Government of Canada Gouvernement du Canada

Directive on Security Management

Note to reader

The Directive on Security Management and its Mandatory Procedures took effect on July 1, 2019. It replaced the Directive on Departmental Security Management, as well as the Operational Security Standard - Business Continuity Planning (BCP) Program, the Operational Security Standard on Physical Security, the Operational Security Standard - Readiness Levels for Federal Government Facilities, and the Operational Security Standard: Management of Information Technology Security (MITS).

The Directive on Security Screening took effect on January 6, 2025. It replaces the Standard on Security Screening, as well as Appendix A: Mandatory Procedures for Security Screening Control of the Directive on Security Management.

1. Effective date

1.1 This directive takes effect on July 1, 2019.

1.2 This directive replaces the following Treasury Board policy instruments:

- Directive on Departmental Security Management (July 1, 2009)
- Operational Security Standard: Business Continuity Planning (BCP) Program (April 23, 2004)
- Operational Security Standard: Management of Information Technology Security (MITS) (May 31, 2004)
- Operational Security Standard on Physical Security (February 18, 2013)
- Operational Security Standard: Readiness Levels for Federal Government Facilities (November 1, 2002)
- Security and Contracting Management Standard (June 9, 1996)
- Security Organization and Administration Standard (June 1, 1995)

1.3 Transitional considerations:

1.3.1 Subsections 4.1.3 and 4.2.5 of this directive will take effect on July 1, 2019 or on the scheduled date for the renewal of the department's security plan, whichever is later.

2. Authorities

2.1 This directive is issued pursuant to the authorities indicated in section 2 of the Policy on Government Security.

3. Objectives and expected results

3.1 The objectives indicated in section 3 of the Policy on Government Security apply to this directive.

3.2 The expected results indicated in section 3 of the Policy on Government Security apply to this directive.

4. Requirements

Chief security officer

4.1 The chief security officer (CSO) designated by the deputy head in compliance with the Policy on Government Security is responsible for managing the departmental security function and the following:

4.1.1 Supporting the deputy head's accountabilities under the Policy on Government Security;

4.1.2 Leading the departmental security function, including:

4.1.2.1 Responsibilities for defining, documenting, implementing, assessing, monitoring and maintaining security requirements, practices and controls; and

4.1.2.2 Authorities for related security risk management decisions;

4.1.3 Overseeing the development, implementation and maintenance of the department's security plan, in collaboration with other senior officials and other stakeholders, which:

4.1.3.1 Provides an integrated view of departmental security threats, risks and requirements; and

4.1.3.2 Includes strategies, priorities, responsibilities and timelines for maintaining, strengthening, monitoring and continuously improving the security practices and security controls described in appendices A to H;

4.1.4 Overseeing the establishment of department-wide processes to assess and document actions taken regarding residual security risks for the department's programs and services and their supporting resources;

4.1.5 Reporting at least annually to the deputy head on progress in achieving the priorities defined in the department's security plan and, as required, recommending changes to departmental security practices, security controls and priorities;

4.1.6 Overseeing the establishment of department-wide processes to monitor and ensure a coordinated response to, and reporting of, department-specific threats, vulnerabilities, security incidents and other security events, including identification of actions to address any deficiencies;

4.1.7 Ensuring that any significant issues regarding policy compliance, suspected criminal activity, national security concerns or other security issues are assessed, investigated, documented, acted on and reported to the deputy head and, as required, to the appropriate law enforcement authority and/or security and intelligence agency (see Appendix I: Standard on Security Event Reporting), and to affected

stakeholders, and as required, cooperating in any resulting criminal or other investigation(s);

4.1.8 Collaborating with other senior officials and other stakeholders to respond to direction, advice and information requests issued by the Privy Council Office, the Treasury Board of Canada Secretariat as the employer (for example, the Office of the Chief Human Resources Officer), and the Government Operations Centre regarding security events that require an immediate or coordinated government-wide action; and

4.1.9 Verifying that written agreements are in place when the organization provides or receives security services from another department or organization pursuant to subsections 6.2 and 6.3

Senior officials in the department's security governance

4.2 Senior officials, who are individuals designated by the deputy head in the departmental security governance as having responsibility for aspects of security and are responsible for the following:

4.2.1 Participating in and reporting to the department's security governance, in accordance with their assigned security responsibilities;

4.2.2 Assigning security responsibilities for programs, services and activities in their area of responsibility, as an integral element of the department's security governance;

4.2.3 Providing advice to the deputy head, the CSO and other stakeholders on departmental security matters in their area of responsibility;

4.2.4 When the department relies on or supports another organization to fulfill a security function or to support the delivery of programs, services or activities within their area of responsibility:

4.2.4.1 Establishing, or recommending the establishment of, a written agreement that defines applicable security requirements and respective security responsibilities;

4.2.4.2 Verifying that these requirements and responsibilities are met; and

4.2.4.3 Monitoring continued compliance (see subsections 6.2 and 6.3);

4.2.5 Identifying security requirements and related resource needs for programs, services and activities within their area of responsibility, while considering other stakeholders and acting in accordance with the department's security governance;

4.2.6 Ensuring that security practices and security controls (see appendices A to H) are defined, documented, implemented, monitored and maintained to meet identified security requirements for programs, services and activities within their area of responsibility, in accordance with the departmental security plan and in collaboration with other

senior officials, security functional specialists, partners and other stakeholders;

4.2.7 Documenting or recommending actions to be taken regarding residual security risks for programs, services and activities within their area of responsibility, and their supporting resources, in accordance with their assigned authority and department-wide processes and in consultation with the CSO;

4.2.8 Establishing processes to monitor, respond to and report threats, vulnerabilities, security incidents and other security events within their area of responsibility, as an integral element of department-wide processes;

4.2.9 Addressing security events that could impact programs, services and activities within their area of responsibility or that require an immediate or coordinated government-wide action, in collaboration with the CSO, partners and other stakeholders; and

4.2.10 Monitoring and reporting on the effectiveness of security practices and controls within their area of responsibility, and sharing the results with the CSO.

Security functional specialists and other designated individuals

4.3 Security functional specialists and other individuals are responsible for coordinating, managing and providing advice and services related to the departmental security controls and program. Other designated individuals in the department’s security governance who

provide input into the departmental security program are responsible for the following:

4.3.1 Defining, documenting, implementing, assessing, monitoring and maintaining departmental security requirements, practices and security controls (see appendices A to H and Appendix J);

4.3.2 Providing advice to the CSO and other stakeholders, as appropriate, on departmental security matters within their area of responsibility; and

4.3.3 Monitoring and reporting on the effectiveness of security practices and security controls within their area of responsibility, and sharing the results with the CSO, to:

4.3.3.1 Assess the extent to which departmental security requirements are met; and

4.3.3.2 Identify necessary actions to address any deficiencies.

Supervisors

4.4 Supervisors are responsible for the following:

4.4.1 Integrating security and related resource considerations into planning and other administrative activities;

4.4.2 Ensuring that individuals are informed of their security responsibilities and that employees are provided with security awareness and training to maintain the required knowledge and skills to meet their responsibilities;

4.4.3 Verifying that employees apply and adhere to departmental security practices and are taking or recommending corrective actions to address any deficiencies;

4.4.4 Informing the CSO of any issues regarding policy compliance, suspected or alleged criminal activity, national security concerns, security incidents or other security events within their area of responsibility; and

4.4.5 Cooperating with the CSO and other stakeholders in the investigation of security incidents and other security events and in identifying and implementing corrective actions.

Employees

4.5 Employees are responsible for the following:

4.5.1 Adhering to government security policy and departmental security practices, including safeguarding information and assets under their control, whether working on-site or off-site;

4.5.2 Participating in security awareness and training activities to maintain awareness of security concerns and issues and understanding of security responsibilities; and

4.5.3 Maintaining vigilance and reporting changes in circumstances, potential security deficiencies, security incidents, suspected criminal activity, national security concerns and other security issues through appropriate departmental channels.

Individuals designated by deputy heads of internal enterprise service organizations to oversee their internal enterprise service activities

4.6 Individuals designated by deputy heads of internal enterprise service organizations to oversee their internal enterprise service activities, which is a service provided by one government of Canada department to another, under the Policy on Government Security are responsible for the following:

4.6.1 Leading the establishment of security governance for internal enterprise services that:

4.6.1.1 Includes responsibilities and authorities for identifying and meeting security requirements throughout the planning, design, delivery, operations and maintenance of services provided to departments; and

4.6.1.2 Is an integral element of the department's security and corporate governance;

4.6.2 Liaising with client departments when identifying security requirements for internal enterprise services, and with the Treasury Board of Canada Secretariat, for services intended to be offered government-wide;

4.6.3 Communicating to client departments the security practices and controls that have been implemented to meet defined security requirements, the security conditions that need to be in place in the client environment, and any remaining residual risks and recommended mitigation measures;

4.6.4 Establishing processes for monitoring services provided to departments to ensure that issues regarding fulfillment of security requirements are examined and acted on, in coordination with affected stakeholders, and that issues that have potential government-wide impacts are documented and reported to the Treasury Board of Canada Secretariat; and

4.6.5 Responding and taking necessary actions regarding security events that could impact the security of the services provided to departments, in collaboration with the CSO, clients and other stakeholders.

5. Roles of other government organizations

5.1 The roles of other government organizations in relation to this directive are described in section 5 of the Policy on Government Security.

6. Application

6.1 This directive applies to the organizations listed in section 6.1 of the Policy on Government Security.

6.2 Subsections 4.1.9 and 4.2.4 of this directive apply only to interdepartmental agreements pursuant to subsection 29.2 of the Financial Administration Act, and to arrangements with Crown corporations, other orders of government, the private sector or other entities that are not governed by the Policy on Government Security,

where the department has authority to enter into such agreements or arrangements.

6.3 Subsections 4.1.9 and 4.2.4 of this directive apply to contracts for the production or delivery of goods or services and to any other arrangement involving the sharing of sensitive information or assets with organizations or individuals that do not fall under the application of the Policy on Government Security (for example, memoranda of understanding with other orders of government and academic or scientific partners).

7. References

7.1 Legislation

- Financial Administration Act
- Access to Information Act
- Criminal Code
- Public Service Employment Act
- Civil Code of Québec (articles 3 and 35 to 41)

7.2 Related policy instruments

- Policy on Government Security
- Policy on Conflict of Interest and Post-Employment
- Values and Ethics Code for the Public Sector
- Directive on Security Screening

8. Enquiries

8.1 Members of the public may contact Treasury Board of Canada Secretariat Public Enquiries for information about this directive.

8.2 Individuals from departments should contact their departmental security management group for any questions regarding this directive.

8.3 Individuals from the departmental security group may contact the Security Policy Division at the Treasury Board of Canada Secretariat, by email at SEC@tbs-sct.gc.ca, for interpretation of any aspect of this directive.

Appendix B: Mandatory Procedures for Information Technology Security Control

B.1 Effective Date

B.1.1 These procedures take effect on July 1, 2019.

B.2 Procedures

B.2.1 These procedures provide details on the requirements to support the deputy head accountability.
The procedures and subsections are as follows:

Procedure	Subsection
Information technology requirements and practices	B.2.2
IT security controls	B.2.3
Security in IT project management	B.2.4
Security in the information system life cycle, and integrity of the IT supply chain	B.2.5

IT security assessment and authorization	B.2.6
Monitoring and corrective actions	B.2.7

B.2.2 **Information technology security requirements and practices:** Define, document and maintain departmental information technology (IT) security requirements and practices:

B.2.2.1 For all information systems that support departmental programs, services or activities or that hold departmental information or information under the custody or control of the department:

B.2.2.1.1 Identify pertinent physical security, business continuity, disaster recovery and information security requirements;

B.2.2.1.2 Identify and assess threats to which information systems are exposed; and

B.2.2.1.3 Define and document requirements for ensuring the protection of departmental information systems throughout their life cycle, commensurate with identified security requirements and threats, and in accordance with applicable legislation, policies, contracts, agreements and memoranda of understanding; and

B.2.2.2 Define and document departmental security practices for implementing and maintaining IT security controls, including practices for conducting IT security assessment and authorization, in accordance with departmental security requirements.

B.2.3 **IT security controls:** Define, document, implement and maintain security controls to meet departmental IT security requirements, in accordance with departmental practices.

B.2.3.1 **Identification and authentication management:** Implement measures to ensure that individuals and devices are uniquely identified and authenticated to an appropriate level of assurance before being granted access to information in information systems, in accordance with Appendix A: Standard on Identity and Credential Assurance of the Directive on Identity Management.

B.2.3.2 **Access management:** Implement measures to ensure that access to information (electronic data) and information systems is limited to authorized users who have been security-screened at the appropriate level and who have a need for access:

B.2.3.2.1 Establish approval, notification, monitoring and operational requirements and procedures for the

creation, activation, modification, periodic review, and disabling or deletion of information system accounts;

B.2.3.2.2 Define access privileges based on departmental security requirements and the principles of least privilege, segregation of duties, and acceptable use of government information systems;

B.2.3.2.3 Inform authorized users of expectations for acceptable use of government information systems, of monitoring practices being applied, and of the consequences for unacceptable use of those systems;

B.2.3.2.4 Establish measures to control the use of accounts that have administrative privileges, including restricting the number of users who have administrative privileges, and restricting the information systems, networks and applications that can be accessed and the operations that can be performed using privileged accounts;

B.2.3.2.5 Verify that individuals who are authorized to conduct privileged operations, such as setting or changing access privileges and implementing or maintaining other IT security controls, are not permitted to alter records of these operations and have been security-screened commensurate with their access level; and

B.2.3.6 Review access privileges periodically, and remove access when it is no longer required (for example, when an employee leaves or changes responsibilities).

B.2.3.3 **Security in IT configuration management:** Manage the configuration of information systems to maintain known and approved system and component designs, settings, parameters and attributes:

B.2.3.3.1 Ensure that change management practices consider security impacts that may result from proposed changes;

B.2.3.3.2 Design and configure information systems to provide only required capabilities and to specifically prohibit, disable or restrict the use of

unnecessary functions, ports, protocols and services;

B.2.3.3.3 Establish measures to ensure that only authorized applications and application components are installed and executed on information systems and their components; and

B.2.3.3.4 Establish measures to ensure that only authorized hardware and devices are connected to, or have access to, information systems and their components.

B.2.3.4 **Secure data storage management:** Implement measures to protect information on electronic media and electronic storage devices at rest (for example, in use or in storage), in transit (for example, in transport or in transmittal), and through appropriate sanitization or destruction before reuse or disposal of the equipment, commensurate with the sensitivity of the information and in accordance with departmental practices:

B.2.3.4.1 Identify secure electronic storage, transportation, transmittal, sanitization and destruction devices, methods and services that are authorized for use in the department, including but not

limited to portable storage devices; and

B.2.3.4.2 Implement appropriate safeguards where other devices, methods or services are used for operational purposes, subject to approval by an individual who has the required authority.

B.2.3.5 **Physical and environmental protection:** Implement measures to protect information systems, their components, and the information processed from physical and environmental threats, commensurate with the sensitivity of the information:

B.2.3.5.1 Implement appropriate physical and environmental safeguards in facilities where information systems are developed, operated, maintained or stored;

B.2.3.5.2 Place physical information system components in appropriate physical security zones; and

B.2.3.5.3 Use emanations security or other measures, as required, to protect information systems from information

leakage owing to the emanation of electromagnetic signals.

B.2.3.6 **System and communications protection:** Implement measures to protect information systems and their components, as well as the information they process and transmit, from internal and external network-based threats, such as threats related to the use of public networks, wireless communications and remote access:

B.2.3.6.1 Define and establish security zones to maintain appropriate separation within physical and virtual IT environments, and ensure that information systems (including virtual instances) that reside in these environments are provided with consistent protection levels that are commensurate with the threat type and level, the sensitivity of the information, and other pertinent security considerations, such as criticality of services and activities supported by the information system;

B.2.3.6.2 Restrict the number of discrete external connections to departmental networks to the minimum necessary to meet departmental and government requirements; and

B.2.3.6.3 Use encryption and network safeguards to protect the confidentiality of sensitive data transmitted across public networks, wireless networks or any other network where the data may be at risk of unauthorized access.

B.2.3.7 **System and information integrity management:** Implement measures to protect information systems, their components and the information they process and transmit against attacks that leverage vulnerabilities in information systems to affect their integrity and that could have an impact on their availability or confidentiality (for example, malicious code):

B.2.3.7.1 Monitor information systems to detect attacks and indicators of potential attacks; unauthorized local, network and remote connections; and unauthorized use of IT resources;

B.2.3.7.2 Identify, document and report vulnerabilities in information systems and their components to the responsible security functional specialist and others, as defined in the department's security governance and security event management processes;

B.2.3.7.3 Analyze impacts of identified vulnerabilities, and implement corrective actions (for example, apply patches and updates, in accordance with defined timelines and, as required, on an emergency basis);

B.2.3.7.4 Coordinate processes for managing vulnerabilities in information systems with departmental and government-wide security event management processes;

B.2.3.7.5 Use, review and regularly update measures to prevent, detect and eliminate malicious code (for example, viruses) in information systems and their components; and

B.2.3.7.6 Establish source authentication and other mechanisms, where required, to ensure that information (for example, messages and financial transactions) can be attributed to an authorized individual.

B.2.3.8 **Information system audit management:** Create, protect and retain information system audit logs and records to enable monitoring, reporting, analysis, investigation and implementation of corrective actions, as required,

for each system, in accordance with departmental practices:

B.2.3.8.1 Implement measures to enable user activities to be authoritatively audited, to ensure that users are accountable for their activities; and

B.2.3.8.2 Monitor the acceptable use of government information systems, regardless of location of access or system used, and report through appropriate channels potential instances of unacceptable use in the department.

B.2.3.9 **Security in IT maintenance:** Ensure that the maintenance of information systems and their components is authorized and recorded and that the maintenance conforms to departmental security practices:

B.2.3.9.1 Ensure that individuals performing maintenance have appropriate authorization, access and direction in the performance of their duties.

B.2.3.10 **IT continuity management:** Establish mechanisms to enable information systems to maintain or return to defined service levels, as applicable:

B.2.3.10.1 Define recovery strategies and restoration priorities for data and information systems, in accordance with departmental business continuity requirements;

B.2.3.10.2 Implement measures to meet identified recovery strategies and restoration priorities; and

B.2.3.10.3 Test IT continuity management mechanisms to ensure an acceptable state of preparedness as an integral element of practices for departmental business continuity management.

B.2.4 **Security in IT project management:** Integrate security considerations into all phases of IT project management to ensure that the security needs of programs and services are considered and addressed when developing, implementing or upgrading information systems.

B.2.5 **Security in the information system life cycle, and integrity of the IT supply chain:** Identify and address security requirements, activities and gating requirements throughout all stages of the information system life cycle, including definition, design, development and procurement, operations, maintenance and decommissioning:

B.2.5.1 Integrate system security engineering and security design processes at the appropriate

stages of the system development lifecycle process;

B.2.5.2 Implement supply chain security measures to establish and maintain reasonable confidence in the security of sources of information systems and IT components, in accordance with applicable security requirements;

B.2.5.3 Identify and address any risks regarding transmission, processing or storage of data, both internal and external to Canada, when planning for an information system, including the complete life cycle of the system; and

B.2.5.4 For information systems managed for or by another organization, and for information systems shared or interconnected by two or more organizations, establish documented arrangements that define applicable security requirements and respective security responsibilities.

B.2.6 **IT security assessment and authorization:** Implement IT security assessment and authorization processes to establish and maintain confidence in the security of information systems that are used or managed by the department, while considering stakeholder security requirements:

B.2.6.1 Assess whether security controls are effective and whether applicable security requirements are met;

B.2.6.2 Implement and document risk mitigation measures when security requirements cannot be fully met before putting an information system into operation, subject to approval by an individual who has the required authority;

B.2.6.3 Authorize an information system before putting it into operation through established IT security assessment and authorization processes;

B.2.6.4 Document security assessments and authorization decisions, including the formal acceptance of residual risk by an individual who has the required authority; and

B.2.6.5 Evaluate and maintain authorization throughout the information system's operational life cycle.

B.2.7 **Monitoring and corrective actions:** Maintain an effective IT security posture:

B.2.7.1 Monitor threats and vulnerabilities;

B.2.7.2 Analyze information system audit logs and records;

B.2.7.3 Review the results of system monitoring, security assessments, tests and post-event analysis; and

B.2.7.4 Take pre-emptive, reactive and corrective actions to remediate deficiencies and ensure that IT security practices and controls continue to meet the needs of the department.

Appendix C: Mandatory Procedures for Physical Security Control

C.1 Effective Date

C.1.1 These procedures take effect on July 1, 2019.

C.2 Procedures

C.2.1 These procedures provide details on the requirements to support the deputy head accountability.
The procedures and subsections are as follows:

Procedure	Subsection
Physical security requirements and practices	C.2.2
Physical security controls	C.2.3
Security in the real property and materiel management life cycles	C.2.4
Facility security assessment and authorization	C.2.5
Security inspections	C.2.6
Arrangements	C.2.7
Monitoring and corrective actions	C.2.8

C.2.2 **Physical security requirements and practices:** Define, document and maintain departmental physical security requirements and practices:

C.2.2.1 For all departmental materiel, materiel held in trust by the department, and other movable assets that support government programs, services and activities, including IT assets, controlled goods, heritage assets, communications security (COMSEC) material, acquisition cards, travel cards, cash, negotiable instruments and any other valuable or sensitive assets:

C.2.2.1.1 Assign a security category to assets commensurate with the degree of injury that could reasonably be expected as a result of their compromise, and group, where appropriate, assets of equivalent sensitivity (see Appendix J: Standard on Security Categorization);

C.2.2.1.2 Identify and assess threats to which assets are exposed; and

C.2.2.1.3 Define and document requirements for ensuring the protection of assets under the custody or control of the department throughout their life cycle, commensurate with potential impacts

of a compromise and identified threats, and in accordance with applicable legislation, policies, contracts, agreements and memoranda of understanding;

C.2.2.2 For all facilities that support departmental programs, services or activities, or for which the department has custodial responsibility:

C.2.2.2.1 Identify relevant information, asset and employee protection and business continuity requirements;

C.2.2.2.2 Identify and assess threats to which facilities are exposed; and

C.2.2.2.3 Define and document requirements for ensuring the protection of departmental facilities throughout their life cycle, commensurate with identified security requirements and threats, and in accordance with applicable legislation, policies, contracts, agreements and understandings; and

C.2.2.3 Define and document departmental security practices for implementing and maintaining physical security controls, including practices for conducting facility security assessment and

authorization, and security inspections of facilities, in accordance with departmental security requirements.

C.2.3 **Physical security controls:** Define, document, implement and maintain security controls to meet departmental physical security requirements, in accordance with departmental practices.

C.2.3.1 **Design of the facility environment:** Design, integrate and manage the external and internal environments of a facility to create conditions that together with specific security controls, detect attempted or actual unauthorized entry and activate an effective response to meet departmental security requirements, including electronic surveillance.

C.2.3.2 **Access management:** Implement measures to ensure that access to information in physical form, government facilities and other assets, including sensitive equipment, telecommunications cabling and information systems, is restricted to authorized individuals who have been security-screened at the appropriate level and who have a need for access:

C.2.3.2.1 Issue identification to employees;

C.2.3.2.2 Issue access cards to employees and other individuals to identify the facility

or zone to which the bearer has authorized access, as applicable;

C.2.3.2.3 Define and establish a discernable hierarchy of physical security zones to progressively control access, and provide consistent protection levels that are commensurate with the threat type and level and with the sensitivity of the programs, services, activities, information or assets in each zone;

C.2.3.2.4 Authorize, control and monitor individuals and assets entering and, where appropriate, exiting government facilities, zones and sensitive areas, and maintain records of these activities, in accordance with departmental security practices and with records retention and disposition schedules; and

C.2.3.2.5 Review access privileges periodically, and remove access when it is no longer required (for example, when an employee leaves or changes responsibilities).

C.2.3.3 **Secure storage, transport, transmittal and destruction:** Implement measures to protect information in physical form, including assets at

rest (for example, in use or in storage), in transit (for example, in transport or in transmittal), and through appropriate destruction, in accordance with their sensitivity and with departmental security practices:

C.2.3.3.1 Identify authorized secure physical storage, transportation, transmittal and destruction devices, methods and services for use in the department;

C.2.3.3.2 Implement appropriate safeguards where other devices, methods or services are used for operational purposes, subject to approval by an individual who has the required authority; and

C.2.3.3.3 Where appropriate, apply relevant security markings to sensitive assets to alert users of the level of protection that should be applied to the asset.

C.2.3.4 **Additional controls:** Implement additional controls, as required, to meet departmental security requirements or to achieve a higher readiness level in the event of emergencies or increased threat situations (for example, screening of incoming mail or deliveries for suspicious packages, special discussion areas, secure rooms, technical surveillance

countermeasures, emergency destruction instructions, and measures for safeguarding sensitive or valuable information or assets).

C.2.4 **Security in the real property and materiel management life cycles:** Integrate security considerations into real property and materiel management processes and throughout all stages of the facility and materiel management life cycles:

C.2.4.1 Integrate security considerations into the planning, site selection, design, procurement, contracting, construction, modification, operation and maintenance of facilities; and

C.2.4.2 Integrate security considerations when assessing requirements, analyzing options and planning the acquisition, operation, use, maintenance, disposal and replacement of materiel.

C.2.5 **Facility security assessment and authorization:** Implement facility security assessment and authorization processes to establish and maintain confidence in the security of facilities that are used, occupied or managed by the department, while considering stakeholder security requirements:

C.2.5.1 Assess whether security controls are effective and whether applicable security requirements are met;

C.2.5.2 Implement and document risk mitigation measures when security requirements cannot be fully met before putting a facility into operation, subject to approval by an individual who has the required authority;

C.2.5.3 Authorize facilities before putting them into operation through established facility security assessment and authorization processes;

C.2.5.4 Document security assessments and authorization decisions, including the formal acceptance of residual risk by an individual who has the required authority; and

C.2.5.5 Evaluate and maintain authorization throughout the use, occupancy and maintenance of a facility.

C.2.6 **Security inspections:** Conduct security inspections in facilities where sensitive or valuable information or assets are handled or stored or in facilities that support critical services or activities, to verify compliance with departmental security practices:

C.2.6.1 Ensure that security inspections are conducted by authorized persons and in accordance with defined processes and timelines;

C.2.6.2 In emergency or increased threat situations, increase the frequency or depth of security inspections to achieve a higher readiness level; and

C.2.6.3 Report issues of non-compliance in accordance with defined processes to enable the implementation of corrective actions, and report to the responsible authorities, as applicable.

C.2.7 **Arrangements:** Establish documented arrangements (for example, lease or occupancy agreements) that define pertinent security requirements and respective security responsibilities where the department relies on or supports another organization, including but not limited to other federal departments, other orders of government, and private sector suppliers and partners, to meet departmental physical security requirements:

C.2.7.1 For facilities where the department is the building custodian:

C.2.7.1.1 Define base building security requirements;

C.2.7.1.2 Provide base building security;

C.2.7.1.3 Inform any tenants of the base building security provided in tenant-occupied facilities;

C.2.7.1.4 Consider tenant security requirements when conducting site selection; and

C.2.7.1.5 Coordinate the integration of additional safeguards into base

building infrastructure to meet tenant security requirements;

C.2.7.2 For facilities where the department is a tenant:

C.2.7.2.1 Define tenant security requirements, while considering resources and activities in tenant-occupied facilities, in consultation with other stakeholders with whom facilities are shared, as applicable;

C.2.7.2.2 Inform the custodian department of its tenant security requirements, to support site selection and tenant fit-up; and

C.2.7.2.3 Verify that additional safeguards have been integrated into base building infrastructure to meet tenant security requirements;

C.2.7.3 For multi-tenant facilities occupied or managed by the department, establish or verify that mechanisms are in place to enable the coordination of security activities, including a building security committee, alignment of the hierarchy of security zones for common areas, identification of responsibilities of the lead tenant, and security event management processes; and

C.2.7.4 When individuals from another department or organization require regular access to facilities occupied or managed by the department, establish or verify that mechanisms are in place to address security requirements and enable the coordination of security activities, including security screening, access management and security event management.

C.2.8 **Monitoring and corrective actions:** Maintain an effective physical security posture:

C.2.8.1 Monitor threats and vulnerabilities;

C.2.8.2 Analyze access records;

C.2.8.3 Review the results of security assessments, security inspections and post-event analysis; and

C.2.8.4 Take pre-emptive, reactive and corrective actions to ensure that physical security practices and controls continue to meet the needs of the department.

Appendix D: Mandatory Procedures for Business Continuity Management Control

D.1 Effective date

D.1.1 These procedures take effect on July 1, 2019.

D.2 Procedures

D.2.1 These procedures provide details on the requirements to support the deputy head accountability.

D.2.2 Procedures are as follows:

D.2.2.1 **Business continuity management practices:** Define, document and maintain departmental business continuity management practices, addressing:

a. Processes for conducting business impact analysis and for developing business continuity plans, measures and arrangements;
b. Coordination of business continuity management with security event management and emergency management activities;
c. Processes and timelines for providing awareness and training and for testing business continuity plans, measures and arrangements;
d. Coordination with partners and other stakeholders; and
e. Processes and timelines for review and maintenance of business impact analysis and business continuity plans, measures and arrangements.

D.2.2.2 **Business impact analysis:** Define departmental business continuity management requirements for all departmental services and activities supporting continued availability of services and associated assets that are critical to the health, safety, security or economic well-being of Canadians or to the effective functioning of government, based on an analysis of the potential impacts of disruption:

D.2.2.2.1 Assign a security category to services and activities commensurate with the degree of injury that could reasonably be expected as a result of their interruption or degradation, and, where appropriate, group services and activities of equivalent criticality (see Appendix J: Standard on Security Categorization);

D.2.2.2.2 Liaise with clients (for services provided to another department) and other stakeholders who may be affected by disruptions in departmental services or activities, to inform them of continuity requirements, strategies and priorities;

D.2.2.2.3 Provide information to the Treasury Board of Canada Secretariat, on a

regular basis or when requested, regarding the department's identified critical services and activities;

D.2.2.2.4 Define business continuity management requirements, expressed as maximum allowable downtime, minimum service levels, recovery time objectives and recovery point objectives;

D.2.2.2.5 Define continuity strategies and recovery priorities;

D.2.2.2.6 Identify supporting resources, including employees, contractors, suppliers, information and assets such as information systems, materiel and facilities, including where the department relies on or supports another organization in delivering a service or activity; and

D.2.2.2.7 Identify any existing operational plans that support business continuity management requirements.

D.2.2.3 **Business continuity plans, measures and arrangements:** Establish business continuity plans, measures and arrangements based on the results of the business impact analysis.

D.2.2.4 **Awareness and training:** Provide awareness and training to all individuals, including specialized training for individuals directly involved in the implementation of business continuity plans, in accordance with departmental practices.

D.2.2.5 **Testing:** Conduct regular testing of business continuity plans to ensure an acceptable state of preparedness, in accordance with departmental practices.

D.2.2.6 **Monitoring and corrective actions:** Review and maintain business impact analysis and business continuity plans, measures and arrangements, while considering changes in services, activities, resources or threat environment, based on the results of tests and the activation of plans, to ensure business continuity management practices continue to meet the needs of the department.

Appendix E: Mandatory Procedures for Information Management Security Control

E.1 Effective date

E.1.1 These procedures take effect on July 1, 2019.

E.2 Procedures

E.2.1 These procedures provide details on the requirements to support the deputy head accountability.

E.2.2 Procedures are as follows:

E.2.2.1 **Information management requirements and practices:** Define, document and maintain departmental information management security requirements and practices.

E.2.2.1.1 For all governmental information resources and intellectual property, including transitory records; information received from Canadian citizens, private sector organizations, other orders of government, international organizations or other partners; information that constitutes controlled goods; COMSEC material; and other information that supports government programs, services and activities:

a. Assign a security category to departmental information resources commensurate with the degree of injury that could reasonably be expected as a result of its compromise,

and group, where appropriate, information resources of equivalent sensitivity (see Appendix J: Standard on Security Categorization);

b. Identify and assess threats to which departmental information resources are exposed; and
c. Define and document requirements for ensuring the protection of information resources under the custody or control of the department throughout their life cycle, commensurate with potential impacts of a compromise and identified threats, and in accordance with applicable legislation, policies, contracts, agreements and memoranda of understanding;

d. Define and document departmental security practices for implementing and maintaining information management security controls, in accordance with departmental security requirements.

E.2.2.2 **Information management security controls:** Define, document, implement and maintain security controls to meet departmental information management security requirements, in accordance with departmental practices.

E.2.2.2.1 **Security marking:** Apply security markings to alert users of the level of protection that should be applied to the information:

a. Apply security markings at the time that information is created or collected, based on the assigned security category and any applicable caveats; and
b. Apply security markings to information in physical and electronic form and, where required, to

electronic media and storage devices that contain sensitive information.

E.2.2.2.2 **Downgrading and upgrading:** Ensure that the time frame for protection of information is kept as short as possible and that the security category continues to reflect the potential impacts of a compromise:

a. Where appropriate and in accordance with privacy requirements and other legal or policy obligations, downgrade the security category assigned to information resources when the expected injury is reduced;
b. Consult the relevant authority before downgrading any information that originates from another organization;
c. When downgrading information received from other orders of government, private

sector organizations or international organizations, abide by agreements or memoranda of understanding with these governments or organizations; and

d. Where appropriate, upgrade the security category assigned to information resources when the expected injury is increased.

E.2.2.2.3 **Additional controls:** Implement additional controls, as required, to meet departmental security requirements.

E.2.2.3 **Security in the information management life cycle:** Integrate security considerations into information management processes throughout all stages of the information life cycle, including planning, creation, receipt, organization, use, dissemination, maintenance, transfer and disposition.

E.2.2.4 **Monitoring and corrective actions:** Monitor information management security practices and

controls to ensure consistent application, and implement changes, as required, to ensure that these practices and controls continue to meet the needs of the department.

Appendix F: Mandatory Procedures for Security in Contracts and Other Arrangements Control

F.1 Effective date

F.1.1 These procedures take effect on July 1, 2019.

F.2 Procedures

F.2.1 These procedures provide details on the requirements to support the deputy head accountability.
The procedures and subsections are as follows:

Procedure	Subsection
Security in the procurement or arrangement process	F.2.2
Security requirements for contracts and information-sharing arrangements	F.2.3
Verifying compliance	F.2.4
Monitoring and corrective actions	F.2.5

F.2.2 **Security in the procurement or arrangement process:**
Define, document and maintain departmental security

practices for procurement and the establishment of information- or asset-sharing arrangements:

F.2.2.1 Define department-wide security requirements that should apply to all contracts or arrangements;

F.2.2.2 Establish a process for identifying security requirements for a specific contract or arrangement;

F.2.2.3 Establish a process for verifying and monitoring continued compliance with security requirements, including any permitted exceptions and risk mitigation measures, as applicable; and

F.2.2.4 Integrate security considerations into departmental procurement processes and into information management, asset management and program management processes, while considering information- and asset-sharing arrangements.

F.2.3 **Security requirements for contracts and information-sharing arrangements:** Identify and document security requirements for all contracts and arrangements:

F.2.3.1 Determine security requirements based on the sensitivity of information, assets or sites to which individuals will require access; the location and the type of work to be performed; the need for the supplier, partner or department to safeguard,

process or produce sensitive information or assets at its facilities or in its information systems; and other relevant factors:

F.2.3.1.1 Security screen individuals who require access to sensitive information, assets or sites in the performance of their work; individuals who need to be relied on to produce and deliver the goods and services being procured; and individuals who, because of their position, could gain access to sensitive information, assets or sites or could adversely affect the delivery of goods and services, including supplier security points of contact and, for certain contracts, suppliers' key senior officials;

F.2.3.1.2 Verify and obtain assurance of the appropriate implementation of;

a. Physical security controls in facilities that are used to store or produce sensitive information or assets or that need to be relied on to produce or deliver the goods or services being procured;

b. Security controls to protect information systems that are used to electronically process or transmit sensitive information or that are relied on to produce or deliver the goods or services being procured;
c. Administrative and operational security controls (including designation of security points of contact, governance, planning, management of subcontracts or arrangements with third parties, security awareness and training, and security event monitoring, reporting and response, as applicable);
d. Any other specific security requirements to meet statutory, regulatory or other obligations (for example, requirements for the management of

COMSEC material; international or defence contracts that are subject to negotiated treaties, international agreements and multinational arrangements; and requirements where duties or access to information, assets or facilities are related to or directly support security and intelligence functions); and

e. Risk-based approach for verifying and monitoring supplier, partner and departmental compliance with security requirements, as applicable.

F.2.3.2 Identify security requirements in the documentation associated with a contract or arrangement:

F.2.3.2.1 For contracts and other arrangements with suppliers, document security requirements in the Security Requirements Check List or an

equivalent document and in other documentation associated with the contract or arrangement;

F.2.3.2.2 For other types of arrangements, document security requirements in the arrangement;

F.2.3.2.3 For contracts or arrangements involving a subcontractor or another third party, identify in the contract or arrangement the need for the supplier or partner to extend applicable security requirements to any other entity involved in fulfilling the contract or arrangement; and

F.2.3.2.4 For contracts or arrangements that do not involve any security requirements, include an attestation to that effect in the documentation of the contract or the arrangement.

F.2.4 **Verifying compliance:** Confirm and document compliance with security requirements before awarding a contract or entering into an arrangement and before granting access to sensitive information, assets or sites, as applicable:

F.2.4.1 Verify compliance with, and obtain assurance of the implementation of, the security requirements using the risk-based approach defined for the

contract or arrangement. To avoid duplication, where possible and in accordance with privacy requirements and other legal or policy obligations:

F.2.4.1.1 Provide the security records of Government of Canada suppliers to internal enterprise service organizations and other departments; and

F.2.4.1.2 Consult the security records of Government of Canada suppliers when verifying supplier compliance;

F.2.4.2 Implement and document risk mitigation measures when security requirements to limit access to sensitive information, assets or sites cannot be fully met before awarding a contract or entering into an arrangement, subject to approval by an individual who has the required authority; and

F.2.4.3 Establish documented arrangements that define respective security responsibilities for contracts or arrangements managed for or by another organization.

F.2.5 **Monitoring and corrective actions:** Monitor supplier, partner and departmental compliance with security requirements throughout the contracting or arrangement

process, using the risk-based approach defined for the contract or arrangement, and take corrective actions to address issues of non-compliance, security incidents or other security events.

Appendix G: Mandatory Procedures for Security Event Management Control

G.1 Effective date

G.1.1 These procedures take effect on July 1, 2019.

G.2 Procedures

G.2.1 These procedures provide details to support the deputy head accountability.
The procedures and subsections are as follows:

Procedure	Subsection
Departmental security event management practices	G.2.2
Security event reporting	G.2.3
Security in emergency and increased threat situations	G.2.4
Administrative investigations of security events	G.2.5
Post-event analysis	G.2.6
Security event records	G.2.7

G.2.2 **Departmental security event management practices:** Define, document and maintain departmental security event management practices:

G.2.2.1 Define security event management processes, including responsibilities of all stakeholders, with consideration given to partners (for example, other departments, suppliers and other orders of government) and government-wide processes;

G.2.2.2 Designate an official departmental contact to support government-wide communications of threats and vulnerabilities, and responses to security incidents and other security events, in accordance with government-wide processes;

G.2.2.3 Establish resources to support the implementation of security event management processes and to enable secure exchange of relevant information within the department and with other stakeholders;

G.2.2.4 Implement measures to ensure that security event management processes can be triggered in the event of disruptions that affect their supporting resources;

G.2.2.5 Coordinate security event management processes with communications plans and with business continuity, emergency management, strike

management, and other contingency plans and measures, as applicable; and

G.2.2.6 Test security event management processes to ensure preparedness and to support continuous process improvement.

G.2.3 **Security event reporting:** Assess, document, report and share information related to threats, vulnerabilities, security incidents and other security events, in accordance with departmental and government-wide processes (see Appendix I: Standard on Security Event Reporting):

G.2.3.1 Ensure that reporting and sharing of information related to threats, vulnerabilities, security incidents and other security events is restricted to authorized users who have been security-screened at the appropriate level and who need to access the information to ensure appropriate preparedness, response or recovery; is effected using mechanisms that provide protection commensurate with the sensitivity of the information and threats to which the information may be exposed; and is conducted within the bounds of applicable legislation, policies or other obligations;

G.2.3.2 Report security events that affect, or that have the potential to affect, government-wide preparedness, response or recovery, to the

appropriate lead security agency or central agency;

G.2.3.3 Report all suspected criminal activity, including but not limited to theft and breach of trust, to the appropriate law enforcement authority; provide all relevant documents, materials and details; and follow protocols to ensure preservation of evidence and cooperation between the department and law enforcement authorities; and

G.2.3.4 Inform other departments and stakeholders when there is reason to believe that an event originated from, or could potentially affect, an organization, including internal enterprise service organizations, departments that provide or receive services under agreements or other arrangements, suppliers and other partners.

G.2.4 **Security in emergency and increased threat situations:** Define, document and implement processes and measures to achieve and maintain a baseline readiness level, and to enable increased levels of security in the event of an emergency or increased threat situation to prevent or minimize impacts and potential losses:

G.2.4.1 Apply defined readiness levels based on the level of threat to Government of Canada employees, information, assets or service delivery;

G.2.4.2 Identify responsibilities for all departmental employees who have responsibilities for implementing readiness processes and measures:

G.2.4.2.1 Designate the departmental contact for security event management as the official liaison for purposes of declaring and applying heightened readiness levels within the department;

G.2.4.3 Report, without delay, a declaration of a higher readiness level and a return to lower levels of readiness to the Privy Council Office, in accordance with **Appendix I: Standard on Security Event Reporting**;

G.2.4.4 Implement changes in readiness level when directed by the Privy Council Office, in response to emergency and increased threat situations that may affect multiple departments,national security and the government as a whole; and

G.2.4.5 Coordinate readiness processes and measures with security event management processes and business continuity plans and with emergency preparedness and response measures.

G.2.5 **Administrative investigations of security events:** Conduct thorough and impartial administrative investigations of security incidents and other security events of significance in a manner that ensures the protection of evidence, respects

the rights of individuals, and does not hinder potential civil or criminal proceedings:

G.2.5.1 Define practices for the conduct of administrative investigations of security events;

G.2.5.2 Inform parties who are involved in administrative investigations of security events of their rights and obligations; and

G.2.5.3 Conduct administrative investigations of security events independently of, and without any specific intent to advance, a criminal investigation in order to avoid compromising such investigations.

G.2.6 **Post-event analysis:** Conduct analysis following security incidents and other security events of significance, to enable the application of corrective actions and to support process improvement:

G.2.6.1 Communicate results of post-event analysis to the appropriate lead security agency or central agency, as applicable and based on the severity and scope of the event.

G.2.7 **Security event records:** Maintain thorough records on all security incidents and other security events of significance, including identification of the programs, services, activities and resources affected; an assessment of the severity and scope of the impacts (degree of injury); findings of administrative investigations; and the results of post-event analysis:

G.2.7.1 Apply protective measures to ensure that access to security event records is restricted to security officials and other authorized users, to maintain the integrity of these records.

Appendix H: Mandatory Procedures for Security Awareness and Training Control

H.1 Effective date

H.1.1 These procedures take effect on July 1, 2019.

H.2 Procedures

H.2.1 These procedures provide details on the requirements to support the deputy head accountability.

H.2.2 Mandatory procedures are as follows:

H.2.2.1 **Security awareness requirements and practices:** Define, document and maintain departmentalsecurity awareness and training requirements and practices, in accordance with government-wide policy requirements.

H.2.2.2 **Security awareness:** Develop, deliver, document and maintain security awareness activities and products to inform and remind individuals of security threats and risks and of their security responsibilities, in accordance with departmental security awareness requirements.

H.2.2.3 **Security training:** Provide, or arrange and document the provision of, security training to all employees, including specialized security training for those individuals who have specific security responsibilities or who could affect the achievement of security objectives as part of their duties, in accordance with departmental security training requirements.

H.2.2.4 **Monitoring and corrective actions:** Assess the effectiveness of security awareness and training activities, and implement changes, as required, to ensure that these activities continue to meet the needs of the department.

Appendix I: Standard on Security Event Reporting

Provides details on Government of Canada organizations that must be contacted to report different types of security events. The Standard on Security Event Reporting can be found here: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32613

Appendix J: Standard on Security Categorization

Provides details on the types of security categories that must be applied to different types of assets, information, or services. The Standard on Security Categorization can be found here: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32614

Appendix K: Definitions

Definitions to be used in the interpretation of this directive can be found in Appendix B of the Policy on Government Security.

ISBN:

Date modified: 2019-07-01