BCLibraries
COOPERATIVE

Privacy and Security Management Plan (PSMP)

Version 9 – February 3, 2016

Table of Contents

1. Introduction

A Privacy & Security Management Plan (PSMP) establishes requirements to ensure that security policies and practices remain current as business needs evolve and technology changes.

The BC Libraries Cooperative (CO-OP or The CO-OP) is a custodian of member and user information. Beginning in FY16/17, The CO-OP will implement this PSMP, providing an even more consistent degree of protection of information and technology resources.

This PSMP is based on the ISO 27002:2005[1] standard for information security management. This standard provides a structured approach to identifying the broad spectrum of information security activities in the life-cycle of information systems. The PSMP provides the framework to establish policies and procedures necessary for the protection of information and technology assets owned by, or in the care of, the CO-OP.

The policies herein incorporate a risk assessment approach to security that considers:

- Business process and CO-OP service delivery implications;
- Technological implications; and,
- Communications strategies including changes to personnel information security awareness programs.

The risk assessment approach herein enables:

- Compliance with legislative and policy objectives;
- Cost-effective allocation of resources based on a risk assessment;
- Responsible governance of CO-OP information assets; and,
- Secure provision of e-services to CO-OP members and customers.

2. Role of the Privacy & Security Management Plan

[1] Note that while the standard was updated in 2013, this version of the PSMP continues to reference the 2005 version. Bi-annual reviews of the PSMP commencing in 2018 will ensure continual adherence to the contemporary standard of the day.

On the difference between 2005 and 2013:

- "Perhaps the biggest difference between the old standard and the new one is the structure. ISO IEC 27002 2005 had 11 main sections (5 to 14) while ISO IEC 27002 2013 now has 14 (5 to 18). These new sections discuss cryptography, communications security, and supplier relationships (sections 10, 13, and 15 respectively). However, while the new standard has three more sections, it is in fact shorter and more focused than the old. The old standard had 106 pages of content while the new one has only 78." http://www.praxiom.com/iso-27002-old-new.htm
- "In our review, very little in the way of information security substance was changed in this version. While several controls were added and several more removed, the update is largely an exercise in moving and renumbering. The essential "key" controls are still required – they have just been moved to a different location." http://www.informationshield.com/security-policy/2013/11/iso-270022013-change-summary-heatmap/

The PSMP establishes requirements to ensure that security policies and practices remain current as business needs evolve and technology changes. This plan must be published and communicated to employees, members, customers and relevant external parties.

The PSMP contains operational policies, standards, guidelines and metrics intended to establish minimum requirements for the secure delivery of enterprise-wide services. Secure service delivery requires the assurance of confidentiality, integrity, and appropriate availability and privacy of the information assets in the custody or under the control of the CO-OP through:

- Management and business processes that include and enable security processes;
- Ongoing personnel awareness of security issues;
- Physical security requirements for information systems;
- Governance processes for information technology;
- Reporting information security events and weaknesses;
- Creating and maintaining business continuity plans; and,
- Monitoring for compliance.

The CO-OP recognizes that information security is a process, which to be effective, requires management commitment, the active participation of all personnel and ongoing awareness programs.

2.1. Privacy & Security Management Plan Review

The Executive Director's Office (EDO) is accountable for the PSMP. The EDO is responsible for ensuring information security policies, standards and guidelines are reviewed on a regular basis. Policies and standards review must be initiated:

- In conjunction with legislative, regulatory or policy changes which have information management implications;
- During planning and implementation of new or significantly changed technology;
- Following a Security Threat and Risk Assessment of major initiatives (e.g. new information systems or contracting arrangements);
- When audit reports or security risk and controls reviews identify high risk exposures involving information systems;
- If threat or vulnerability trends produced from automated monitoring processes indicate the probability of significantly increased risk;
- After receiving the final report of investigation into information security incidents;
- Prior to renewing third party access agreements which involve major programs or services of the CO-OP; and
- When industry, national or international standards for information security are introduced or significantly revised to address emerging business and technology issues.

2.2. Information Security Policies

The CO-OP has and will continue to develop, and/or implement information security policies that meet or exceed industry standards, and are reflective of the sensitivity of the information it owns or holds on behalf of members. The EDO must ensure that:

- Operational security policies are documented, implemented and reflected in employment and contractor agreements;
- A personal information security and privacy policy is documented, implemented and publicly available on the CO-OP website;
- The personal information security and privacy policy is reviewed at planned intervals and when significant changes occur, to ensure its continuing suitability, adequacy, and effectiveness;
- Employees, contractors and partners have easy access to the personal information security and privacy policy;
- Members, service providers and the public have access to information about the personal information security and privacy policy; and
- A network security infrastructure policy exists that includes a copy of the network diagrams of all enterprise applications.

3. Organizational Security

The protection of information assets requires a multi-disciplinary approach that is supported by the CO-OP information security organization. This section describes the management structure needed to coordinate privacy and information security activities including required information security activities, who coordinates them and what agreements are required. This coordination applies to internal teams and to external parties accessing or managing the organization's information assets.

The information privacy and security organization requires the support of a network of contacts in the information privacy and security community to elicit advice, identify trends and to deal with other external factors.

The PSMP provides the infrastructure necessary to protect The CO-OP's information assets and those of its members by:

- Establishing an information security architecture for standard security controls across the enterprise;
- Defining organizational roles and responsibilities for information security;
- Developing and reviewing specific information security policies;
- Monitoring and measuring the implementation of these policies; and,
- Developing and delivering a program to maintain privacy and security awareness.

3.1. Management Commitment & Assignment of Roles and Responsibilities

CO-OP management actively supports personal information privacy and security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of personal information privacy and security responsibilities. The CO-OP has appointed a Privacy & Security Officer (PSO).

The CO-OP's foundational documents include a Service Management Agreement (SMA) which specifies the processes for CO-OP governance and service delivery, and lays out general and joint responsibilities between the CO-OP and members with respect to privacy and security of corporate and personal information.

Operational privacy and security policies have been endorsed by CO-OP management and are communicated to staff and members. The EDO is responsible for ensuring that enterprise-wide policies, procedures, guidelines and standards have been defined and assigned. The CO-OP PSO is responsible for reviewing and updating security and privacy policies, procedures, guidelines and standards.

3.2. Privacy & Security Officer

The Privacy & Security Officer (PSO) must establish an Information Privacy and Security Program to manage and co-ordinate information privacy and security activities across the enterprise by:

- Providing leadership on methodologies and processes for information privacy and security;
- Identifying security controls required to enable secure service delivery and documenting those controls in the Privacy Security Management Plan, standards and guidelines;
- Providing security-related technical architecture advice to planning and development groups;
- Promoting information privacy and security education, training and awareness throughout the organization;
- Identifying significant threat changes and exposures to threats of assets associated with information security;
- Ensuring the Information Incident Management Process is followed for all suspected or actual information incidents;
- Evaluating information received during and after an information security incident;
- Implementing performance measurement processes for security controls;
- Ensuring information security activities are in compliance with the Information Security Policy;
- Identifying responses to remediate activities that are not in compliance with policies, standards or best practices;
- Co-ordinating the implementation of information security controls;
- Recommending appropriate actions in response to identified information privacy or security incidents and initiating audits where necessary; and,
- Building relationships with stakeholder and partner organizations including suppliers, partners and other security incident response centres to assist in maintaining the CO-OP Privacy Security Management Plan.

4. Asset Classification and Control

Information and information systems services constitute valuable resources. The asset management section establishes the blueprint to identify the rules of acceptable use and the rules for protection: what assets to protect, who protects them and how much protection is adequate.

This section sets the foundation for a system that classifies information to identify appropriate security levels, to specify how much protection is expected and how information should be handled at each level. Not all the information requires the same level of protection because only some information is sensitive or confidential.

4.1. Documenting and maintaining asset inventories

The CO-OP must document, maintain and verify asset inventories on a regular basis, depending on the criticality and value of the assets, and validate the measures taken to protect the assets as part of an enterprise risk management strategy.

The following information should be recorded to facilitate system planning and asset recovery in the case of interruption, corruption, loss or destruction:

- Type of asset;
- Ownership;
- Format;
- Location;
- Back-up information and location;
- License information;
- Sensitivity and safeguards requirements;
- Criticality for service delivery and maintaining business functions; and
- Consequences of loss.

The EDO is accountable for asset identification and inventory maintenance.

4.2. Loss, theft or misappropriation of assets

The loss, theft or misappropriation of assets must be reported immediately to the EDO and PSO. Where the loss, theft or misappropriation involves information, the Information Incident Management Process must be followed (see section 10.3).

4.3. Information and information system security classification

The EDO must ensure a valid and consistent information classification system is used to categorize information and information systems.

A valid and consistent information security classification must:

- Apply to information types rather than discrete data elements;
- Determine the relative value of information including factors such as:
    - Compatibility with member-driven requirements,
    - Statutory or regulatory requirements,
    - Impact to health and well being or personal safety,
    - Impact on other information or information systems,
    - Economic impact from loss of information,
    - Effects of data aggregation,
    - Cost to create or replace the information,
    - Impact to the CO-OP business plan from loss of information confidentiality, integrity and availability,
    - Changes to information sensitivity over time; and
    - Maintain compatibility with CO-OP policies on information retention and disposition.

The Information Security Classification determination includes:

- Defining information types for categorization;
- Making decisions on categorization of information; and,

- Periodic reassessment of the information security categorization processes.

The CO-OP has adopted the following categories of information:

1. *Class One*:
   Personal information (PI) that must be protected in accordance with the Freedom of Information and Protection of Privacy Act in effect in the Province of British Columbia;
2. *Class Two*:
   User access credentials (usernames, passwords, biological credentials, etc.) must be protected with encryption and logical controls to prevent unauthorized access, use or disclosure; and
3. *Class Three*:
   All other information, including confidential business information of The CO-OP and its members must be protected in accordance with its sensitivity as determined by the EDO in consultation with the PSO and business and member partners.

5. Personnel Security

Training must be conducted for all employees, data custodians, information managers, contractors and management to ensure they are aware of and understand:

- The value of information as an asset;
- Their privacy and security responsibilities;
- Security policies and practices;
- Permitted access, use and disclosure of personal and corporate information;
- Information retention and disposal policies; and
- Requirements for password maintenance and proper password security

Registration, attendance and training session performance evaluations, if indicated, are recorded. Privacy and security training is refreshed periodically.

5.1. Confidentiality and Non-disclosure Agreements

CO-OP staff may have access to confidential business or personal information as part of their duties. To help ensure the security of such information, the PSO must ensure:

- Employees, contractors, data custodians and information managers must sign a Confidentiality Agreement, Non-disclosure Agreement or both as the case may be; and
- The Confidentiality Agreement and the Non-disclosure Agreement clearly define individual's responsibilities for security.

5.2. Hiring and Terminations

The PSO must ensure that:

- Potential employees who will have access to personal information held by The CO-OP are adequately and appropriately screened, including reference and background checks as appropriate; and
- A process has been implemented to ensure immediate recovery of keys and pass cards and the revocation of access privileges and appropriate notification of security personnel when a termination (voluntary or involuntary) occurs.

5.3. Contractors and Third Parties

The PSO must ensure that:

- Private sector organizations and individuals who have access to personal information held by the CO-OP are adequately and appropriately screened;
- Necessary security requirements are specified in contractual documentation with contractors and third parties;
- All contracts that may involve access to personal information must contain a privacy protection schedule requiring, at a minimum, compliance with BC's FIPPA legislation and the standards for security controls contained therein;
- Contractors are required to comply with the organization's privacy and security policies or equivalent policies to ensure that contractors are bound by the same standards as the organization;
- Contractors and other third parties are required to return personal information to the contracting organization upon completion of the contract or as otherwise directed; and
- If Contractors and other third parties are not required to return personal information, Contractors and other third parties are required to securely destroy, using an approved method, the personal information at the completion of the contract.

6. Physical and Environmental Security

This section identifies requirements for the protection from environmental and man-made threats to personnel and property in information processing facilities (data centres). A primary measure is the use of security zones to place computers, people and information in secure areas. Requirements for the installation, operation, protection and maintenance of computer equipment are identified to preserve the confidentiality, integrity and availability of information and information systems.

Appropriate security controls must be applied to reduce the level of identified risks and include:

- A structure that prevents external visual and audio observations and complies with all local building codes for structural stability (external walls, internal walls, ceilings and doors). Walls surrounding the facility must be extended from true floor to true ceiling (slab to slab), to prevent unauthorized entry and minimize environmental contaminations such as that caused by fires and floods. Appropriate control mechanisms (e.g., locks, alarms and bars on windows and doors) must be applied to prevent unauthorized access;
- All information processing facilities must be equipped with physical intrusion alarm systems that automatically alert monitoring staff to take immediate action;
- Information processing facilities must be equipped with doors that close automatically and must set off an audible alarm when kept open beyond a certain period of time;
- All fire doors must be equipped with crash bars to allow a quick exit in the event of an emergency. When the doors are opened an audible alarm may also be set off;
- Alarm systems must be continuously monitored (i.e. 24 hours a day, 7 days a week); and
- Access to restricted zones must be controlled, authorized and monitored as required by the applicable zone.

6.1. Security Perimeter

The following guidelines support physical and environmental security by establishing perimeter security for information processing facilities (data centres):

- Common service spaces such as eating areas, washrooms, cloakrooms, boardrooms and storage areas should be located so that they cannot be used to circumvent physical security;
- Visitor reception should be separate from entrance areas but provide an unobstructed view of the entrance; and
- When physical security is outsourced, the contract must require that contracted personnel are security screened and bonded.

6.2. Restricted Access Zones

The effective use of restricted access zones in an open office environment depends on the implementation of appropriate security procedures, which may include:

- Respecting the need-to-access principle and zone perimeters;
- Escorting visitors;
- Securing sensitive or valuable information and assets when leaving the work areas; and
- Taking precautions when discussing sensitive information.

6.3. Entry Controls

Access to any information processing facility (data centre) must be restricted. Entry controls must identify, authenticate and monitor all access attempts to a Restricted Access Operations Zone or a Restricted Access Security Zone as follows:

- Every person authorized to enter a facility including visitors must be issued with an identification badge that contains identifying information (such as name and photograph) and their level of building access. Badge colour or some other bold identifier may be used to represent the level of access;
- All badges must be checked prior to entry. A receptionist, security guard or electronic reader that logs the identity, time, date, and access privileges of each entry attempt must do such checking. Entry control may be achieved using keys, proximity card readers or other technologies;
- Personnel must challenge anyone in a secure area who is not displaying an identification badge;
- Visitor or temporary access badges must be returned and accounted for at the end of each day;
- Entry logs must be reviewed on a regular basis;
- All entry logs must be secured and maintained according to a records retention schedule approved by the PSO for the system or information asset;
- Activities within a secure area are confidential and must not be discussed in a non-secure area, or with persons who do not have a need-to-know;
- Sensitive information must not be discussed with persons without a need-to-know;
- No type of photographic (including cameras in mobile devices), video, audio or other recording equipment is to be brought into the Secure Data Centre unless authorized; and
- Access rights to secure areas and entry controls must be reviewed and updated regularly.

Unoccupied secure areas must be physically locked and periodically checked. Physical intrusion alarms must be installed to automatically alert monitoring staff of a breach.

6.4. Controlling access to delivery and loading areas – Secure Data Centre

Information custodians, planners and architects must ensure that access to delivery and loading areas or Reception Zone is controlled when considering building design and specifications. The following factors must be considered:

- A combination of internal and external locking doors or gates must be used to provide security;
- Incoming material must be inspected for potential threats before being moved to or from the delivery and loading area. Inspections can be undertaken randomly if resources are not available to inspect every package;
- Bills of lading must be compared to goods delivered;
- Loading docks and delivery areas must be regularly inspected and actively monitored; and
- Records must be kept for deliveries and pick-ups.

For leased facilities that include delivery and loading areas, an inspection prior to leasing should be conducted to determine that access can be adequately controlled.

6.5. Security controls for co-located information processing facilities and loading areas

When delivery and loading areas are not separate from information processing facilities or other secure areas the following security controls shall be considered:

- Physical controls (e.g., locked doors) that secure the external doors of a delivery and loading area when the internal doors are opened;
- Setting and maintaining hours of operation for delivery and pick-up;
- Continuous monitoring of the access to information processing facilities;
- Continuous monitoring of the delivery and loading areas; and
- Records must be kept for deliveries and pick-ups.

6.6. Equipment location

The design and layout of information processing facilities (data centres) must provide protection from security threats including:

- Locating servers and other centralized computing equipment within a Restricted Access Security Zone;
- Locating work stations, laptops and printers in an Restricted Access Operations Zone;
- Protecting information processing equipment from observation by unauthorized persons, including by observing through windows and walking through work areas; and
- Locating shared printers, scanners, copiers, and facsimile machines away from public or reception areas, or in passageways or other areas where users who do not have a need-to-know can access printed material.

6.7. Equipment protection

Design and layout of information processing facilities (data centres) provides protection from physical and environmental hazards, including:

- Ensuring that equipment is properly vented and that the temperatures and humidity in information processing facilities are appropriate for operating equipment safely;
- Ensuring lightning protection for information processing facilities which includes surge protection for power and communications;
- Assessing and protecting equipment to minimize damage from fire suppression and other safety systems;
- Protecting equipment from potential damage from environmental hazards such as water, dust, vibration, and sunlight;
- Providing personnel with approved eating and drinking areas separate from work areas containing equipment;
- Briefing personnel who work with equipment about safety practices in the workplace;
- Keeping information processing facilities free of biological pests that pose hazards to equipment and power systems; and
- Inspecting regularly the information processing facility(s) for integrity of ceilings, walls, windows, and other infrastructure for damage from water and other environmental factors that may pose a threat to safe equipment operation.

In addition to meeting the building code and other regulations, the following shall be included in facility specifications:

- Uninterruptible power supply, back-up generators, and fuel, as required by business and technical requirements;
- Emergency power off switches located near emergency exits in equipment rooms;
- Emergency lighting;
- Alarms to indicate inadequate water pressure for fire suppression;
- Alarms to indicate malfunctions in heating, ventilation, air conditioning, humidity control and sewage systems;
- Multiple connections to the power utility for critical systems and equipment;
- Multiple telecommunications connections to prevent loss of voice services; and
- Adequate voice communications to meet regulatory requirements for emergencies.

6.8. Equipment Security Controls

Equipment must be protected using documented security controls when off-site from The CO-OP premises.

Such controls ensure that:

- Sensitive data is encrypted where necessary to prevent unauthorized access or disclosure;
- Equipment is protected from unauthorized access by the use of a logical or physical access control mechanism (e.g., password, USB key or smart card);
- Equipment is protected from loss with a physical locking, restraint or security mechanism when appropriate; and
- Personnel are familiar with operation of the protection technologies in use.

To provide further protection personnel must:

- Not leave equipment unattended in a public place;
- Ensure that equipment is under their direct control at all times when travelling;
- Take measures to prevent viewing of sensitive information other than by authorized persons;
- Not permit other persons to use the equipment; and
- Report loss of equipment immediately to the PSO.

6.9. Destruction of hardware

The PSO is responsible for ensuring hardware media used to store information or software is destroyed in a secure manner. Warranty repairs or servicing for hardware used to store information or software must be sent to an approved site in a secure manner. Hardware must be destroyed if the integrity of the information cannot be ensured during warranty repairs and servicing, e.g., work done outside Canada.

Equipment, information or software belonging to The CO-OP, its members or customers must not be removed from CO-OP premises without prior authorization.

7. Communications and Operations Management

This section establishes a framework to support the integration of information security in the services provided by CO-OP information processing facilities. Planning and management of the day-to-day activities is required to ensure the availability and capacity of information service resources. This framework identifies requirements to control and monitor operations for service delivery and to manage changes as the operations evolve.

Controls for operations include documented processes, staff duties and formal methods to implement changes to facilities. This includes: methods to protect information, create copies for back-up, and to manage the media where those copies are stored. Network protection requirements from threats such as viruses or unauthorized disclosure are also described.

7.1. Operating procedures

Systems administrators must ensure that approved operating procedures and standards are:

- Documented;
- Consistent with industry standards; and
- Reviewed and updated as indicated;

Reviewed and updated when there are:

- Alterations to building layouts,
- Changes to equipment/systems located in the facility, and
- Changes in business services and the supporting information systems operations; and,
- Reviewed and updated as part of any related security incident investigation.

Operations documentation must contain adequate instructions regarding:

- Information processing and handling;
- System re-start and recovery;
- Back-up and recovery, including on-site and off-site storage;

- Exceptions handling, including a log of exceptions;
- Output and media handling, including secure disposal or destruction;
- Audit and system log management;
- Change management including scheduled maintenance and interdependencies;
- Computer room management and safety;
- Information Incident Management Process;
- Disaster recovery;
- Business continuity; and
- Operations, technical, emergency and business contacts.

7.2. Segregation of duty

The CO-OP will reduce the risk of disruption of information systems by:

- Requiring complete and accurate documentation for every information system;
- Automating functions to reduce the reliance on human intervention for information systems;
- Requiring that individuals authorized to conduct sensitive operations do not audit those operations;
- Requiring that individuals responsible for initiating an action are not also responsible for authorizing that action, where possible and practicable in a non-profit corporate structure with limited staffing; and
- Implementing information systems security controls to minimize opportunities for collusion.

7.3. Separation requirements

The Systems Administrator(s) must protect operational information systems by:

- Separating operational environments from test and development environments using different servers, domains and partitions;
- Preventing the use of test and development identities and credentials for operational information systems;
- Using approved change management processes for promoting software from development/test to operational information systems; and
- Prohibiting the use of personal information in development, test or training information systems.

7.4. Identifying security requirements in procurement documents

The CO-OP must include security requirements in procurement documents for information and information system services being delivered by external parties. Security requirements must be documented when:

- Drafting procurement documents (e.g., Request for Information, Request for Proposal);
- Evaluating bids to confirm acknowledgement and capability;
- Preparing agreements or contracts; and
- Developing transition and fall-back plans (e.g., migration from one service provider to another).

7.5. Service level continuity

The PSO must ensure that service agreements with external parties document service level continuity requirements and include processes for:

- Ongoing review of service level needs with business process areas;
- Audit and compliance monitoring rights and responsibilities;
- Communicating requirements to service providers;
- Obtaining periodic confirmation from service providers that adequate capacity is maintained; and
- Reviewing the adequacy of the service provider’s contingency plans for responding to disasters or major service failures.

7.6. Monitoring and review of external party services

For all services that pertain to member-facing services, the PSO must establish processes to manage and review the information security practices of external party delivered services by:

- Assigning responsibility for monitoring to a designated staff member;
- Maintaining an inventory of agreements and associated access rights;
- Monitoring for compliance through processes such as:
  - Conducting internal self assessments of control processes,
  - Requiring external parties conduct and submit self assessments,
  - Requiring external parties to submit to management assertions that controls are being adhered to,
  - Conducting independent security reviews, audits and updates to risk and controls reviews,
  - Analysis of audit logs, and,
  - Establishing a process, jointly with the service provider, to monitor, evaluate, investigate and remediate incidents.

7.7. Change Management

Acceptance criteria for new information systems, upgrades and new versions must be established and suitable tests of the systems carried out prior to acceptance.

The PSO must ensure that definitions of system acceptance criteria are included as part of the system development and acquisition process. Prior to implementing new or upgraded information systems, the PSO must ensure acceptance criteria are identified and confirmed, including:

- Projected performance and resource capacity requirements;
- Disaster recovery, restart, and contingency plans and procedures;
- Impact on standardized routine operating procedures and manual procedures;
- Implementation of security controls;
- Statutory privacy compliance;
- Assurance that installation of the new system will not adversely affect existing systems, particularly at peak processing times;
- Business continuity arrangements; and
- Training requirements.

7.8. Protection against malicious code

The PSO must ensure that security awareness, prevention and detection controls are utilized to protect information systems against malicious code, including such activities as:

- Installing, updating and consistently using software (e.g., anti-virus or anti-spyware software) designed to scan for, detect and provide protection from malicious code;
- Prohibiting the use of unauthorized software;
- Checking files, including electronic mail attachments and file downloads for malicious code before use;
- Maintaining business continuity plans to recover from malicious code incidents; and
- Employing specific malicious code countermeasures (e.g., blocked websites, blocked electronic mail attachment file types and blocked network ports).

7.9. Restrictions on mobile code

The PSO must establish methods to restrict or contain mobile code that include:

- Compartmentalization of mobile code execution to a logically isolated environment; and
- Restricting system resources available to the mobile code.

User systems must be configured to warn users of mobile code risks and prompt them to consider risks prior to opening files or e-mail attachments that may contain mobile code. Mobile code authored by CO-OP staff must be:

- Digitally signed;
- Published on an authorized, trustable source; and
- Transmitted to users systems over encrypted channels

7.10. Communications and Operations Management – Back-up

Systems Administrators must define and document backup and recovery processes that reflect the security classification and availability requirements of information and information systems including:

- Confirming that the backup and recovery strategy complies with:
    - Business continuity plans; and
    - Policy, regulatory and other legal obligations.

Systems Administrators must document the backup and recovery processes including:

- Types of information to be backed up;
- Schedules for the backup of information and information systems;
- Backup media management (e.g., retention period, pattern of backup cycles);
- Methods for performing, validating and labelling backups; and
- Methods for validating recovery of the information and information system.

7.11. Safeguarding backup facilities and media

Systems Administrators must ensure safeguards for backup facilities and media that are commensurate with the value and sensitivity of the information and information systems. Safeguards include:

- Using encryption to protect the backed up information;
- Using digital signatures to protect the integrity of the information;

- Physical and environmental security;
- Access controls;
- Methods of transit to and from offsite locations (e.g., by authorized couriers, via entrusted employees, by encrypted electronic transfer);
- Storage of media adhering to manufacturer recommendations for storage conditions and maximum shelf-life; and
- Remote storage of backup media at a sufficient distance to escape any damage from a disaster at the main site.

Systems Administrators must ensure regularly test backup and recovery processes.

7.12. Network security management

The CO-OP must implement network infrastructure security controls and security management systems for networks to ensure the protection of information and attached information systems.

Selection of controls must be based on a reasonable assessment of risk, taking into account the information security classification determined by the EDO in conjunction with the PSO and information owners, and applicability to the network technology.

The risk assessment must consider network-related assets which require protection including:

- Information in transit;
- Stored information (e.g., cached content, temporary files);
- Network infrastructure;
- Network configuration information, including device configuration, access control definitions, routing information, passwords and cryptographic keys;
- Network management information;
- Network pathways and routes;
- Network resources such as bandwidth;
- Network security boundaries and perimeters; and
- Information system interfaces to networks.

7.13. Configuration control

To maintain the integrity of networks, Systems Administrators must manage and control changes to network device configuration information such as configuration data, access control definitions, routing information and passwords. Network device configuration data must be protected from unauthorized access, modification, misuse or loss by the use of controls such as:

- Encryption;
- Access controls and multi-factor authentication;
- Monitoring of access;
- Configuration change logs;
- Configuration baselines protected by cryptographic checksums; and
- Regular backups.

Status accounting must be regularly performed to ensure that configuration baselines reflect actual device configuration.

7.14. Secured path

Where required by information classification and security threat and risk assessment, information must only be transmitted using a secured path. Secured paths for information transmission must use controls such as:

- Data, message or session encryption, such as SSH, SSL or VPN tunnels; and,
- Systems to detect tampering.

7.15. Wireless Local Area Networking

Wireless Local Area Networks must utilize the controls specified by the Systems Administrators and must include:

- Strong link layer encryption, such as Wi-Fi Protected Access;
- User and device network access controlled by Cooperative authentication services;
- The use of strong encryption keys and passwords;
- Segregation of wireless networks from wired networks by the use of filters, firewalls or proxies; and

7.16. Equipment management

The EDO must document responsibilities and procedures for operational management of network infrastructure, including devices at network boundaries and in user areas.

Logging, monitoring and detection

To facilitate monitoring, response and investigation, logging to a centralized log management service must be enabled, including logging of:

- Security-relevant events on network devices; and
- Security-relevant events on systems that provide authentication and authorization services to network infrastructure devices such as routers, firewalls or switches.

Logs must be reviewed to security events and intrusions.

- Active automated surveillance of networks must be implemented to detect and report on security events (e.g., network intrusion detection systems).
- Sensors enabling on-demand capture of network traffic must be implemented at network security boundaries and within networks housing sensitive information or information systems if indicated by a reasonable assessment of risk.

7.17. Network service agreement

Formal network service agreements must be established between network service providers and consumers of network services to specify service levels, services offered, security requirements and security features of network services. Network service agreement must include specification of:

- The rules of use to be followed by consumers of service to maintain the security of network services;
- The schedule for ongoing verification of network security controls;
- The rights of either party to monitor, audit or investigate as needed;
- Security incident response responsibilities, contacts and procedures; and
- The requirement to meet or exceed industry security policy and standards.

The PSO must confirm that the specified security features are implemented prior to commencement of service delivery.

7.18. Media handling – portable devices

All removable computer media must be managed with controls appropriate for the sensitivity of the data contained on the media. The use of portable storage devices to store or transport information increases the risk of information compromise. Portable storage devices are typically small, portable and are easily lost, stolen or damaged, particularly when transported in public environments.

The PSO must:

- Ensure that use of portable storage devices is managed and controlled to mitigate risks;
- Document processes for authorizing use of portable storage devices; and
- Ensure personnel using portable storage devices protect information and information technology assets in their custody or control.

7.19. Portable Devices – Human factors

The PSO must ensure personnel using portable storage devices are:

- Aware of the additional risks and responsibilities inherent with portable storage devices;
- Familiar with operation of the required protection technologies and when they must be used; and
- Familiar with security event and loss reporting procedures.

8. Access Control

This section identifies the mechanisms that restrict access to CO-OP information assets and the information assets it manages on behalf of members and customers. Access restrictions protect organizations from security threats such as internal and external intrusions. The restrictions are guided by legislation that protects particular types of information (e.g., personal information and sensitive business information). Mechanisms for access control include password management, user authentication and user permissions.

Access control policies provide the blueprint for the management of user access, authorizations and control mechanisms for computer networks, operating systems, applications and information. This section identifies security best practices and responsibilities for management and staff.

8.1. Access control policy

The PSO responsible for establishing, documenting and approving access control policies which must:

- Support and enable business requirements identified in Security Risk Assessments or Privacy Impact Assessments;
- Be based upon a reasonable assessment of risk; and
- Include classification of assets.

Access control policies must additionally:

- Consider both physical and logical access to assets;
- Apply the "need to know" and "least privilege" principles; and
- Have permissions assigned to roles rather than individual user identifiers.

8.2. Access control policy management

The PSO is responsible for establishing processes to manage the access control policies, including:

- Ensuring the process is communicated to all personnel;
- Identifying roles and/or functions which require multi factor authentication; and,
- Identifying and justifying exceptional cases where there is a need for enhanced personnel security screening for sensitive assets.

8.3. Review of access control policy

The PSO must conduct periodic reviews of the access control policy as part of an ongoing process for risk management, security, and privacy. Reviews must be conducted:

- Annually or at such regular periods as deemed reasonable by the PSO;
- Prior to the introduction of new or significantly changed systems, applications or other services or major technology changes; and
- When the threat environment changes or new vulnerabilities arise.

8.4. User Access Management – Registration

The EDO is responsible for managing access to the assets under CO-OP control and must implement registration processes which require approval of all access rights. This process should:

- Ensure access requests are approved by the supervisor/manager of the user requesting access;
- Ensure the reasons for requesting access are consistent with job responsibilities;
- Ensure personnel understand the conditions of access and, when appropriate, have signed confidentiality agreements;
- Ensure access rights are consistent with the data uses documented in the approved Privacy Impact Assessment and Security Access Matrix;
- Ensure accesses are traceable to an identifiable individual or process; and
- Ensure each user is assigned a single unique identifier for accessing information systems unless multiple identifiers are required to meet unique business requirements provided the rationale is documented and approved by the PSO as appropriate.

8.5. Managing, restricting and controlling the allocation and use of system privileges

The PSO is responsible for authorizing system privileges and must:

- Identify the system privileges associated with each information system or service;
- Ensure the process for requesting and approving access to system privileges includes management approval(s) prior to granting of system privileges;
- Ensure processes are implemented to remove system privileges from users concurrent with changes in job status (e.g., transfer, promotion, termination);

- Limit access to the fewest number of users needed to operate or maintain the system or service;
- Ensure the access rights granted are limited to and consistent with the users' job function and responsibilities;
- Maintain a record of users granted access to system privileges;
- Ensure use of system privileges is recorded in audit logs which are unalterable by the privileged user; and
- Ensure user identifiers with system privileges must only be used for performing privileged functions and not used to perform regular activities. User identifiers established to perform regular activities must not be used to perform privileged functions.

8.6. Access Control – Passwords

When selecting passwords users must select complex passwords, i.e., a mixture of characters as specified in the Standard. The effectiveness of access control measures is strengthened when users adopt good security practices for selecting passwords.

Passwords must be changed:

- During installation of computer hardware and or software which is delivered with a default password;
- Immediately if a password is compromised or if compromise is suspected. If compromise has taken place or is suspected the incident must be reported to the EDO and PSO and,
- Comply with password change instructions issued by an automated process (e.g., password lifecycle replacement) or an appropriate authority.

8.7. Privileged accounts

Privileged accounts have wider and more powerful access rights to information assets. In addition to the requirements above, users authorized to create or who hold privileged accounts must use public key encryption over secure shell to access servers, which ensures only machines with the matching private key are allowed to connect to servers.

8.8. Protection and use of passwords

Passwords are highly sensitive and must be protected by not:

- Sharing or disclosing passwords;
- Permitting anyone to view the password as it is being entered;
- Writing down a password;
- Storing other personal identifiers, access codes, tokens or passwords in the same container as the token;
- Keeping a file of passwords on any computer system, including Personal Digital Assistants, BlackBerry®, iPhone® and other similar devices; and
- Employing any automatic or scripted logon processes for personal identifiers; and
- Not using personal identifiers, access codes, or passwords associated with CO-OP accounts for personal or other purposes.

8.9. Passwords Standards

The Password Standard for CO-OP systems requires that passwords:

- Contain a minimum of 7 characters;
- Contain characters from three of the following categories:
    - English upper case characters (A to Z), numerals (0 to 9), and lower case characters (a to z)
    - Non-alphanumeric keyboard symbols (e.g., ! $ # %).

For example, the complex password “T#ocitpi7”is derived from the phrase “The number of clowns in the parade is seven”. Complexity can be further increased by substituting numbers for vowels.

8.10. Protection of unattended equipment

The PSO must ensure that users prevent unauthorized access to information systems by securing unattended equipment. Measures include:

- Locking or terminating information system sessions before leaving the equipment unattended;
- Enabling a password protection features on the equipment (e.g., screen savers on workstations);
- Shutting down and restarting unattended workstations at the end of each workday;
- Enabling password protection on mobile devices including portable storage devices; and
- Being aware of their responsibility to report security weaknesses where the above controls have not been applied.

8.11. Access Control – Network access control

Users must only be provided access to the information systems they have been specifically authorized to use. Controls must enable only those network services needed to support business requirements (e.g., by explicitly enabling needed services and disabling unneeded services). Access to network services will be controlled at network perimeters, routers, gateways, workstations and servers.

Information system network access must be restricted to the authorized users and systems, using the principle of least privilege, as defined in the access control policies for the information system. The relevant portions of the access control policy must be communicated to personnel as part of awareness training.

8.12. Remote access to Cooperative networks or services

In providing remote network access services for CO-OP members and employees, the PSO must:

- Conduct a reasonable assessment of risk for each remote access service to determine the authentication methods to be implemented;
- Require remote users to connect through designated remote access services or security gateways; and
- Require user identification and authorization prior to permitting each remote network connection.

Automatic equipment identification must be used, as appropriate, to authenticate connections from specific locations and equipment.

8.13. Protection of diagnostic ports

Physical and logical access to diagnostic ports must be securely controlled. The PSO must implement access control processes for the physical and logical access controls of the ports, services and systems for diagnostic, maintenance and monitoring activities to prevent bypassing of information system access controls.

Physical and logical access controls to be considered for implementation include: physical locks, locking cabinets, access control lists and filters, network filters and user authentication systems. Diagnostic ports must be kept inactive until needed, and kept active for the minimum time required.

Access to diagnostic ports from remote locations, or by external parties, or service providers must be authorized by agreements, contracts and conditions of use. Use of diagnostic ports must be logged and monitored for suspicious activity.

Security Access Matrices are documented, implemented and used to grant and control access to the CO-OP enterprise environment.

8.14. Segregation based on risk and requirements

Systems Administrators must segregate services, information systems and users to support business requirements for information system connectivity and access control based on the principles of least privilege, management of risk and segregation of duties. Segregation is used to isolate information systems, users and networks based on risk and business connectivity requirements to control information flow, minimize unauthorized connection attempts and limit the spread of damage in case of compromise.

Systems Administrators must establish network perimeters and control traffic flow between networks. Network traffic flow control points such as firewalls, routers, switches, security gateways, VPN gateways or proxy servers must be implemented at multiple points throughout the network to provide the required level of control.

The techniques and technologies selected for network segregation must be based on a reasonable assessment of risk. Factors to consider include:

- The information and information system security classification;
- The trustworthiness of the network, based on the amount of uncontrolled malicious traffic present, the level of device identification and authentication in the networks and sensitivity to eavesdropping (e.g., the Internet is a less trusted network than a controlled server network zone);
- Transparency, usability and management costs of network segregation technologies; and
- The availability of compensating controls for detection, prevention and correction of malicious network traffic and unauthorized access attempts.

8.15. Logical and physical network connection control

The connection capability of users must be restricted in shared networks in accordance with the access control policy of the information system. Systems Administrators must restrict the ability of users to physically and logically connect to networks according to the access control policy. Techniques may include:

- Physical cabling protection;
- Physical control of network ports in public areas and meeting rooms;
- Segregated networks for unauthenticated devices;
- User and device authentication prior to issuing network addresses;
- Router access control lists;
- Scanning for unauthorized network equipment (e.g., unauthorized wireless access points, modems); and
- Virtual LANs.

Direct network connections to information systems must only be permitted if required for information system function. For example, database server hardware should be placed in a network security zone to segregate it from direct network connections by user workstations.

8.16. Wireless networks

Systems Administrators must prevent unauthorized connection to wireless networks through use of identification and authentication techniques as determined by a reasonable assessment of risk.

8.17. Network address control - routing

Systems Administrators must implement mechanisms to prevent network address spoofing and routing of spoofed network traffic (e.g., through use of router access control lists). Security gateways must be considered for network access control points, in accordance with information system security classification requirements. Gateways may be used to validate source and destination addresses when proxy servers or network address translation are used with secondary identity verification techniques (e.g., user identifier and password, digital certificates).

Systems Administrators must implement processes and controls to prevent unauthorized access to, or tampering of, network routing information (e.g., through use of encryption, authenticated routing protocols, access control lists). Server side 128 bit Secure Socket Layer encryption is enabled for the user's connection to secure portions of the CO-OP's enterprise environment, including Sitka.

8.18. Information displayed during logon

The PSO must ensure logon processes are configured to minimize the opportunity for unauthorized access. This includes:

- Not displaying details about backend systems (e.g., operating system information, network details) prior to successful completion of the logon process to avoid providing an unauthorized user with any unnecessary assistance;
- Displaying a general warning notice that the Information System be accessed only by authorized users;

- Validating logon information only on completion of all input data; and
- Not displaying passwords in clear text as they are entered.

8.19. Unsuccessful logon attempts

The PSO must ensure logon processes are configured to:

- Record unsuccessful logon attempts;
- Allow a limited number of unsuccessful logon attempts;
- Limit the maximum and minimum time allowed for the logon procedure. If exceeded, the system should terminate the logon; and
- Force a time delay or reject further logon attempts if the limited number of consecutive unsuccessful logon attempts is reached.

8.20. Allocation of unique identifier

The PSO must ensure users are issued unique user identifiers (userIDs) for their use only. The documented and approved process for allocating and managing unique identifiers must include:

- A single point of contact to:
  - manage the assignment and issuance of user identifiers,
  - ensure that users, except for privileged users, are not issued multiple identifiers for any one information system or platform, and
  - record user status (e.g., employee, contractor);
- Identify those individuals or positions authorized to request new user identifiers;
- Confirm that the user has been informed of appropriate use policies;
- Ensure terminations and extended leave actions are coordinated with initiation, suspension or cancellation of user identifiers;
- Maintain the status of identifiers issued to contractors; and
- Conduct annual reviews to confirm the continued requirement for the user identifier.

To segregate roles or functions, privileged users may be issued multiple identifiers for an information system or platform.

The PSO must ensure that user identifiers are authenticated by an approved authentication mechanism.

User identifiers authenticated by means other than a password must use a mechanism approved by the PSO.

8.21. Shared user identifiers

In highly exceptional circumstances, where there is a clear business benefit identified by the PSO, the use of a positional user identifier for a group of users or a specific job can be used, provided:

- Positional user identifiers are not used for privileged users; and
- The Manager responsible for the position using the positional user identifier:
  - Maintains a record of the name of the individual, the user identifier, and the start- and end-date of use, and,
  - Deactivates the user identifier when not in use by requesting a password reset.

8.22. Restriction and control of system utility programs

The PSO must limit use of system utility programs by:

- Defining and documenting authorization levels;
- Restricting the number of users with access to system utility programs;
- Regularly reviewing the status of users with permissions to use system utility programs;
- Ensuring that the use of system utilities maintains segregation of duties;
- Ensuring that all system utility programs are identified and usage logged;
- Segregating system utilities from application software where possible; and
- Removing or disabling unnecessary and obsolete system utilities and system software.

8.23. Session time-out

The PSO must define and implement automatic termination or re-authentication of active sessions after a pre-determined period of inactivity.

CO-OP information systems must have session time-outs managed by operating system access, application or CO-OP infrastructure controls. Application and network sessions must be terminated or require re-authentication after a pre-defined period of inactivity commensurate with the:

- Risks related to the security zone;
- Classification of the information being handled; and
- Risks related to the use of the equipment by multiple users.

8.24. Access Control – Mobile computing and teleworking

The use of portable storage devices such as laptops, BlackBerry®, iPhone® devices or Personal Digital Assistants to access, store, or process information increases the risk of information compromise.

Users of mobile computing services must ensure that information and information technology assets in their custody or control are protected. In particular, users must protect against visual eavesdropping of passwords, PINs and other credentials, especially when in public places.

8.25. Protection of network endpoint and physical devices

Portable storage devices are typically used to store information or remotely access CO-OP networks and services. The policies and procedures governing remote access apply to mobile devices. Where Remote Access services are used, the portable storage device must be configured to prevent its use as a conduit between the CO-OP and non-CO-OP networks (e.g., VPN split tunnelling must be disabled).

Network access to portable storage devices from networks not managed by the CO-OP must be blocked by implementation of firewall or filtering technologies to protect against attack (e.g., to prevent network attacks against the mobile device).

Portable storage devices must be protected against mobile and malicious code and must be locked and/or secured when unattended to prevent unauthorized use or theft (e.g., use device locks, cable locks, physical container locks, PINs or screensaver locks).

8.26. Bring Your Own Device (BYOD) / distributed workforce security controls to ensure that information resources are not compromised.

The PSO must ensure that CO-OP information and information technology assets are adequately protected by implementing security controls supported by a reasonable assessment of risk. The risk assessment must consider:

- The sensitivity of information that may be accessed or stored at remote locations;
- The physical security of information and information technology assets;
- Unauthorized information access by people at remote locations, either inadvertent or deliberate; and
- Remote access threats if remote access is utilized.

Security controls that must be considered include:

- Restriction of permitted information types and classifications at remote locations;
- Provision of CO-OP-managed equipment, if appropriate, due to information sensitivity or volume;
- Provision of locking cabinets, shredders and other physical security equipment;
- Encryption of data, where indicated, when stored at remote locations;
- Security awareness training for protection of information and information assets, including clear desk policy, information handling rules, physical security issues and remote access training; and
- Monitoring and review of BYOD equipment for security events and incident response.

8.27. BYOD, distributed workforce context

The CO-OP is a "bring your own device (BYOD)" environment. Staff, be they employees or contractors, are required to supply their own computing equipment, with the exception of data centre equipment. All staff must:

- Ensure that the equipment is fit for the job;
- Sign Privacy and Protection Schedules (PPS);
- Actively protect information and information technology assets;
- Protect information from inadvertent or deliberate disclosure to people at remote locations by using, e.g. locking cabinets, passwords, locked rooms or shredders;
- Maintain secure backups;
- Meet or exceed specified wireless networking security controls;
- Report security events or unusual activity;
- Grant right of the CO-OP to monitor and investigate security events at remote locations, including access to employee owned equipment used for work; and
- Establish and maintain security controls.

9. System Development and Maintenance

This section establishes requirements for incorporating security measures into the life cycle of an information system. Security controls must be identified as part of the business requirements for new information systems or enhancements to existing information systems.

Information security is integrated into the creation, modification, implementation and expansion by ongoing security practices such as the management of vulnerable points and securing system files. For applications, information security can be applied to the validation of data input and output and by encoding information using electronic keys.

Security controls must be identified as part of the business requirements for new information systems or enhancements to existing information systems.

9.1. Security requirements for information systems

During the requirements phase when developing, implementing major changes to, or acquiring an information system, the PSO must:

- Identify the security requirements necessary to protect the information system;
- Assign a security classification to the information and information system;
- Test the information system to verify that it functions as intended; and
- Enforce change control processes to identify and document modifications or changes which may compromise security controls or introduce security weaknesses.

9.2. Input data validation

Developers and Systems Administrators, under the direction of the PSO, must ensure the validity and integrity of data input to information systems by:

- Limiting fields to accept specific ranges of data (e.g., defining out of range values or upper and lower data volume limits);
- Checking for invalid characters in data fields;
- Making key fields mandatory;
- Verifying the plausibility of input data using business rules;
- Protecting against common attacks (e.g., buffer overflows); and
- Using control balances to verify complete input and processing.

9.3. Internal processing

The PSO must ensure that information systems include internal processing checks to:

- Detect unauthorised or incorrect changes to information;
- Prevent information from being accidentally overwritten;
- Prevent internal information from being disclosed via information system responses;
- Protect against common attacks (e.g., buffer overflows);
- Check the integrity, authenticity or any other security feature of data or software downloaded or uploaded between central or remote computers; and
- Provide error and exception reports.

9.4. Output data validation

The PSO must ensure that processes are documented to validate the data output from an information system by:

- Reconciling control balances to verify that data is processed accurately;
- Verifying the plausibility of output data using business rules;
- Providing sufficient information for a reader or subsequent information system to determine the accuracy, completeness, precision and classification of the information; and

- Providing error and exception reports.

9.5. Acceptable use of cryptography

The type and quality of cryptographic controls used in information systems must be based on a reasonable assessment of risk and include consideration of:

- Confidentiality requirements, in accordance with information classification, labelling and handling requirements;
- Integrity requirements (e.g., for financial payment instructions in excess of a specified dollar amount);
- Non-repudiation requirements (e.g., for proof of the occurrence or non-occurrence of an event);
- Authentication requirements (e.g., proof of identity);
- Other security measures (e.g., for proof of origin, receipt, or ownership);
- Legislation, regulations or policies requiring the use of cryptography;
- Restrictions on the export or use of cryptographic products; and
- Risks relating to the long-term storage of electronic information (e.g., recovery of encrypted data, long-term key maintenance).

9.6. Management of cryptographic keys

The PSO is responsible for approving key management standards and processes, including:

- Selection of cryptographic keys with sufficient lengths;
- Distribution, storage and periodic updating of cryptographic keys;
- Revocation of cryptographic keys (e.g., when a recipient changes job);
- Recovery of cryptographic keys that are lost, corrupted or have expired;
- Management of cryptographic keys that may have been compromised;
- Archival of cryptographic keys and the maintenance of cryptographic key history; and
- Allocation of activation/de-activation dates.

9.7. Changes to operational information systems

The PSO must ensure and Systems Administrators must implement procedures to control software installation on operational information systems to ensure that:

- Updates of operational information systems are planned, approved, impacts assessed, tested, logged and have a rollback plan;
- Operations personnel and end users have been notified of the changes, potential impacts and if required have received additional training;
- New releases of software are reviewed to determine if the release will introduce new security vulnerabilities;
- Modifications to operational software are logged;
- The number of personnel able to perform the updates is restricted and kept to a minimum;
- Development code or compilers are not present on operational information systems; and,
- Vendor supplied software is maintained at the supported level.

Pre-implementation Guidelines:

- Limitations of security controls are known and documented;
- Performance and capacity requirements can be met and support organizations have the capacity to maintain the information system;
- Development problems have been resolved successfully;
- The effects on existing operational information systems are known;
- Arrangements for fall-back have been established if the updated or new information system fails to function as intended;
- Changes are communicated to users who may be affected by the change;
- Error recovery and restart procedures should be established;
- Business continuity plans should be developed or updated;
- Operating procedures should be tested;
- Users should be educated to use the information system correctly and securely; and
- Computer operators/system administrators should be trained in how to run the information system correctly and securely.

Implementation Guidelines

The installation process should include:

- Validating the load or conversion of data files;
- Installing executable code only, and not source code;
- Providing ongoing technical support;
- Implementing new or revised procedures/documentation;
- Discontinuing old software, procedures and documentation;
- Arranging for fall-back in the event of failure;
- Informing the individuals involved of their roles and responsibilities;
- Transferring responsibility for the information system from development teams to operational teams to ensure segregation of duties; and
- Recording installation activity.

9.8. Protection of test data

Systems Administrators must implement procedures to ensure that:

- Sensitive or personal data from operational information systems is not used as test data;
- Using test data extracted from operational information systems must be authorized and logged to provide an audit trail;
- Test data is protected with controls appropriate to the security classification of the information and information system; and
- Data from operational information systems is removed from the test environment once testing is complete.

Where personal or sensitive data is used for testing purposes, sensitive details and content should be removed, depersonalized or modified beyond recognition. Output from test systems should be labelled “test”.

9.9. Modifying commercial-off-the-shelf software

Other than vendor supplied patches, commercial-off-the-shelf (COTS) software must not be modified except in exceptional circumstances when needed for a critical business requirement. This requirement must be documented and approved by the PSO.

If changes to COTS software are required, the PSO must determine:

- The effect the change will have on the security controls in the software;
- If consent of the vendor is required;
- If the required functionality is included in a new version of the software; and
- If CO-OP will become responsible for maintenance of the software as a result of the change.

If changes are made to COTS software the original software must be kept unaltered and the changes must be:

- Logged and documented, including a detailed technical description;
- Applied to a copy of the original software; and
- Tested and reviewed to ensure that the modified software continues to operate as intended.

9.10. Applying vendor supplied patches and updates

A software update management process must be maintained for COTS software to ensure:

- The most up-to-date approved patches have been applied; and
- The version of software is vendor supported.

10. Information Security Incident Management

This section establishes requirements for reporting a possible breach of information security as quickly as possible. This includes establishing procedures and processes so that personnel understand their roles in reporting and mitigating security events.

Information security incident management policies identify mechanisms to detect and report when information security events occur and the directives for the consistent management of such events. The information collected about the events can be analyzed to identify trends and to direct efforts continually improve and strengthen the CO-OP's information security infrastructure.

10.1. Information security event reporting

Employees must immediately report all suspected or actual information security events to the EDO and to the PSO as required by the Information Incident Management Process. Requirements for reporting events must be included in contracts and service agreements.

10.2. Reporting security weaknesses

Employees are responsible for following the Information Incident Management Process for responding to suspected or actual security weaknesses which includes reporting to the EDO and PSO as appropriate. The response process must:

- Ensure all reports are investigated and handled in a secure, confidential manner, and,
- Ensure the individual who reported the weakness is advised of the outcome when the investigation is complete; and,

The PSO must conduct an awareness program on information security advising personnel that they have a responsibility to report observed or suspected weaknesses. Suspected or observed weakness must not be tried or tested and weaknesses should not be discussed, or made known, except through approved reporting channels.

10.3. Incident Management Process

This section defines the steps that must occur in response to an information incident, including the roles and responsibilities of the stakeholders. An information incident is a single or a series of unwanted or unexpected events that threaten privacy or information security. Information incidents include the collection, use, disclosure, access, disposal, or storage of information, whether accidental or deliberate, that is not authorized by The CO-OP or the business owner of that information.

Information incidents include privacy breaches whether accidental or deliberate involving the unauthorized creation, collection, disclosure or disposal of personal information under BC FIPPA legislation.

The EDO is responsible for the coordination, investigation, and resolution of information incidents. All actual or suspected information incidents must be reported immediately to the EDO and PSO using the process below.

Event Reporting

1. Any employee, service provider or other person who discovers a suspected or actual information incident (including privacy breaches) must immediately report it to their supervisor or designated management contact as the case may be.

2. The supervisor or management contact, must immediately report the information incident to the EDO and PSO by contacting Co-op support at bc.libraries.coop and stating they require an “Information Incident Investigation”.

3. In circumstances where the supervisor or management contact is not immediately available (in person or by phone), the employee, service provider or other person must immediately report the information incident as indicated above.

4. The help desk will take contact information and create a ticket for the incident report. The ticket will be delivered to the EDO and PSO.

5. The EDO/PSO or the assigned staff lead contacts the party that reported the incident to:

    - Assess and document the information incident including, if applicable, the nature, sensitivity, volume, impact and type of incident (physical and/or information);

- Assist with resolving the incident and containing the information incident (if applicable) if it is still ongoing; and
- Provide the information incident reporter with instructions explaining the incident response process and priorities (e.g., contain the loss, prevent a recurrence, and determine next steps).

6. The incident lead determines whether the information incident is major or minor, based on relevant factors that include:

    - The incident involves multiple applications or business lines;
    - The incident involves personal or sensitive business information;
    - Whether there is, or could have been, a reasonable expectation of harm to any individuals as a result of the incident; and
    - Whether individuals will need to be notified that their personal information was breached.

7. The incident lead will then immediately assemble an incident response team (IRT) including the CO-OP Systems Administrator(s) and/or backup and take steps to manage the incident. In communication with the EDO and PSO, the IRT will conduct the remaining steps.

Containment

8. The first priority in every incident is to contain the incident as quickly as possible. An incident is considered contained when no additional harm can be caused and the incident handler is able to focus on remediation. Containment consists of three stages:
    a. Short-term containment: stopping the progress of the incident or attacker.
    b. Information gathering.
    c. Long-term containment**:** making changes to the production system.

Remediation

9. The goal of the Remediation phase is to clean up a system and remove any artifacts (e.g., rootkits) left from the attacker. During the remediation phase, the IRT must also determine and document the cause and symptoms of the incident: isolating the attack based on information gathered during the detection phase, and determining how the attack was executed.

Resolution

10. During the Resolution phase, the IRT restores normal business operations. It is critical to carefully handle incident Resolution and verify system performance and security before being brought back online. Tests must be completed and baseline system activity must be compared to ensure the system is verified before operations are restored.

Closure and Lessons Learned

11. In this final phase, the IRT and PSO documents findings from the incident, and the handling of the incident is reviewed by the EDO and Board of Directors. The expected

outcome of this phase is improved operations and improved incident response procedures.

Business Continuity Management

12. Business continuity management is addressed in the CO-OP Service Management Agreement (SMA): bc.libraries.coop

Statutory (legal) Compliance

13. All relevant statutory, regulatory and contractual requirements are explicitly defined and documented. The EDO must ensure the CO-OP complies with the statutory requirements concerning the protection of Personal Information according to BC's FIPPA.