AR0200 – INFORMATION SECURITY

Interior Health would like to recognize and acknowledge the traditional, ancestral, and unceded territories of the Dãkelh Dené, Ktunaxa, Nlaka'pamux, Secwépemc, St'át'imc, Syilx, and Tŝilhqot'in Nations, where we live, learn, collaborate and work together.

Interior Health recognizes that diversity in the workplace shapes values, attitudes, expectations, perception of self and others and in turn impacts behaviors in the workplace. The dimensions of a diverse workplace includes the protected characteristics under the human rights code of: race, color, ancestry, place of origin, political belief, religion, marital status, family status, physical disability, mental disability, sex, sexual orientation, gender identity or expression, age, criminal or summary conviction unrelated to employment.

1.0 PURPOSE

The purpose of this policy is to protect and manage Interior Health's (IH) digital information Systems and paper-based records. This is the over-arching policy for Information Security and covers a range of Controls. Topic specific policies and resources provide additional guidance and are referenced throughout this document.

Specifically, this policy:

- establishes a framework to minimize risk and respond effectively to Information Security Incidents.
- protects information by meeting legal and ethical obligations.
- communicates Information Security roles and responsibilities.
- establishes a secure and stable environment for processing, storage, retention and destruction of information.
- guides adherence to Information Security measures.
- determines the status of Information Security management activities ensuring that security risks are effectively managed.

2.0 DEFINITIONS

TERM	DEFINITION
Access	*The ability to view and/or manipulate information on paper or in electronic form, or through dialogue, based on a User's need or right to know the information.*
Confidentiality	*The duty to ensure that personal information is kept private and accessible only to authorized persons.*
Confidential Information	*Any information that identifies an individual or that can be combined with other information to identify an individual. This definition applies to anyone, living or*

	dead. Types of information include patient/client address, telephone number and health card number personal health number (PHN). Any corporate information which has not been authorized for disclosure.
Control	*Any method of managing risk, including policies, procedures, guidelines, practices, standards or organizational structures, which can be of administrative, technical, management, or legal. Control is also a synonym for safeguard or countermeasure.*
Digital Information System or "System"	*The software, hardware, and telecommunications networks used to enable communication and collaborative work; to collect, send or store data. Includes all computers or electronic devices used by IH to collect, store or send information. This includes all computer platforms, but is not limited to, workstations and laptops, tablets, smart phones, cellular telephones, fax machines and printers. Software includes all applications whether developed in-house, commercial off the shelf, or purchased by a User as defined in this policy. All IH processing facilities, on-premises and off-premises are included.*
Encryption	*The process of scrambling data into a completely unreadable format. Only people possessing the correct key can return the data to a readable format. The most effective way to achieve data security.*
Information Security	*The preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation, and reliability can also be involved. In some instances, Information Security also refers to a program within Digital Health.*
Information Security Event or "Event"	*An identified occurrence of a System, service or network state indicating a possible breach of Information Security policy or failure of safeguards, or a previously unknown situation that may be security relevant.*
Information Security Incident	*A single or series of unwanted or unexpected information security Events that have a significant probability of compromising business operations and Threatening Information Security.*
Password	*A form of authentication data that is used in combination with a User-ID to Control Access to a System.*
Privacy	*The right of an individual to determine what information about themselves may be collected, used, and shared with others.*
Staff	*The officers, directors, employees and physicians under the employment of IH.*

Threat	*A potential cause of an unwanted Incident, which may result in harm to a System or organization.*
User	*Any individual who has been authorized and provided Access to an application or platform. This includes any IH Staff, business party, external party, entity, individual directly/indirectly associated with IH in a business relationship; including but not limited to: allied health care professionals, non-IH health-care professionals, students, volunteers, contractors, sub-contractors, researchers, vendors and suppliers.*

3.0 POLICY

3.1 Scope

This policy applies to all Users of the System, paper-based and electronic information, and information in any other format.

This policy applies to all digital information Systems owned or administered by IH or operated by User on behalf of IH.

This policy applies while employed by IH or conducting business for, or on behalf of IH. This policy applies when off-duty and extends beyond the completion of the employment or business relationship.

3.2 Principles

Information Security is a shared responsibility that requires the attention and participation of all Users of the System.

IH must provide clear policy direction for the protection of the System and its Information.

Information Security Controls put in place to protect the Confidentiality, integrity and availability of information must be equivalent with the level of sensitivity, value, and importance of the information being protected.

Information Security Controls must comply with relevant legislative and regulatory requirements.

IH will use established frameworks as the foundation of Information Security management (e.g., NIST Cybersecurity Framework 1.1, ISO/IEC 27002: Code of Practice for Information Security Management).

IH will develop and leverage procedures and technical standards to support this policy.

3.3 Information Security Risk Management

A risk assessment must be conducted before deploying a new System and following any changes thereafter, to identify Vulnerabilities and implement appropriate Controls to mitigate risk.

3.4 Organization of Information Security

3.4.1 Internal Organization

IH will implement and manage an Information Security program to protect Systems and stored Confidential Information. The Information Security program is overseen by the Executive Director, Technology or designate.

The security program will:

- identify Information Security goals, meet organizational requirements, and integrate requirements into relevant processes.
- keep current Information Security and related policies guidelines, procedures and standards.
- monitor the effectiveness of this policy and other related policies, guidelines, procedures and standards.
- direct and manage support for security initiatives.
- provide the resources needed for Information Security.
- assign specific roles and responsibilities to support Information Security.
- initiate plans and programs to maintain Information Security awareness.
- lead the consistent implementation of Information Security Controls across IH.

All Information Security responsibilities must be clearly defined. Individuals with allocated Information Security responsibilities may delegate security tasks to others; however, the individual remains responsible for ensuring that any delegated tasks have been correctly performed.

3.4.2 Independent Review

The IH Information Security program and the effectiveness of Controls, policies, processes, guidelines and procedures must be reviewed independently at minimum every 3 years, or when significant changes

to the security program occur. The independent review will be initiated by the Executive Director, Technology. The review will be carried out by experts in the field of Information Security, such as external contractors specializing in such reviews. This could also include subject matter experts brought in by IH Internal Audit. The results of the independent review must be recorded and reported to the IH Senior Executive Team. If the independent review determines that the approach and implementation to managing Information Security is inadequate or non-compliant with this policy, the Executive Director Technology will take corrective actions as necessary.

3.4.3 Users

The security of IH's Systems and Confidential Information must not be compromised by a User. Access to IH's Systems or facilities by any User external to IH must be controlled and authorized by System owners who are fully accountable for those solutions. System owners must report any significant risks or Threats to Information Security upon notification of risk or Threat. A risk assessment must be carried out to determine security implications and Control requirements before an external User is granted Access to IH Systems or Confidential Information to complete required business needs to obtain or provide a product or services.

Agreements with external Users involving Accessing, processing, communicating or managing IH's Systems or Confidential Information must comply with all relevant security requirements. System owners are required to conduct periodic reviews to ensure compliance with agreements with external Users. Reviews must be conducted on an annual basis, or as required based on criticality of the System.

Out-sourced services must be compliant with all IH policies.

3.5 Asset Management

3.5.1 Responsibility for Assets

Management responsibility must be identified for all major Systems and Confidential Information. The responsibility for the maintenance of appropriate Controls must be assigned to System owners who are accountable for their solutions.

The following asset information must be included within the IH Configuration Management Database (CMDB):

- System owner
- Physical devices
- Associated systems
- Software platforms

- Applications
- Configuration details
- Solution architecture diagrams
- Organizational communication and data flows (System integrations)
- Any other relevant documentation and artifacts related to the solution.

Rules for the acceptable use of Systems and Confidential Information must be identified, documented and implemented. Refer to Policy: AR0100 – Acceptable Use of Digital Information Systems.

3.5.2 Information Classification
All major Systems and Confidential Information will be identified and classified according to the value, legal requirements, sensitivity and criticality to IH. An appropriate set of procedures for information labeling will be developed and implemented in accordance with the IH data governance and information classification scheme.

3.6 Human Resources Information Security

3.6.1 Prior to Employment or Commencement of Services
Information Security roles and responsibilities of Staff and Users require defining and documenting in accordance with this policy.

All IH Staff members must successfully complete the IH Information Privacy & Security Training module prior to commencing employment and annually thereafter.

All Users must agree to a data Access and Confidentiality undertaking or appropriate terms of use governing their use of the System(s) to which they have been provided Access. The User's Manager must provide the User with appropriate policies and guidelines that pertain to Information Security, acceptable use of information Systems, protection of Privacy and Confidential Information, and general standards of conduct. Users must agree to review and acknowledge all provided policies before Accessing any IH information System.

External Users must not be granted Access to a System or Confidential Information unless there is an external Access agreement in place between the external User and IH. The agreement must include appropriate Privacy, Confidentiality and security obligations governing Access to Digital Information Systems or confidential information.

Background verification checks on all candidates for employment, contractors and external Users must be carried out in accordance with

relevant laws and regulations, and proportional to the business requirements, the classification of the information to be Accessed and the risks.

3.6.2 During Employment or Delivery of Services
All Users must receive appropriate Information Security awareness, education or training and regular updates to IH security policies, guidelines, procedures and standards, as relevant for their job functions or delivery of services.

3.6.3 Termination or Change of Employment or Services
All Staff, Users and agents must return all of IH's assets, equipment, keys, Access cards and records (physical and digital) in their possession upon termination of their employment or relationship with IH.

The Access rights of all Staff, Users and agents to Systems and Confidential Information must be removed upon termination of their employment, contract, or upon completion of their final workday. The service desk must be notified by the manager or external user sponsor within 5 business days when User Access is no longer required. This includes any modifications to Access resulting from a change in position or functional role. Removal of Access must be initiated by the manager responsible once identified Access is no longer required.

3.7 Physical and Environmental Security

3.7.1 Secure Areas
Security perimeters (barriers such as walls, lockable entry doors or manned reception desks) must be used to protect areas that contain Systems or Confidential Information.

Secure areas must be protected by appropriate entry Controls to only allow Access to authorized personnel.

Access points such as entrances, delivery and loading areas where unauthorized persons may enter the premises must be controlled and, where possible, isolated from information processing locations to avoid unauthorized Access.

3.7.2 Equipment Security
Systems must be protected to reduce the risks from environmental Threats and hazards.

Systems must be protected from power failures and other disruptions caused by failures in supporting utilities.

Systems must be maintained and kept up to date to ensure availability and integrity.

Information Security Controls must be applied to Systems used off-site with permission considering the different risks of working outside of IH premises.

All storage media (e.g., hard drives, CD-ROMS, flash drives) must be checked to ensure that any Confidential Information and licensed software has been removed, securely overwritten, or physically destroyed prior to disposal.

3.8 Communications and Operations Management

3.8.1 Operational Procedures and Responsibilities

Documented procedures must be created and maintained for the secure operation of all Systems.

Operational Systems and software must be subject to strict change management Control. Changes to Systems must be controlled via a change approval process (e.g., Change Advisory Board) to maintain Control of all changes to equipment, software or procedures. When changes are made, an audit log containing all relevant information must be retained.

Duties and areas of responsibility must be segregated where appropriate to reduce opportunities for unauthorized or unintentional modification or misuse of Systems.

Development, test and production Systems must be segregated (physically or logically) to reduce the risks of unauthorized Access or changes to the production System.

3.8.2 Service Contract Management

Security Controls, service definitions and delivery levels must be included in any external service contract. IH must verify the implementation of agreements, monitor compliance with the agreements and manage changes to ensure that the services being delivered meet all requirements agreed with the external service provider.

The services, reports and records provided are to be monitored and reviewed with annual audits.

Any changes to the services provided by external Users must be re-assessed to confirm compliance with Information Security policies, procedures and Controls.

3.8.3 System Planning and Acceptance

The use of Systems must be monitored, tuned and projections made for future capacity requirements to continue to meet the required level of System performance.

Acceptance criteria for new Systems, upgrades and new versions must be established and suitable tests of a System(s) carried out during development and prior to acceptance.

3.8.4 Protection against Security Threats

Detection, prevention and recovery Controls to protect against security Threats and appropriate User awareness procedures must be implemented.

3.8.5 Back-Up

Back-up copies of essential information within Systems must be taken regularly and recovery of Systems tested.

It is the responsibility of System owners for identifying data requiring a back-up and saving on appropriate network drives.

3.8.6 Network Security Management

The IH network must be adequately managed and controlled to protect against Threats and to maintain security for the Systems and applications using the network, including data in transit and data at rest.

Devices connected to the IH network must not be modified, disconnected or relocated without prior approval by Digital Health.

Wireless Access points, peer to peer wireless connections and Wi-Fi devices must be configured and installed as per Policy: AR0300 - Wireless (Wi-Fi) Network.

Security features, service levels and management requirements of all network services must be identified and included in any network services agreement, whether these services are provided by IH or outsourced.

3.8.7 Media Handling

Procedures for handling, reusing, and disposing of media containing Confidential Information must be established and communicated to Users in accordance with Security Standards for the Handling of Confidential Information (Security Bulletin #8).

3.8.8 Exchange of Information

Formal exchange policies, procedures and Controls must be in place to protect the exchange of information through the use of all types of communication methods.

Agreements must be established for the exchange of information and software between IH and external Users.

Media containing Confidential Information must be protected against unauthorized Access, misuse or corruption during the transportation beyond IH's physical boundaries.

Policies and procedures must be developed and implemented to protect information associated with the integration of Systems.

Confidential Information involved in electronic messaging must be appropriately protected as described in Policy: AR0500 – Email and Text Messaging and supporting Emailing Personal Information Guidelines.

3.8.9 Electronic Commerce Services

Confidential Information involved in electronic commerce passing over public networks must be protected from activities including but not limited to fraudulent activity, contract dispute, and unauthorized disclosure and modification.

3.8.10 Monitoring & Logging

Audit logs recording exceptions and other relevant security Events must be produced and retained for an agreed period to assist in future investigations and Access Control monitoring. The retention period will be a minimum of 90 days, or the maximum possible dependent upon the System if 90-day retention is not possible.

Procedures for monitoring and auditing use of Systems must be established by the System owners and the results of the monitoring activities reviewed on a weekly basis.

Logging facilities and log information must be protected against tampering and unauthorized Access.

3.9 Access Control

3.9.1 Application and Information Access Control

Access to Systems, networks and Confidential Information are controlled on the principle of Least Privilege.

System owners are responsible to permit Access to only those who require such Access to complete duties. Access reviews should be conducted twice per year.

3.9.2 User Access Management

There must be a formal User provisioning, User role changes and User de-provisioning procedures in place for granting, changing and revoking Access to all Systems and Confidential Information.

The allocation of Passwords must be controlled through a formal process and as described in Policy: AR0700 - User Identification and Password.

Management and, where applicable, IH's agents are responsible for ensuring appropriate User Access to IH Systems.

Temporary, term and casual Staff must have defined start and end dates. Management must request extensions through the Access Request procedure if necessary.

3.9.3 Operating System Access Control

Access to operating Systems must be controlled by a secure log-on procedure.

All System Passwords must follow standards defined in Policy: AR0700 - User Identification and Password.

Restrictions on connection times must be used to provide additional security for high-risk applications and/or Systems where inactive sessions must timeout after a defined period of inactivity.

User activity with proper authorization(s) may be subject to audits to support investigations and non-compliance with IH policies and standards.

3.9.4 Mobile Computing and Teleworking

Appropriate security measures must be adopted to protect against the risks introduced through the use of mobile computing and communication devices.

Users must not transport Confidential Information stored on portable storage devices, paper records or portable media without prior approval of their manager or immediate supervisor.

Staff and Users who commonly work outside the workplace environment must follow the Privacy and security standards defined in

Policy: AU1300 - Flexible Work Location and Guidebook. Teleworking security standards are also defined in the Work from Home (Security Bulletin #3).

3.10 Information Security in System Acquisition, Development and Maintenance

3.10.1 Security Requirements of Systems

Statements of business requirements for new Systems or enhancements to existing Systems must specify the requirements for security Controls.

All security requirements must be identified at the requirements phase of a project and justified, agreed and documented as part of the overall business case for Systems.

The use of operational data or databases containing Confidential Information must not be used for testing purposes. Production data may be used for certain types of System testing provided that all personally identifiable data elements or sensitive content is removed or de-identified before use.

Where feasible, appropriate Controls, audit trails and activity logs must be designed into systems containing Confidential Information. Control requirements must be determined by risk assessment.

3.10.2 Data Integrity

System owners are responsible for ensuring appropriate Controls are in place to maintain the integrity of information within the System. This includes managing the input, output, usage, and manipulation of the information.

3.10.3 Encryption Controls

Encryption must be used in appropriate circumstances to protect Confidential Information from unauthorized and unintended disclosure. Refer to Security Bulletin 8: Security Standards for the Handling of Confidential Information.

3.11 Information Security Incident Management

3.11.1 Reporting Information Security Breaches

All Staff and Users of Systems are required to report any confirmed or suspected security breaches as defined in Policy: AR0450 – Managing Privacy and Security Breaches.

3.11.2 Logging of Information Security Incidents

Security Incidents must be logged, tracked and significant Incidents identified and reviewed by the Digital Health Leadership Team.

Digital Health reserves the right to disconnect any solutions or services, or temporarily disable accounts, deemed as a significant risk to IH operations and/or to the Confidentiality, integrity and availability of IH's information assets.

3.12 Compliance

3.12.1 Compliance with Legal Requirements

Appropriate procedures must be implemented and kept current to comply with legislative, regulatory, and contractual requirements on the use of information including intellectual property rights and on the use of proprietary software products.

Confidential records must be protected from loss, destruction and falsification, in accordance with statutory, regulatory, and contractual requirements. Retention periods for IH information are defined in Policy: AL0700 – Records Retention, Storage and Destruction.

Data protection and security Controls must be implemented as required by relevant legislation, regulations, and, if applicable, contractual clauses.

3.12.2 Compliance with Security Policies and Standards

Staff and Users are accountable for complying with this policy and related policies, standards and guidelines. Any material violations to this policy must be reported to the IH Information Security Department. Where compliance cannot be achieved, due to the limitation of a System, technology, vendor, or process, the System owner must request a temporary exemption by contacting IH Information Security. If a temporary exemption is granted, the System owner must provide an action plan and timeline to bring the System and its Users into compliance.

Managers are required to ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with this and related policies.

Failure to comply with this policy and other related policies may result in disciplinary action including, but not limited to, termination of Access, termination of employment, termination of contract, loss of privileges as a student placement or volunteer role, withdrawal of privileges or professional sanctions, and prosecution and liability for loss or damages.

3.12.3 Information Systems Audit Considerations
Audit requirements and activities involving checks on Systems must be carefully planned and agreed to minimize the risk of disruptions to business processes.

Access to System audit tools must be protected to prevent any possible misuse or compromise.

On-going planned and ad-hoc compliance reviews for IH, partners and service providers must be conducted. Consent of the asset owner or facility manager is not required by IH Information Security, Information Privacy or Internal Audit. All Systems are subject to inspection at any time.

4.0 PROCEDURES

4.1 Staff and Users

4.1.1 Review this policy prior to commencing employment or a relationship with IH and on an annual basis thereafter.

4.1.2 Report any breaches of this policy to a supervisor, designate, and to the IH Information Security department without fear of reprisal. If necessary, complete an Incident report in coordination with Information Security and/or Information Privacy. All reported breaches are kept strictly Confidential.

4.2 Managers / Chief of Staff

4.2.1 Agree to this policy on an annual basis.

4.2.2 Follow-up on compliance audits in consultation with Human Resources and/or management and take appropriate action when required.

4.3 Digital Health / Information Security

4.3.1 Oversee the security of IH Systems and ensure Controls are in place to prevent Threats from compromising IH Systems.

4.3.2 Monitor the IH computer and wireless network for unauthorized Access, compliance and other Privacy/security vulnerabilities.

4.3.3 Conduct audits as necessary, investigating any alleged compliance misconduct in consultation with IH Human Resources, Medical Administration, Risk Management and Internal Audit.

5.0 REFERENCES

1. IH Policy: AL0700 Records Retention
2. IH Policy: AR0100 Acceptable Use of Digital Information Systems
3. IH Policy: AR0500 Email and Text Messaging
4. IH Guideline: Emailing Personal Information Guidelines.

5. IH Policy: AR0450 Managing Privacy and Security Breaches / Violations
6. IH Policy: AR0700 User Identification and Password
7. IH Policy: AR0300 Wireless (Wi-Fi) Network
8. IH Policy: AQ1800 Surplus Equipment Disposal
9. IH Policy: AU1300 Flexible Work Location
10. IH Policy: AU1300 Flexible Work Location Guide
11. IH Policy: AU0100 Standards of Conduct for Interior Health Employees
12. IH Security Bulletin #8: Security Standards for the Handling of Confidential Information
13. IH Security Bulletin #10: Acceptable Portable Storage Use
14. Information Security Branch, Office of the Chief Information Officer, Ministry of Citizen's Services, Province of British Columbia – Information Security Policy
    - http://www.cio.gov.bc.ca/cio/informationsecurity/policy/isp_summaries.page
15. NIST Cybersecurity Framework 1.1
    - https://doi.org/10.6028/NIST.CSWP.04162018
16. Center for Internet Security (CIS) Controls
    - https://www.cisecurity.org/controls/cis-controls-list
17. PHSA Privacy & Security Schedule
18. Payment Card Industry Standards Council, Payment Card Industry Data Security Standard (PCI-DSS) v4.0
    - https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf
19. Information Systems Audit and Control Association, Control Objectives for Information and related Technology (COBIT)
    - https://www.isaca.org/resources/cobit
20. Freedom of Information and Protection of Privacy Act (FIPPA)
    - http://www.oipc.bc.ca/about/legislation.aspx