CMHC Information Technology Security Policy
Senior Management Level

Policy Sponsor/Owner: Chief Information Officer
Effective Date: February 2018

Version 1.0

Protected – Operations/Proprietary

Canada

CMHC SCHL
HOME TO CANADIANS

SUMMARY PAGE

Policy Category[1]	Senior Management – Enterprise-Wide policy
Policy Name	Information Technology (IT) Security Policy
Purpose of Policy	To provide CMHC with a direction for identifying, measuring, managing/mitigating, monitoring and reporting security risks associated with IT activities within sectors, across the organization and when engaging with external entities.
Approval Authority and Date	Executive Committee February 2018
Policy Creation Date	February 2018
Previous Review Date	N/A
Transition Timeframe	Gradual implementation in 2017 with full implementation no later than March 2018. All personnel with access to CMHC's data and/or its network will be required to complete security training by Q4 2018.
Review Cycle	Annual
Policy Sponsor / Owner	Chief Information Officer

[1] Policy categories include Board-level policies and Senior Management policies (Enterprise-wide policies or Business/Support Function policies).

TABLE OF CONTENTS

1. Introduction and Purpose

CMHC is committed to the protection of its information assets and technology infrastructure which support the Corporation's mandate. CMHC recognizes that Information Technology (IT) enables the Corporation to carry out its business activities and to achieve its strategic directions.

The purpose of this policy is to mitigate risks related to IT security and cybersecurity. These risks are defined in the Operational Risk Taxonomy.

This policy mitigates these risks by establishing policy requirements and related monitoring, reporting and roles & responsibilities. This policy supplements the IT Security requirements in the IT Risk Management policy.

2. Scope and Application

This policy applies to all users of CMHC IT assets, infrastructure and/or data including the Pension Plan and Fund.

Personnel who violate this policy may be subject to disciplinary measures in accordance with CMHC's Disciplinary Measures Policy.

3. Policy Requirements

This policy is an integral part of CMHC's Operational Risk Management Framework (ORMF) described in the Operational Risk Management (ORM) Policy. The ORMF contains a number of tools that are used to identify, assess, manage, monitor and report on IT Risk.

CMHC safeguards against risks associated with IT security that could impact the confidentiality, integrity and/or availability of CMHC assets. CMHC utilizes the ISO27001:2013 standard[2] to establish, implement, maintain and continually improve its Information Security Management System (ISMS), including requirements for assessment and treatment of information security risks. Enhanced security controls, network monitoring tools and data loss prevention techniques included in this policy and the related supporting documentation are part of the overall approach to mitigate risks associated with IT Security.

3.1 Risk Appetite

The Risk Appetite Framework includes all approved Risk Appetite Statements which apply to CMHC's activities and risks.

3.2 IT Security Principles

[2] Standard created by the International Organization for Standardization (ISO) which specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization.

CMHC adheres to the following IT security principles:

- CMHC safeguards and protects information assets and technology infrastructure from loss;
- Assets are protected in accordance with their level of criticality and risk;
- All personal and competitive commercial information is protected at all times in accordance with the Privacy Act and the Access to Information Act;
- All IT activities comply with applicable laws, CMHC's Code of Conduct and standard operating procedures/directives of IT use as per the ISO27001:2013 standard;
- Through effective IT security awareness training, personnel have the knowledge to perform their functions and to safeguard against any IT security threats and;
- Active monitoring and testing of CMHC IT ensures efficient operation, benchmarking performance, isolation and resolution of problems, and compliance with IT sector policies.

3.3 IT Security Management

Risks associated with IT security are mitigated through a series of measures which include (but are not limited to) the use of network monitoring tools, access control mechanisms, training and acceptable use parameters. The policy requirements identified in sub-sections 3.3.1 to 3.3.7 are supported by the directives, outlined in Section 8.

The overall governance of IT security must be consistent with the CMHC Corporate Security program which includes IT security as a core security element (See Corporate Security policy).

3.3.1 Acceptable Use

All personnel must be advised of their responsibilities when utilizing CMHC IT assets and network resources and must comply with established guidelines for usage of social media, removable storage media, Wi-Fi networks and mobile operation.

Personnel must use corporate applications and systems for CMHC business and communications. Limited personal use is permitted when it is conducted on personal time, and not for financial gain, as defined in the Acceptable Use directive.

All personnel must obtain appropriate approvals prior to installing or using any software.

IT Security Division monitors the use of CMHC's electronic network to ensure compliance with the requirements of the Treasury Board, to ensure appropriate use and that confidentiality, integrity and availability of the systems are maintained.

IT Security Division must perform monitoring activities, conduct any necessary reviews or investigations of CMHC's electronic network and report any instances or suspected cases of non-compliance with this policy to the Manager, Security and Business Continuity, Operational Risk Oversight Division and/or to Human Resources.

3.3.2 Access Control

Access controls with respect to information assets and technology infrastructure must be established. This includes the employment of processes and controls such as, but not limited to, trusted platform modules, firewalls, secure portals, Virtual Private Network (VPN) connections etc. that ensure the protection of CMHC's proprietary data against inappropriate user access.

CMHC must restrict access to information assets and technology infrastructure to employees who have been identified, screened, authenticated and authorized, and must keep this access to a level that permits employees to perform their duties. Access to sensitive data (Protected A and above) must be based on the least-privilege principle and must be consistent with the security designation or classification level of the applications and systems being accessed.

Approving, granting and revoking access to CMHC applications, systems and the CMHC network must be done by the system owner and managers. IT Security Division must regularly review and monitor all access (including remote access, mobile access, third party access and cloud/Software as a Service (SaaS).

3.3.3 Awareness & Training

IT Security Division must develop, implement, deliver, maintain and oversee an IT Security Training and Awareness Program to meet the needs of CMHC and ensure that delivery of this program to new and existing personnel is done on a timely basis.

Awareness & Training is governed by the Security and Privacy Awareness Working Group comprised of IT Security, IT Risk &Compliance, Operational Risk Oversight Division, Corporate Security, Privacy and Accenture Security.

Personnel needs for security awareness and training must be identified and defined including orientation training, annual training and specialized training for specific job responsibilities.

3.3.4 Communications

IT Security Division must ensure that management of the CMHC network, including wall outlets, cabling, network devices, firewalls, Wi-Fi access and external access points is performed.

Network management includes supporting, enhancing and ensuring the availability of the network and protecting the confidentiality and integrity of the data traversing the network.

Network services and protocols must be approved and established to support the CMHC traffic including e-mail, file transfer and application/system access.

3.3.5 Cryptography

CMHC must ensure that cryptographic mechanisms are in place to ensure that CMHC information is effectively safeguarded against unauthorized disclosure, modification or misuse, to protect its confidentiality, authenticity and/or integrity and to comply with applicable best practices, policies, directives and standards.

The IT Security Division must manage encryption, which includes, but is not limited to, conducting encryption control risk assessments, selecting and implementing encryption algorithms and managing encryption keys/digital signatures.

3.3.6 Incident Management

IT Security Division must develop incident management processes and procedures to address information, technology and security related incidents. Incidents are categorized based on severity and nature. Categorization from P1 (Priority 1) to P4 (Priority 4) determines the extent of escalation required.

All IT security incidents must be responded to in accordance with incident management directive and must be reported using documented incident management processes and communication channels.

3.3.7 Operations (includes mobile operations)

The IT Security Division must ensure that operational security requirements are defined and in place for CMHC approved mobile devices provided to facilitate CMHC business activities (including, but not limited to laptops, pagers, cellular phones, wireless PDAs, Blackberries, Smartphones, iPads, tablets, mobile modems, and other types of remote access devices).

CMHC information must be password protected and is further protected by established usage guidelines in the Operations directive. The Operations directive must define the day-to-day operational procedures that, in support of the other IT security directives, will manage and mitigate security risks associated with IT operations.

4. Monitoring and Non-Compliance Handling

Monitoring is performed at the macro level to ensure that operational and performance targets are met and that a continuous improvement process can be established to support improved Capability Maturity Models (CMM) for IT security related risks. At the micro level, monitoring of IT security-related events is performed to identify potential areas of non-compliance with this policy and the supporting directives. For additional monitoring details, please refer to IT directives as outlined in Section 8.0, Reference Documents.

Non-compliance with the IT Security Policy must be reported to the Director, IT Security, where the need for additional escalation is assessed depending on the impact and severity of the policy violation.

Actual or possible policy violations and operational risk incidents must be reported to Operational Risk Oversight Division. Material[3] policy violations must be reported in the Quarterly Risk Management Report (QRM) or other reports to senior management and the Board.

Security breaches, are investigated by the Security and Business Continuity group in accordance with the Security and Business Continuity Investigation Directive and reported to the employee's immediate supervisor, with a copy to Employee Relations as required.

5. Exceptions

Exceptions to this policy must be approved by the Chief Information Officer with material[4] exceptions approved by the Chief Risk Officer and reported in risk reporting.

6. Reporting Requirements

Reporting requirements are based on Key Performance Indicators (KPIs), Key Risk Indicators (KRIs) and other factors that provide operational and performance measurements. Specific reports are identified and described in the IT Risk Management Policy.

7. Roles and Responsibilities

Executive Committee

The Executive Committee reviews and approves this policy.

Security & Privacy Advisory Committee (SPAC)

The SPAC's mandate is to provide strategic direction and leadership related to security practices and risk management, to ensure that CMHC's security program is effectively managed across the Corporation, to mitigate risks and minimize vulnerabilities from all threats. As such, the Committee monitors key IT risks and related action plans.

For more detail, refer to the SPAC Terms of Reference.

IT Risk Management Steering Committee

The IT Risk Management Steering Committee is tasked with identifying the key IT risks facing CMHC and determining their importance given their potential impact and likelihood of occurrence. The role of the Committee includes ensuring that CMHC's IT risk level remains

[3] Materiality is determined by the CRO.
[4] Materiality is determined by the CIO.

within CMHC's risk appetite or that operational management is taking appropriate mitigating actions where risk appetite is or is at risk of being breached.

For more detail, refer to the IT Risk Management Steering Committee Terms of Reference.

The following table summarizes roles and responsibilities assigned in this policy, in alignment with the Three Lines of Defence Risk Governance Model.

Role	Responsibilities and Accountabilities
1st line of defence	**IT Security Division (IA Function)** (1A) responsibilities: • Ensure risks are within CMHC's risk appetite • Conduct incident reviews and/or investigations as required • Monitor network access • Develop, implement and deliver IT Security Awareness & Training Program • Manage and monitor use of CMHC networks • Ensure operational security requirements are in place **IT Risk & Compliance (1B Function)** (1B) responsibilities: • Monitor risk management activities performed by 1A; • Monitor compliance with CMHC's risk appetite statements and risk management policies; • Provide input for risk reporting **Security and Business Continuity** • Corporate Security will take the lead on the investigation of incidents categorized as a Priority 1 or 2 and are informed on Priorities 3 and 4. **All System Owners and Managers** • Approve, grant and revoke access
CRO Sector **2nd line of defence**	**Sector of the Chief Risk Officer** The CRO sector challenges and provides oversight that IT security risk is managed to acceptable levels, within CMHC's established risk appetite. **Operational Risk Oversight Division (OROD)** OROD is responsible for: • Guiding and supporting sectors in their efforts to identify, assess, manage, monitor and report on IT security risk;

	• Reporting to Senior Management and the Board quarterly (through the QRM) on IT risk management activities.
Audit & Evaluation **3rd line of defence**	CMHC's Internal Audit function is responsible for providing independent assurance on the effectiveness of governance, risk management, and internal controls.

8. Reference Documents

The following governance documents are referenced in this policy document:

- CMHC Risk Appetite Framework
- CMHC IT Risk Management Policy
- CMHC Corporate Security Policy
- CMHC Operational Risk Management (ORM) Policy
- Disciplinary Measures Policy (available on HR Online)
- Privacy Act
- Access to Information Act
- Operational Risk Taxonomy

Supporting directives for the IT security requirements are as follows:

- Acceptable Use
- Access Control
- Awareness and Training
- Communications
- Cryptography
- Incident Management
- Operations
- Mobile Operations

9. Approval, Review and Revision History

The IT Security Policy is owned by the CIO and will be reviewed annually. This policy will be amended as required, with changes to be approved by the Executive Committee.

Dates/Timing	*Details*
Approval Date	February 2018
Effective Date	February 2018
Review Frequency	Annual
Next Review Date	February 2019

10. Definitions

1. **Access:** Gaining entry to an electronic network that CMHC has provided to personnel. Access to such electronic networks may be from inside or outside CMHC premises. Access may support teleworking and remote access situations, or situations where personnel are using electronic networks provided by CMHC on their own time for limited personal use.

2. **Electronic Network:** Group of computers and systems including without limitation, CMHC electronic data networks, voice and video network infrastructure, service provider networks and public (Internet) and private networks external to the CMHC network. The network includes both wired and wireless components.

3. **Technology Infrastructure:** Physical information technology device in the work environment that is used by personnel to access or perform an automated function or tasks using the CMHC computer or electronic networks and databases. IT assets can include, but are not limited to, the following: desktop workstations, laptops, notebooks, tablets, smart phones, cell phones, peripherals such as printers and scanners, memory devices such as USB flash drives, CD drives and DVD drives, webcams and any other computer hardware devices used to obtain, manipulate, store or send information.

4. **Cybersecurity:** It is the defense of digital information and IT assets against internal and external, malicious and accidental threats. This defense includes detection, prevention and response to threats through the use of software tools and IT services. .

5. **Software as a Service (SaaS):** Software distribution model in which a third-party provider hosts applications and makes them available to customers over the Internet.

6. **Protected A:** Information that could reasonably be expected to cause injury to interests other that the national interest, for example, the name of an individual in conjunction with another piece of information associated with the individual such as date of birth, address, employee number etc.