# Information Security Policy

**Policy:**
Information Security Policy

<table>
<thead>
<tr>
<th>Version No.:</th>
<th>Policy Owner:</th>
<th>Branch:</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.0</td>
<td>Senior Program Consultant, Information Security</td>
<td>Information Security</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Effective Date:</th>
<th>Approval Authority:</th>
<th>Next Revision Date:</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014-07-10</td>
<td>Senior Management Committee</td>
<td>2015-07-10</td>
</tr>
</tbody>
</table>

**Consultation Authorities:**
- Privacy and Legal Services
- ITS Operations Committee
- Manager, Corporate Administration

**Security Classification:**
Public

**Introduction:**
The Canadian Institute for Health Information (CIHI) is committed to protecting the privacy of individuals and ensuring the security of their personal health information.

CIHI is a secondary collector of personal health information. To receive this information, CIHI has entered into bilateral and data-sharing agreements with most provinces and other health care stakeholders across Canada. Pursuant to these agreements, CIHI has contractual obligations to protect the security and confidentiality of the information that it receives from its data providers. As well, CIHI is a prescribed entity under Section 45 of the Ontario’s *Personal Health Information Protection Act* (PHIPA). As a prescribed entity, CIHI is subject to independent oversight by the Ontario Information and Privacy Commissioner and must have its information practices reviewed and approved by the Commissioner every 3 years. This review process provides the Canadian public with the assurance that CIHI’s information management practices comply with PHIPA and with the privacy and security standards of practice expected from that office. CIHI therefore adheres to this and any other applicable privacy legislation.

CIHI is committed to safeguarding its information technology (IT) ecosystem, to securing its data holdings and to protecting health information with administrative, physical and technical security safeguards appropriate to the sensitivity of the information. These safeguards protect CIHI’s data holdings against theft, loss, unauthorized use or disclosure, or unauthorized copying, modification or disposal.

**Purpose:**
The purpose of the Information Security Policy is to provide management with direction and support regarding information security in accordance with business requirements and relevant laws and regulations and to outline the responsibilities of management and staff with respect to information security. For additional information, refer to the Glossary in this document.
Scope:
This policy and all related standards, guidelines and procedures apply to all employees, contractors, consultants, temporary employees and other workers at CIHI.

Policy:
CIHI’s management supports the development and maintenance of an Information Security Program in accordance with business, legal and privacy requirements. This program must comprise the following control objectives and practices:

- A security governance framework;
- Ongoing review of the security policies, procedures and practices implemented;
- An information security awareness and training program for all staff;
- Policies, standards, practices and/or procedures regarding
  - The physical security of the premises;
  - The security of information-processing facilities;
  - The protection of information throughout its lifecycle (creation, acquisition, retention and storage, use, disclosure and disposition);
  - The control of access to information (administrative, physical and technical controls that are required to ensure that information is accessed on a need-to-know basis only);
  - Information systems acquisition, development and maintenance, including the security requirements of information systems, correct processing of applications, cryptographic controls, security of system files, security in development and support procedures and technical vulnerability management;
  - Security audits, including monitoring, maintaining and reviewing system control and audit logs;
  - Network security management, including patch management and change management;
  - Acceptable use of information technology;
  - Backup and recovery;
  - Information security incident management; and
  - The establishment of protection against malicious and mobile code.

Specific obligations and responsibilities of management and staff in support of the Information Security Program are outlined below.

Responsibilities:
The following CIHI positions and groups have specific responsibilities to the Information Security Program:
- All staff
- Senior management
All Staff

All information under the care and control of CIHI is a corporate asset and must be securely managed throughout its lifecycle. The protection of CIHI’s information assets is a basic responsibility of all staff, and staff must understand and agree to their obligation to protect such assets throughout the information lifecycle—creation, acquisition, retention and storage, use, disclosure and disposition (“the lifecycle”). CIHI staff shall create, acquire, retain, store, use, disclose, transfer or destroy information only in accordance with CIHI policies, standards and guidelines, and applicable legislation.

Staff must at all times engage in practices that are consistent with published information security policies, procedures, standards and guidelines. Additionally, staff are obliged and expected to report all privacy and information security incidents and breaches immediately upon learning of them. (For more information, refer to CIHI’s Privacy and Security Incident Management Protocol.)

Senior Management

Senior management shall provide the necessary guidance and support for the development and maintenance of the Information Security Program, in line with privacy and legal requirements and business strategy objectives.

This support includes, but is not limited to, the following:

- Integrating information security goals into relevant processes;
- Providing clear direction and visible management support for security initiatives;
- Providing the resources required for information security; and
- Approving assignment of specific roles and responsibilities for information security across the organization.

Vice President and Chief Technology Officer

The vice president and chief technology officer (CTO) has overall responsibility for information security and represents CIHI’s Executive Committee. This person will ensure that information security goals are identified, that they meet organizational requirements and that they are addressed within the Information Security Program.

Chief Information Security Officer

Reporting to the vice president and CTO, the chief information security officer (CISO) is responsible and accountable for leading CIHI’s Information Security Program, including defining goals, objectives and metrics consistent with the corporate Strategic Plan and CIHI’s Privacy Program to ensure that the organization’s security principles, policies, procedures and practices support the protection of the organization’s information. The CISO will manage and coordinate the design, implementation, operation and maintenance of CIHI’s Information Security Management System (ISMS) within the defined scope. In addition, the CISO will actively foster a culture of information security by leading and supporting activities both internally and externally to increase awareness of CIHI’s security principles, policies and procedures.

Director, Human Resources and Administration

The director, Human Resources and Administration is responsible for the physical security of the premises and
for ensuring that records management processes protect the confidentiality, integrity and availability of all paper records maintained by the organization.

Management

At all times, management will protect the confidentiality, integrity, and availability of information assets within its assigned area of control, per CIHI’s privacy and security policies.

Senior Program Consultant, Information Security

The senior program consultant, Information Security is responsible for creating and managing key corporate IT security initiatives, along with corresponding documentation, to ensure the ongoing security and integrity of CIHI’s data holdings in accordance with CIHI’s Privacy and Security Framework and suite of privacy and security policies, procedures, standards and guidelines. This person will also ensure that CIHI is employing effective security practices and is compliant with all industry best practices and the expectations/requirements of key external stakeholders (for example, the Ontario Information and Privacy Commissioner).

Compliance:

CIHI’s Code of Business Conduct describes the ethical and professional behaviour related to work relationships, information (including personal health information) and the workplace. All employees are required to comply with the code, as well as with all of CIHI’s policies, protocols and procedures. Compliance with CIHI’s Privacy and Information Security programs is monitored, and instances of non-compliance with privacy and security policies are managed through the Privacy and Security Incident Management Protocol. Violations of the Code, including violation of privacy and security policies, procedures and protocols are referred to Human Resources, as appropriate, and may result in disciplinary action up to and including dismissal.

Glossary:

Business Record

Business records are defined as any information created, received or maintained as evidence and information by CIHI, in the transaction of business or in the pursuance of legal obligations. Business records may be in physical or electronic form and include, but are not limited to,

- Information collected from data providers, clients and stakeholders;
- Official organizational records;
- Transitory records; and
- Records available to the public owned by CIHI.

Information Asset

For the purposes of this policy, “information” or “information asset” shall include the following:

- All health information maintained by CIHI for the purposes of meeting our mandate; and
- All business records of the organization, regardless of security classification.

Information may be in physical or electronic format.

Information Security

For the purposes of this policy, “information security” is defined as the concepts, techniques, and technical and administrative measures used to protect information assets from deliberate or inadvertent unauthorized acquisition, damage, disclosure, manipulation, modification or loss.

Staff

For the purposes of this policy, “staff” is defined as all full-time, part-time and casual employees of CIHI, including individuals working at CIHI on secondment, students, volunteers, contractors and consultants.
**For More Information:**
Contact DL-InfoSec Branch

### Revision History:

<table>
<thead>
<tr>
<th>Date Y/M/D</th>
<th>Version</th>
<th>Description of Revisions</th>
<th>Approval Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>2008-05-15</td>
<td>0.1</td>
<td>Initial document creation</td>
<td>N/A</td>
</tr>
<tr>
<td>2008-10-20</td>
<td>1.0</td>
<td>Publish document</td>
<td>N/A</td>
</tr>
<tr>
<td>2009-09-23</td>
<td>1.1</td>
<td>Document review and modified Background Information section to reflect CIHI's legislative and contractual obligations to the protection of information, including reference to PHIPA.</td>
<td>PLS</td>
</tr>
<tr>
<td>2009-10-22</td>
<td>1.2</td>
<td>Formal edit</td>
<td>N/A – minor amendment</td>
</tr>
<tr>
<td>2010-01-06</td>
<td>1.3</td>
<td>Formal review and minor style edits</td>
<td>N/A – minor amendment</td>
</tr>
<tr>
<td>2010-01-25</td>
<td>1.4</td>
<td>Include protection of information assets throughout their lifecycle as a basic responsibility of all staff. Add definition of Business Record and minor edit to definition of Information Asset.</td>
<td>N/A – minor amendment</td>
</tr>
<tr>
<td>2011-09-20</td>
<td>1.6</td>
<td>Formal Review Change to new corporate template</td>
<td>N/A – minor amendment</td>
</tr>
<tr>
<td>2013-03-01</td>
<td>1.7</td>
<td>Formal Review Reflect new position of CISO as identified in job description.</td>
<td>N/A – minor amendment</td>
</tr>
<tr>
<td>Date</td>
<td>Version</td>
<td>Change Notes</td>
<td>Approval Status</td>
</tr>
<tr>
<td>------------</td>
<td>---------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For approval at SMC</td>
<td></td>
</tr>
</tbody>
</table>

Version 2.0

Security Classification: Public