)?

h) May have a significant impact on a third party?

i) Has been reported to other regulatory or other authorities?

[8] The term Customers includes, amongst others, depositors, policy holders and plan members.

MATERIAL INCIDENT EXAMPLES

Scenario Name	Scenario Description	Impact
Cyber Attack	An account takeover botnet campaign is targeting online services using new techniques, and current defenses are failing to prevent customer account compromise.	• High volume and velocity of attempts • Current controls are failing to block attack • Customers are locked out • Indication that accounts have been compromised
Service Availability & Recovery	There is a technology failure at a data centre.	• Critical online service is down and the alternate recovery option failed • Extended disruption to critical business systems and operations
Third Party Breach	A material third party's system is breached, and the PRFI is notified that the third party is investigating.	• Third party is designated as material to the PRFI • Material impact to PRFI data is possible
Extortion Threat	A PRFI has received an extortion message threatening to perpetrate a cyber-attack (e.g. Distributed Denial of Service attack unless a Bitcoin payment is received)	• Threat is credible • Probability of critical online service disruption
Internal Breach	An employee or contractor has intentionally or inadvertently caused sensitive data to be accessed destroyed, modified, or made inaccessible.	• Indications that accounts have been compromised.

Appendix 2: Information Security Incident Reporting Template

PRFIs should notify BCFSA in the event of a material incident as soon as possible. Thereafter, as soon as possible but within 72 hours after a material incident has occurred, PRFIs should provide BCFSA with a written incident report. Where specific details are unavailable at the time of the initial report, the PRFI should indicate 'information not yet available.' In such cases, the PRFI 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,
    - Known impact to one or more business segment, business unit, line of business or regions, including any third party involved,
    - Whether the incident originated at a third party or has an impact on third party services, and
    - Number of clients impacted;
- Primary method used to identify the incident;
- Current status of incident;
- Date for internal incident escalation to pension plan administrator, senior management or Board of Directors;
- Mitigation actions taken or planned;
- Known or suspected root cause; and
- Name and contact information for the PRFI incident lead and liaison with the BCFSA.

SUBSEQUENT REPORTING REQUIREMENTS

PRFIs 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, PRFIs should provide to BCFSA situation updates, including any short term and long-term remediation actions and plans.

Following incident containment, recovery, and closure, the PRFI 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