1. Purpose

To define the deliverables, and their associated roles and responsibilities, needed to integrate information security into the operation of government information systems and information processing facilities.

This document provides detailed security specifications to support the IMIT 6.27 Operations Security Standard. Both the standard requirements and these specifications MUST be followed.

2. Resources

Appropriate Use Policy	High-level requirements for accessing and managing government information and using information technology resources.
Defensible Security Framework	Critical security controls (assessment and tools).
Information Security Glossary	List of information security terms and definitions.
IMIT 6.10 Cryptographic Security Standard	Framework for the use of cryptography in government that helps organizations meet their goals to protect their information and technology assets.
IMIT 6.11 Security Threat Risk Assessment Standard	Requirements to assess (identify, analyze, and evaluate), define planned treatments, and report security threats and risks in information systems.
IMIT 6.18 Information Security Classification Standard	Four levels of security classification applied to government information based on expected harm that could result from unauthorized disclosure.
IMIT 6.24 Access Control Security Standard	Blueprint for the management of access, authorizations, and control requirements for computer networks, operating systems, applications, and information.

IMIT 6.26 Physical and Environmental Security Standard	Security requirements for protection from environmental and man-made threats to employees and property
IMIT 6.27 Operations Security Standard	Corresponding standard for these specifications.
OCIO Patch Guidelines	Current patching expectations for government assets and the Cybersecurity and Digital Trust Branch's expected patch mitigation plan for vulnerable systems based on risk rating.

3. Specifications

3.1 Operational controls

3.1.1 Operational procedures

1. The OCIO (for enterprise systems) and ministries (for ministry systems) MUST:
   a. Ensure operating procedures and standards for the information system or information processing facility are:
      i. Approved.
      ii. Documented in the system security plan.
      iii. Consistent with government policies, standards, specifications, and guidelines.
      iv. Reviewed and updated at least annually or when:
         - Changes occur to building layouts.
         - Changes occur to equipment/systems located in the facility.

- Changes occur in business services and supporting information system operations.
- A security incident investigation finds weaknesses in the operating procedures or standards.

b. Ensure the operations documentation contain detailed instructions regarding:
   i. Information processing and handling.
   ii. Last review and update.
   iii. Classification of document.
   iv. System restart and recovery.
   v. Backup and recovery, including onsite and offsite storage.
   vi. Exceptions handling, including a log of exceptions.
   vii. Output and media handling, including secure disposal or destruction of media.
   viii. Audit and system log management.
   ix. Change management, including scheduled maintenance and interdependencies.
   x. Computer room management and safety.
   xi. Information incident management process.[1]
   xii. Disaster recovery.
   xiii. Business continuity.
   xiv. Operations, technical, emergency, and business contacts.

c. Develop and maintain:
   i. Critical incident management plans for critical systems.
   ii. Disaster recovery plans.
   iii. Business continuity plans.

2. The Chief Information Security Officer (CISO) MUST implement processes to ensure critical incident management plans are maintained.

[1] The information incident management process includes developing and maintaining a critical incident management plan for the information system.

3.1.2 Changes to information systems and information processing facilities

The OCIO (for enterprise systems) and ministries (for ministry systems) MUST:

Pre-implementation

1. Plan for changes to the information system or information processing facility by assessing the impact of the proposed change on security.
2. Plan, document, and implement a change management policy and process (see Appendix A: Change management process steps) to control changes to information systems or information processing facility.
3. Notify affected parties, including business partners and third parties, about changes to the information system or information processing facility.
4. Complete any re-certification and re-accreditation as required of the information system or information processing facility that will be changed.

Implementation

5. Implement the planned changes following the documented change management process and procedures for information systems or information processing facility.

Post-implementation

6. Review the changed information system or information processing facility for vulnerabilities and fix the identified vulnerabilities.
7. Update disaster recovery and business continuity plans for the information system or information processing facility.

3.1.3 Controls to limit information leakage

The OCIO (for enterprise systems) and ministries (for ministry systems) MUST:

1. Reduce opportunities for information leakage in information systems by implementing processes to:
   a. Scan for malicious code.
   b. Monitor resource usage in information systems.
   c. Control and manage access to information systems.

d. Identify and remove untrusted connections in and out of the government network.
e. Control and manage third party network connections; for example, by limiting them to only authorized traffic.
f. Control and manage installation of software.
g. Use high-integrity software.[2]
h. Monitor information systems.
i. Review usage and access logs for irregularities.
j. Review logs for data exfiltration.

3.1.4 Resource capacity planning and management

The OCIO (for enterprise systems) and ministries (for ministry systems) MUST:

Resource capacity management

1. Document resource capacity management processes and review them at a frequency that meets the availability requirements of the system.
2. Ensure that resource capacity management processes:
   a. Document capacity requirements and capacity planning processes.
   b. Identify and manage storage requirements.
   c. Include capacity requirements in service agreements.
   d. Monitor and optimize information systems to detect impending capacity limits.
   e. Project future capacity requirements based on:
      i. New business and system requirements.
      ii. Statistical or historical capacity requirement data.
      iii. Current and expected trends in processing capabilities (for example, introduction of more efficient hardware or software).

[2] Canadian Common Criteria Scheme (CCCS) certification may be considered for evaluation of high-integrity software.

Resource capacity planning

3. Use trend information from the resource capacity management process to identify and resolve potential bottlenecks that present a threat to system security or services.
4. Plan and budget for business and service capacity management.
5. Perform capacity planning for critical systems for the projected life of the system.
6. Consider additional demand for capacity when planning for an information system project and automate the resource capacity management processes where feasible.

3.1.5 Separation requirements

The OCIO (for enterprise systems) and ministries (for ministry systems) MUST:

1. Complete the following to protect production information systems:
    a. Separate non-production environments from production environments (for example, use separate locations/platforms [physical or virtual] for each environment, servers [physical or virtual], domains, and partitions).
    b. Prohibit use of login credentials for production information systems in non-production information systems.
    c. Store sensitive production code in a secure location that is separate from the non-production environments and restrict its access to authorized employees.
    d. Prevent access to compilers, editing, and other tools from production information systems.
    e. Promote software from non-production to production information systems using approved change management processes.
    f. Prohibit access to production data from non-production information systems.
    g. Prohibit use of production data in non-production information systems unless:
        i. Approval has been obtained and documented with the business need.

ii. Security controls that are equivalent to those in the production system are in place.
iii. Production data that contains personal or sensitive information is masked or de-identified when used in non-production information systems.

2. Require architecture diagrams to illustrate clear separation between non-production and production information systems.
3. Document the controls that ensure separation of the non-production and production information system environments during a security threat and risk assessment.
4. Separate information system duties to match the assessed value, sensitivity of the information, and criticality of the information asset or system.
5. Separate non-production information system activities from production information system activities.

3.2 Protection from malware

3.2.1 Prevention and detection controls

1. The OCIO (for enterprise systems) and ministries (for ministry systems) MUST:
   a. Protect government information assets and systems from cyber threats by completing the following activities, as a minimum:
      i. Install, update, and consistently use tools that scan for, detect, and protect against network and host-based threats.
      ii. Prohibit the use of unauthorized software in information systems.
      iii. Check files, including electronic mail attachments and file downloads, for malware before use.
      iv. Perform back up and test information assets and systems as often as needed to meet the availability requirements of information assets and systems.
      v. Check the data backups are completed successfully and regularly test the backed up data for disaster recovery.

vi. Maintain current disaster recovery and business continuity plans for information systems.
vii. Conduct vulnerability scans on information systems as often as needed to meet the assessed value and sensitivity of the information, and the availability requirements of the information system.
viii. Regularly review file and data content on critical information systems to identify unapproved or unauthorized files and file changes.

b. Require a current anti-malware solution or other similar security measures to be installed on devices connecting to the government network.
c. Document the following in a registry for specific threat countermeasures (such as blocked websites, blocked electronic mail attachment file types, blocked network ports, additional monitoring):
   - Description
   - Rationale
   - Approval authority
   - Date the countermeasure was applied

2. The Chief Information Security Officer MUST develop the process to maintain the registry of specific threat countermeasures.

3.2.2 User awareness

1. The Chief Information Security Officer MUST develop user awareness programs and training.
2. The OCIO (for enterprise systems) and ministries (for ministry systems) MUST:
   a. Develop user awareness programs for threat countermeasures.
   b. Conduct awareness activities regarding cyber threats.
   c. Require employees to complete the information protection courses as part of their awareness training.
3. Ministry Information Security Officers MUST conduct awareness activities on cyber threats and communicate technical advice and information.
4. Employees MUST participate in security awareness training.

3.3 Backups

3.3.1 Backup and recovery process requirements

The OCIO (for enterprise systems) and ministries (for ministry systems) MUST ensure:

1. Documented backup and recovery processes reflect the security classification and availability requirements of information and the information systems per their Business Impact Assessments.
2. The backup and recovery processes document the following:
   a. Types of information to be backed up.
   b. Schedules for the backup of information and information systems.
   c. Backup media management; for example, retention period, pattern of backup cycles, storage and handling requirements, labelling.
   d. Methods for performing, validating, and labelling backups.
   e. Methods for validating recovery of the information and information system.
3. Backup and recovery procedures are documented and updated.
4. Backup and recovery strategies comply with the following:
   a. Business continuity plans.
   b. Policy, standard, legislative, regulatory, and other legal obligations.
   c. Records management requirements, including Administrative Records Classification System (ARCS) and Operational Records Classification System (ORCS).

3.3.2 Backup facilities and media safeguards

The OCIO (for enterprise systems) and ministries (for ministry systems) MUST:

1. Identify safeguards that meet the value and sensitivity of the information and information systems during a security threat and risk assessment (see IMIT 6.11 Security Threat Risk Assessment Standard) for backup facilities and media. The safeguards MUST include:
   a. Use of encryption (see IMIT 6.10 Cryptographic Standards) to protect the backed-up information.

b. Use of digital signatures to protect the integrity of the information.
c. Physical and environmental security measures (see IMIT 6.26 Physical and Environmental Security Standard).
d. Access control measures (see IMIT 6.24 Access Control Security Standard) that meet the sensitivity of the backed-up data to secure the backup data.
e. Use of secure methods to transport backed-up information between the offsite and main site locations; for example, authorized couriers, approved encrypted electronic transfer.
f. Storing backup media following manufacturer's recommendations for storage conditions and maximum shelf life.
g. Storing backup media in a manner consistent with disaster recovery and business continuity requirements.

3.4 Logging and monitoring

3.4.1 Audit logs

The OCIO (for enterprise systems) and ministries (for ministry systems) MUST:

Logging requirements

1. Require logging for the information asset or system to be sufficient to detect activities that can negatively impact their value, sensitivity, and availability.
2. Require logs to contain details to enable:
   a. Investigating the activities that resulted in an incident.[3]
   b. Resolving the incident.
3. At minimum, require the logs to include the following (as appropriate for the information asset or system being logged):
   a. For information systems:

[3] Examples of incidents are:
- Unauthorized system configurations changes, access permission changes, access to sensitive information, or bulk copy or transfer of data
- Unexpected system outages or shutdowns, loss of data, encryption of data
- Denial of service attacks

i. User identifier
ii. Dates, times, and details of key events (for example, login and logout)
iii. Login method, machine ID, and network address
iv. Records of successful and unsuccessful system login attempts
v. Records of successful and unsuccessful data access (including record and field access where applicable) and other resource access attempts
vi. Changes to system configuration
vii. Use of privileges
viii. Use of system utilities and applications
ix. Files accessed and type of access (for example, view, read, modify, delete)
x. Activation and deactivation of protection systems (for example, antivirus, intrusion detection)
xi. When electronic file transmissions occur, the name and size of file attachments that are part of, or are included in, data transmissions (for example, email, instant messaging, unified communications platforms)
xii. System faults, errors, or exceptions

b. For voice calls:
   i. Source and destination telephone numbers
   ii. Date, time, and length of call
c. For networks:
   i. Network address (source and destination)
   ii. Ports (source and destination)
   iii. Protocols
   iv. Transferred network data traffic flow (packets and bytes)
d. For physical access control systems:
   i. Location of alarms
   ii. Date and time
   iii. Type of alarm

4. Protect audit logs and restrict their access to employees who are authorized to access the audit logs.
5. Protect audit logs of information systems against alteration, erasure, or deactivation by anyone, including owners of the information system or people authorized to manage the information system.
6. Update the privacy impact assessment (PIA) and Statement of Acceptable Risks (SoAR) when audit logging for the information system will be deactivated or will not be activated, and include the following details:
   - Name and position of the decision maker
   - Date and rationale for the deactivation or non-activation

Review of monitoring activities

7. Set up and document the processes and resources required for an audit log review.
8. Require the audit log review process to:
   a. Prioritize reviews of high value and highly sensitive information assets based on the risks identified in a documented Statement of Acceptable Risks (SoAR).
   b. Use automated tools to identify exceptions (for example, failed access attempts, unusual activity) and facilitate ongoing analysis and review.
9. Review audit logs at a frequency based on the assessed value and sensitivity of the information and the criticality of the information asset or system.
10. Monitor audit logs and set up alerts to automatically flag alarms found in audit logs based on the value and sensitivity of information and criticality of the information asset or system.
11. Evaluate the effectiveness of audit log monitoring at least annually to confirm that desired events are detected.
12. Use the results of monitoring activities to:
    a. Assess the efficacy of user awareness and training.
    b. Identify new training requirements.
    c. Detect:
       i. Vulnerabilities that could be or that are being exploited.

ii. Increases or decreases in unauthorized access attempts or unauthorized use of privileges.

Audit log retention

13. Retain audit logs following the approved records retention schedule for the information asset or the system.
14. Retain all audit logs related to a security investigation until the investigation has been concluded and the audit logs are no longer required based on the records retention schedule.

Response to alarms

15. Document the alarm response procedure, including the authority to shut down all or part of a system or network when an alarm indicates new unacceptable threats are present. The authority includes who approved the shutdown and conditions for the shutdown.
16. Document the response to an alarm, which normally includes:
    a. Identification of the alarm event.
    b. Isolation of the event, including affected assets.
    c. Identification and isolation or neutralization of the source.
    d. Corrective action.
    e. Forensics analysis of event.
    f. Action to prevent reoccurrence.
17. Report the circumstances to the Information Owners as soon as possible when the authority to shut down a system or network is exercised.
18. Secure the audit logs as evidence.

3.4.2 Protection of information system logging facilities and log information

The OCIO (for enterprise systems) and ministries (for ministry systems) MUST:

Protecting information system logging facilities

1. Implement security controls to protect logging facilities and log files from unauthorized modification, access, or disposal. Security controls include physical security safeguards such as situating logging facilities within a secure zone with restricted access.

2. Conduct periodic[4] independent reviews or audits to confirm the appropriate controls have been implemented.

Protecting log information

3. Implement controls to protect log files from tampering, unauthorized access, and unauthorized disposal. The controls include:
   a. Implementing multi-factor authentication for access to sensitive log records.
   b. Backing up audit logs to offsite locations.
   c. Preventing log files from being overwritten due to insufficient log storage capacity.
   d. Retaining the audit logs per the records management schedule appropriate with requirements of the business.
   e. Implementing digital signatures for the log files, where available.
4. Implement controls to ensure all employees, including privileged users, DO NOT have permission to alter or erase logs, or to deactivate logging of their own activities.
5. Log access to audit logs.

3.4.3 Privileged user activities logging

The OCIO (for enterprise systems) and ministries (for ministry systems) MUST:

Logging activities

1. Require privileged user activity logs to capture the following:
   a. Event occurrence times.
   b. Identity of the account and the privileged user involved.
   c. Event details, such as:
      i. Access and permissions granted, changed, or removed
      ii. Corrective action
      iii. Errors
      iv. Files accessed, modified, or deleted

[4] The review frequency depends on the criticality, value, and sensitivity of the information assets and the systems being logged.

v. System configuration changes

d. System processes involved.

Independent review

2. Prohibit privileged users from reviewing logs of their own activities.
3. Randomly select a privileged user for review if there is more than one privileged user for an information system.
4. Conduct reviews of privileged user activity logs at a frequency that protects the criticality, value, and sensitivity of the information asset or the system.
5. Require verified logs to be signed by the reviewer (digitally, where available), and stored or archived securely based on the approved records retention schedule.
6. Review audits logs before they are discarded or overwritten.

3.4.4 Fault reporting and logging

The OCIO (for enterprise systems) and ministries (for ministry systems) MUST:

Reporting and logging faults

1. Determine fault logging requirements through a security threat and risk assessment and a privacy impact assessment (PIA) if appropriate.
2. Implement processes to log, monitor, analyze, correct, and report system faults.
3. Require fault management reports to include:
   a. Description of fault, including date, time, location, and extent of fault.
   b. Analysis of probable source and cause.
   c. Corrective actions taken to respond to and resolve the fault.

Fault analysis, resolution, and corrective action

4. Require analysis and corrective action to include:
   a. Defining the fault and probable cause(s).
   b. Assessing the effectiveness of corrective action(s).
   c. Verifying that corrective action has not introduced unforeseen vulnerabilities.
   d. Identifying trends so that corrective action makes increasingly effective use of resources while improving results.

e. Recommending upgrades, replacement of components, software, or other elements that create or cause faults.
f. Improving fault detection and reporting to reduce the time between fault occurrence and taking corrective action.
g. Measuring the exposure caused by the fault.
h. Reporting on performance impact(s).
i. Periodically reassessing logging requirements.

5. Identify faults that cause information security issues with an appropriate action plan at annual information security reviews.

3.4.5 Computer clock

The OCIO (for enterprise systems) and ministries (for ministry systems) MUST:

Synchronization

1. Require information system clocks to synchronize to either the:
   a. Local router gateway.
      OR
   b. Government-approved clock host.[5]

Verification

2. Require confirmation that system clocks are still synchronized:
   a. Following power outages or fluctuations.
   b. After the performance of every system update or patch application.
   c. As part of incident analysis and audit log reviews.
   d. At least twice a year.
3. Require time discrepancies to be reported to OCIO Helpdesk, Customer Service Centre.

[5] Government-approved clock hosts are synchronized with a national time service such as the Government of Canada, National Research Council's Network Time Protocol server.

3.5 Control of production information systems

3.5.1 Software changes to production information systems

The OCIO (for enterprise systems) and ministries (for ministry systems) MUST:

1. Control software installation on production information systems with procedures that ensure:
   a. Updates to production information systems are planned, approved, assessed for impact(s), tested, logged, and have a rollback plan.
   b. Software version releases are reviewed for:
      i. Potential security vulnerabilities.
      ii. Changes that may negatively impact existing security controls.
2. Confirm the version of the vendor-supplied software to be installed is still maintained and supported by the vendor.
3. Notify operations employees and end users of the changes and potential impacts and, if required, provide additional training to them.
4. Log changes to production software.
5. Restrict the number of employees able to perform the updates.
6. Review and remove development code or compilers from production information systems.

3.5.2 Information system implementation controls

The OCIO (for enterprise systems) and ministries (for ministry systems) MUST:

Pre-implementation

1. Require the following before an updated or a new information system is implemented into the production environment:
   a. A completed and approved Statement of Acceptable Risks (SoAR).
   b. A completed and approved privacy impact assessment (PIA).
   c. Documented limitations of security controls.
   d. Confirmation that performance and capacity requirements can be met.
   e. Confirmation that organizations responsible for maintaining and supporting the information system have the capacity to do so.

f. Successful resolution of development problems.
g. Identification of the effects to existing production information systems.
h. Arrangements to return the system back to what it was before the change if the new or updated information system fails to function as intended.
i. Documented and tested error recovery and restart procedures.
j. Developed or updated business continuity plans.
k. Updated and tested operating procedures.
l. Notification to affected users and interested parties about the changes.
m. Education of users to use the information system correctly and securely.
n. Training of computer operators and system administrators in how to run the information system correctly and securely.

Implementation

2. Require the following to be included as part of the installation process:
   a. Validation of the load or conversion of data files.
   b. Installation of executable code only, and not source code.
   c. Provision of ongoing technical support.
   d. Implementation of new or revised procedures and documentation.
   e. Discontinuation of old software, procedures, and documentation.
   f. Arrangements to revert the system back to what it was before the change in the event of failure.
   g. Individuals involved are informed of their roles and responsibilities.
   h. Transfer of responsibility for the information system from development teams to production teams.
   i. Detailed documentation of the installation activity.

Post-implementation

3. Require post-implementation reviews to include:
   a. The efficiency, effectiveness, and cost of security controls.
   b. Lessons learned and scope for improvements of security controls.
   c. Security incidents resulting from the updated or new information system implementation, and mitigation measures.

3.5.3 Protection of systems documentation

The OCIO (for enterprise systems) and ministries (for ministry systems) MUST:

1. Establish and follow procedures for the secure use and storage of systems documentation that include:
   a. Requiring all systems documentation be labelled with an information security classification label. See IMIT 6.18 Information Security Classification Standard.
   b. Establishing lists of users authorized to access systems documentation.
   c. Establishing handling rules for the information regardless of storage media (for example, electronic, paper).
   d. Requiring use of access controls, passwords, encryption, or digital signatures appropriate to the information security classification label. See IMIT 6.10 Cryptographic Security Standard, IMIT 6.18 Information Security Classification Standard, and IMIT 6.24 Access Control Security Standard.
2. Establish a compliance monitoring process to ensure the procedures above are followed.

3.6 Technical vulnerability management

3.6.1 Vulnerability response processes

1. The Chief Information Security Officer MUST:
   a. Ensure roles and responsibilities for the coordination of vulnerability management are identified and established.
   b. Require vulnerabilities to be evaluated and have the OCIO and ministries notified about vulnerabilities.
   c. Provide advice on appropriate response to vulnerabilities.
   d. Initiate incident response processes to address vulnerabilities when required.
   e. Require progress in responding to vulnerabilities to be monitored.
   f. Publish summary reports on vulnerability response activities and cost.

2. The OCIO (for enterprise systems) and ministries (for ministry systems) MUST:
   a. Identify and establish roles and responsibilities for the coordination of vulnerability management.
   b. Document and follow emergency procedures for high-risk vulnerabilities.
   c. Require all vulnerability patches to be logged in the system security plan for information systems.
   d. Establish a priority patching criterion based on risk to address the most critical applications and information systems first.
   e. Include responsibilities for vulnerability response in service agreements with external service providers.
   f. Address vulnerabilities that impact information systems following the OCIO Patch Guidelines to mitigate or minimize the impact on operations.
   g. Manage vulnerabilities that may impact information assets or systems by establishing processes to:
      i. Monitor external sources of information on published vulnerabilities.
      ii. Assess the risk of published vulnerabilities to information systems.
      iii. Test and evaluate options to mitigate or minimize the impact of vulnerabilities.
      iv. Apply corrective measures to address the vulnerabilities.
      v. Verify the corrective measures have addressed the vulnerabilities.
      vi. Report the progress in responding to vulnerabilities to the Chief Information Security Officer.
   h. Complete a Statement of Acceptable Risk (SoAR) if the medium- to high-risk vulnerability will not be patched.

3.6.2 Rules governing software installation

Employees MUST:

1. Receive authorization[6] before installing software on government devices.
2. Follow the requirements of the Appropriate Use Policy when installing software on government devices.

3.7 Information systems audit considerations

3.7.1 Management of information systems compliance checking

The OCIO (for enterprise systems) and ministries (for ministry systems) MUST:

1. Make an employee[7] responsible for compliance-checking activities for production information systems.
2. Define, document, and approve compliance-checking activities for production information systems (such as audits, risk and controls reviews, monitoring, or security reviews) before the activities start.
3. Determine and agree on the scope, duration, and level of detail of the compliance-checking activity to minimize disruption.
4. Determine handling requirements for copies of files made by employees who complete compliance-checking activities.
5. Establish a separate environment for the analysis of files and:
   a. Restrict access to those files.
   b. Log accesses made to those files.
   c. Erase files when compliance-checking activities have concluded, unless the files are needed to support report findings.
6. Identify special testing or processing that may impact production information systems (for example, ethical hacking, server vulnerability assessments).

[6] Unauthorized software installed on computing devices can introduce vulnerabilities that lead to information leakage, loss of integrity or other information security incidents, or to violation of intellectual property rights.
[7] Ensure the employee has sufficient authority to enforce approved compliance-checking activities.

7. Notify the Chief Information Security Officer before conducting compliance-checking activities to prevent triggering false security alarms within the infrastructure.
8. Schedule tests to minimize disruption.
9. Submit reports of penetration tests or vulnerability assessments to the Chief Information Security Officer immediately upon receipt.
10. Ensure that employees conducting compliance-checking activities on the production information systems are not also responsible for operating and managing the same production information systems.
11. Implement security controls to maintain the privacy requirements of sensitive information in the production information systems during compliance-checking activities.

3.7.2 Protection of information systems during compliance checking

The OCIO (for enterprise systems) and ministries (for ministry systems) MUST:

1. Authorize the use of audit tools.
2. Limit access rights to production information systems for compliance-checking employees to “read only.”
3. Monitor and log all access to production information systems.
4. Control the use of audit tools by:
   a. Restricting access to the audit tools to authorized employees.
   b. Installing or enabling specialized audit tools as required during the compliance-checking activity.
   c. Removing the audit tools and access to them at the end of the compliance-checking activities.

4. Revision history

These specifications are reviewed annually and updated as needed.

Version	Revision Date	Author	Description of Revisions
1.0	August 2024	S. Gopaldas Johnston	New guidelines document to support the Operations Security Standard V2.0.

5. Contact

For questions regarding these specifications, contact:

Cybersecurity and Digital Trust Branch, Office of the Chief Information Officer
Ministry of Citizens' Services
Email: InfoSecAdvisoryServices@gov.bc.ca

Appendix A: Change management process steps

At minimum, the OCIO (for enterprise systems) and ministries (for ministry systems) MUST:

1. Identify and record changes to be made to the information system or information processing facility.
2. Assess the potential impact of the planned changes, including the security impact and the size of the planned change.[8]
3. Identify the impact on agreements with business partners and third parties, including Information Sharing Agreements (ISA), Memoranda of Understanding (MOU), licensing, and provision of services for the information system or information processing facility that will be changed.
4. Develop an implementation strategy for the planned changes.
5. Obtain approval for the planned changes to be obtained from person(s) accountable or responsible for the information system or information processing facility.
6. Document rollback procedures to revert the information system or information processing facility back to what it was before the planned change.
7. Communicate change details to parties impacted by the planned change.
8. Where technically possible, test the planned changes to verify the results of the change are as expected before they are implemented in production.
9. Document all change activity in the testing and implementation phases.
10. Review change activity logs to ensure only planned changes were performed and no other unauthorized changes were made.
11. Confirm the results from the implemented changes are as expected.
12. Review and update the systems documentation for the information system or information processing facility.

[8] A security threat and risk assessment need not be conducted for minor changes like the installation of a software service pack or a security patch for a vulnerability. A security threat and risk assessment MUST be conducted for major changes like installing a software version upgrade or new software, or implementing a functional change. See IMIT 6.11 Security Threat Risk Assessment Standard.

13. Provide training on the changes to technical and operations employees.