


# First Nations Health Authority

## Board Policy



First Nations Health Authority  
Health through wellness

<b>Policy Name</b>	<b>Information Security Policy</b>
<b>Department</b>	Innovation and Information Management Services (IIMS)

For Corporate Services and CEO Office (do not fill this in)			
Document #	Effective	Replaces	Dated
IIMS-15-04-001	August 7, 2015	new	
Board Approved Date		Authorization (BoD Motion Number)	
August 7, 2015 		0815-BOD-6H	

### 1.0 Purpose

- 1.1 The purpose of this policy is to ensure the confidentiality, integrity, and availability of confidential information stored on all of FNHA's information systems, including shared information systems ("systems").
- 1.2 This is FNHA's primary policy for information security and covers the range of control objectives described in the international standard: ISO/IEC 27002:2013, the "Code of practice for information security controls".
- 1.3 This policy supports organizational Directive 3: Improve Services and Directive 7: Function at a High Operational Standard, and also supports the Shared Value of Excellence. This policy also supports the following Operating Principle: sustainability, integrity, efficiency and innovation are essential components to the business approach that FNHA brings to its programs, services and initiatives.

### 2.0 Scope

- 2.1 This policy applies to all computer and network systems owned or administered by FNHA, or operated by a third party for FNHA. This includes all of FNHA's processing facilities, all platforms, all computers (regardless of size), and all application systems (whether developed in-house or purchased by third parties).
- 2.2 This policy applies to all workers and users of systems, including part-time, temporary staff, physicians, students, as well as all business and health-care delivery partners, consultants, contractors, and other service providers.

### 3.0 Policy Statements

#### ***Information Security Risk Management***

- 3.1 Information security requirements must be identified by a methodical assessment of security risks. The results of the risk assessments will help FNHA determine the appropriate management action and priorities for managing information security risks and for implementing the appropriate controls to protect against these risks.
- 3.2 Expenditure on controls must be balanced against the business harm likely to result from security failures.
- 3.3 Risk assessments must be repeated periodically to address any changes that might influence the risk assessment results.

# First Nations Health Authority

## Board Policy



First Nations Health Authority  
Health through wellness

- 3.4 Information security risk management is detailed in the Compliance Directive under the Security Threat and Risk Assessment section.

### ***Information Security Policy, Directives, Procedures, and Standards***

- 3.5 IIMS will set a clear direction and demonstrate support for, and commitment to, information security through this policy and related information security directives, procedures, and standards.
- 3.6 This policy will be reviewed at planned intervals, when industry standards change, or in response to a security incident. Policy reviews must be conducted in accordance with FNHA's information security framework to ensure the policy's continuing suitability, adequacy, and effectiveness.

### ***Organization of Information Security***

#### *Internal Organization*

- 3.7 FNHA will implement and manage an Information Security Program to protect systems and confidential information stored on systems. The Information Security Program is managed by the Chief Information Officer.
- 3.8 The Program will:
- a) ensure that information security goals are identified, meet organizational requirements, and are integrated into relevant processes;
  - b) formulate, review, and approve this policy and related directives and standards;
  - c) review the effectiveness of the implementation of this policy and other related FNHA policies and directives;
  - d) provide clear direction and visible management support for security initiatives;
  - e) provide the resources needed for information security;
  - f) approve assignment of specific roles and responsibilities for information security across FNHA;
  - g) initiate plans and programs to maintain information security awareness; and
  - h) ensure that the implementation of information security controls is coordinated and consistent across FNHA.
- 3.9 Information security activities will be coordinated by representatives from different parts of FNHA with relevant roles and job functions.
- 3.10 All information security responsibilities must be clearly defined. Individuals with allocated security responsibilities may delegate security tasks to others; however, the individual remains responsible for ensuring that any delegated tasks have been performed correctly.

#### *Independent Review*

- 3.11 IIMS' approach to managing information security and its implementation, including controls, policies, directives, and procedures, should be reviewed independently at planned intervals, or when significant changes to the information security implementation occur. The independent review must be initiated by FNHA's Senior Executive Team (SET). Such a review must be carried out by individuals independent of the area under review, e.g., an internal audit group or a third-party organization specializing in such reviews. The results of the independent review must be recorded and reported to SET and FNHA's Board of

# First Nations Health Authority

## Board Policy



First Nations Health Authority  
Health through wellness

Governors (the Board). If the independent review determines that FNHA's approach and implementation to managing information security is inadequate or non-compliant with this policy, SET or the Board will take corrective actions as necessary.

### *External Parties*

- 3.12 The security of FNHA's systems and confidential information must not be compromised by the introduction of external parties, the products or services they provide, or external users. Access to FNHA's systems facilities by external parties must be controlled. Where there is a business need for working with external parties that may require access to FNHA's systems and confidential information, or obtaining or providing a product or service from or to an external party, an assessment must be carried out to determine the security implications and control requirements as per the *Security Threat and Risk Assessment (STRA)*. Controls must be agreed to, and defined in, an agreement with the external party.
- 3.13 Agreements with external parties involving accessing, processing, communicating, or managing FNHA's confidential information or systems must cover all relevant security requirements. Periodic reviews may be required to ensure that external parties comply with these agreements.
- 3.14 Outsourcing arrangements must address the risks, security controls, and procedures for systems and security-incident reporting in the contract between FNHA and external parties.
- 3.15 Security requirements must be identified and addressed before giving external parties or external users access to FNHA's confidential information or systems.

### ***Human Resources Security***

#### *Prior to employment or commencement of services*

- 3.16 Security roles and responsibilities of staff, external parties, and external users must be defined and documented in accordance with this policy.
- 3.17 All users must agree to adhere to the appropriate terms of use governing the system(s) to which they will be provided access and maintain the confidentiality and integrity of the systems(s). Users must also be provided with appropriate policies, directives and procedures that pertain to acceptable use of technology, protection of privacy and confidentiality, and general standards of conduct.
- 3.18 External parties must not be given access to a system or confidential information unless there is an agreement in place between the external party and FNHA that includes appropriate privacy, confidentiality and security obligations governing external parties' access to the system or confidential information.
- 3.19 Background verification checks on all employee, contractor and external-user candidates must be carried out in accordance with relevant laws, regulations, and ethics, and must be proportional to the business requirements, the classification of the information to be accessed, and the risks.

#### *During employment or delivery of services*

- 3.20 FNHA's management must ensure that staff and users comply with their security responsibilities as outlined in this policy, related directives and operational procedures.
- 3.21 All users must receive appropriate information security awareness education or training that is relevant to their job functions. External parties and external users must also receive security awareness education or training that is appropriate for their level of access to systems or confidential information. Users must be trained on the appropriate security procedures and the correct use of systems to minimize the potential security risks. All users must be informed of significant changes to FNHA's Security Policy and directives and be provided with the appropriate awareness training.

# First Nations Health Authority

## Board Policy



First Nations Health Authority  
Health through wellness

- 3.22 Any material violations of this policy or other organizational security directives will be addressed through a formal disciplinary process and / or termination of services.

### *Termination or change of employment or services*

- 3.23 All staff and users must return all of FNHA's assets, equipment, and records in their possession upon termination of their employment or relationship with FNHA.
- 3.24 The access rights of all staff and users to systems and confidential information must be removed upon termination of their employment, contract or agreement with FNHA or modified accordingly if their position or functional role and employment status within FNHA changes.

## **Asset Management**

### *Responsibility of assets*

- 3.25 Management responsibility must be identified for all systems and confidential information contained therein. Responsibility for the maintenance of appropriate controls must be assigned to designated individuals.
- 3.26 IIMS is responsible for approving all computer equipment installations, disconnections, modifications, repairs, servicing, and relocations. Rules for the acceptable use of systems and confidential information must be defined and implemented. Acceptable uses of systems are set out in the *Acceptable Use Directive*.

### *Information classification*

- 3.27 All major systems and confidential information must be identified and classified according to the value, legal requirements, sensitivity, and criticality to FNHA as per the *Asset Management Directive* under *Information Security Classification*. An appropriate set of procedures for information labeling and handling must be developed and implemented in accordance with the classification scheme.

## **Physical and Environmental Security**

### *Secure areas*

- 3.28 Security perimeters (barriers such as walls, card-controlled entry doors, or manned reception desks) must be used to protect areas that allow access to systems and confidential information.
- 3.29 Secure areas must be protected by appropriate entry controls to ensure that only authorized personnel are allowed access to such areas.
- 3.30 Physical security for offices, rooms, and facilities must be designed and applied.
- 3.31 Physical access is granted based upon defined job descriptions or roles.
- 3.32 Access points, such as delivery and loading areas and other points where unauthorized persons may enter the premises, must be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

### *Equipment security*

- 3.33 All systems must be protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
- 3.34 Systems must be protected from power failures and other disruptions caused by failures in supporting utilities.

# First Nations Health Authority

## Board Policy



First Nations Health Authority  
Health through wellness

- 3.35 Power and telecommunications cabling carrying data or supporting information services must be protected from interception or damage.
- 3.36 Systems must be correctly maintained to ensure their continued availability and integrity.
- 3.37 Equipment taken off-site must be secured from loss and unauthorized access.
- 3.38 All systems containing storage media must be checked to ensure that any confidential information and licensed software has been removed or securely overwritten prior to disposal. Systems containing confidential information must be physically destroyed or the information must be destroyed, deleted, or overwritten using techniques that make the original information non-retrievable.

### ***Communications and Operations Management***

#### *Operational procedures and responsibilities*

- 3.39 Documented procedures must be created and maintained for the secure operation of all systems.
- 3.40 Changes to systems must be controlled. Operational systems and application software must be subject to strict change management control. Formal management responsibilities and procedures must be in place to ensure satisfactory control of all changes to equipment, software, or procedures. When changes are made, an audit log containing all relevant information must be retained.
- 3.41 Duties and areas of responsibility must be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of systems.
- 3.42 Development, test and operational systems environments must be segregated to reduce the risks of unauthorized access or changes to the operational system.

#### *External-party service delivery management*

- 3.43 Security controls, service definitions, and delivery levels must be included in any external-party service delivery agreement. FNHA must verify the implementation of agreements, monitor compliance with the agreements, and manage changes to ensure that the services delivered meet all requirements agreed to with the external party.
- 3.44 The services, reports, and records provided by the external party must be regularly monitored and reviewed, and audits must be carried out regularly.
- 3.45 Changes to the provision of external-party services, including maintaining and improving existing information security policies, procedures, and controls, must be managed, taking into account the criticality of business systems and processes involved and re-assessment of risks.

#### *System planning and acceptance*

- 3.46 The use of systems must be monitored and tuned, and projections must be made for future capacity requirements to ensure the required system performance.
- 3.47 Acceptance criteria for new systems, upgrades, and new versions must be reviewed by FNHA's Change Control process, and suitable tests of the systems must be carried out during development and prior to acceptance.

#### *Protection against malicious and mobile code*

- 3.48 Detection, prevention, and recovery controls to protect against malicious code and appropriate user-awareness procedures must be implemented as described in the *Operational Security Directive* under *Malware Protection*.

# First Nations Health Authority

## Board Policy



First Nations Health Authority  
Health through wellness

- 3.49 Mobile code must be controlled within systems. Systems deploying mobile code must ensure that the authorized mobile code operates according to a clearly defined security directive and that unauthorized mobile code is prevented from executing.

### *Back-ups*

- 3.50 Back-up copies of essential information within systems must be taken regularly and tested to ensure recovery system(s) and network security patches are maintained.
- 3.51 Not all systems or data are backed up (e.g., "C" drive), and users are responsible for ensuring that all systems and data requiring back-up are saved on appropriate network drives.

### *Network security management*

- 3.52 FNHA's network must be adequately managed and controlled to protect it from threats and to maintain security for the systems and applications using the network, including confidential information in transit.
- 3.53 Devices connected to FNHA's network must not be modified, disconnected, or relocated without appropriate approval by IIMS.
- 3.54 Wireless access points, peer-to-peer wireless connections, and Wi-Fi devices (even if they are not connected to the network) must be installed as per the *Identity and Access Management Directive* under *Wireless (Wi-Fi) Network Access*.
- 3.55 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 FNHA or outsourced to an external party.

### *Media handling*

- 3.56 Procedures for handling, reusing, and disposing of media containing Confidential Information must be established and communicated to users.
- 3.57 Media must be disposed of securely and safely when no longer required, as per the *Information Asset Security Directive* and the *Records and Information Management Policy*.
- 3.58 Procedures for the handling and storage of confidential information must be established to protect the information from unauthorized access, disclosure, or misuse.

### *Exchange of information*

- 3.59 Formal directives, procedures, and controls must be in place to protect the exchange of information through the use of all types of communications facilities.
- 3.60 Agreements must be in place for the exchange of confidential information and software between FNHA and external parties.
- 3.61 Media containing confidential information must be protected against unauthorized access, misuse, or corruption during transportation beyond FNHA's physical boundaries.
- 3.62 Confidential information involved in electronic messaging must be appropriately protected.
- 3.63 Directives and procedures must be developed and implemented to protect confidential information associated with the interconnection of systems.



# First Nations Health Authority

## Board Policy



First Nations Health Authority  
Health through wellness

### *Electronic commerce services*

- 3.64 Confidential information involved in electronic commerce passing over public networks must be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.
- 3.65 Confidential information involved in on-line transactions must be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, and unauthorized message duplication or replay.
- 3.66 The integrity of confidential information being made available on a publicly available system must be protected to prevent unauthorized modification.

### *Monitoring and logging*

- 3.67 Audit logs recording exceptions and other security-related events must be produced and retained for an agreed period to assist in future investigations and access-control monitoring.
- 3.68 Procedures for monitoring and auditing system use must be established, and the results of the monitoring activities must be reviewed regularly.
- 3.69 Logging facilities and log information must be protected against tampering and unauthorized access.
- 3.70 System administrator and system operator activities must be logged.
- 3.71 Faults must be logged, analyzed, and appropriate action taken.
- 3.72 The clocks of all relevant information processing systems within an organization or security domain must be synchronized with an accurate time source.
- 3.73 See the *Operational Security Directive*.

### *Firewalls*

- 3.74 Access to FNHA's network and networked systems must be controlled and managed by firewall devices. Firewall appliances and similar devices will be implemented to control the flow of network traffic at network boundaries between networks with differing security postures, such as at the boundary between the public Internet and FNHA's internal network.
- 3.75 End-point protection must be installed on all authorized devices accessing the network where indicated by a STRA or based on its sensitivity as per the *Asset Management Directive* under *Information Security Classification*.

## **Access Control**

### *Business requirements for access control*

- 3.76 Access to systems, networks, and confidential information must be controlled on the basis of business and security requirements as specified in the *Identity and Access Management Directive* under *Role-Based Access Management*.
- 3.77 Access control rules must be based on the premise of "need to know" and the principle of "least privilege".

### *User access management*

- 3.78 A formal user registration and de-registration procedure must be in place for granting and revoking access to all systems and confidential information as described in the *Identity and Access Management Directive*.
- 3.79 Allocation and use of privileges must be restricted and controlled.

# First Nations Health Authority

## Board Policy



First Nations Health Authority  
Health through wellness

- 3.80 The allocation of passwords must be controlled through a formal management process as described in the *Identity and Access Management Directive* under *User Identification and Passwords*.
- 3.81 All of FNHA's user accounts, computers, and portable devices (including laptops, personal digital assistants, and cellular devices with data capabilities) that access FNHA's network and/or data must employ appropriate protection controls and have them enabled.
- 3.82 Management must review users' access rights at regular intervals using a formal process as described in the *Identity and Access Management Directive*.

### *User responsibilities*

- 3.83 Users must follow security best practices regarding the selection and use of passwords in accordance with FNHA's password standards.
- 3.84 Users must ensure that unattended equipment is appropriately protected.
- 3.85 A clear desk policy and clear screen policy for systems must be adopted as per the *Physical Security Directive*.
- 3.86 Users must not use the "remember password" feature of any software application (e.g., Internet Explorer).
- 3.87 Users must use automatic password-protected screen savers with timeout periods appropriate to the sensitivity of the data being accessed.

### *Network access control*

- 3.88 Users must be given access to only the systems and confidential information that they have been specifically authorized to use.
- 3.89 Appropriate authentication methods must be used to control access by remote users. Controls for remote access, including authentication mechanisms to FNHA's network, are defined in the *Identity and Access Management Directive* under *Remote Access*.
- 3.90 Automatic equipment identification must be used, where appropriate, as a means to authenticate connections from specific locations and equipment.
- 3.91 Physical and logical access to diagnostic and configuration ports must be controlled.
- 3.92 Groups of systems, confidential information, and users must be segregated on FNHA's network, as required.
- 3.93 For shared networks, especially those extending across FNHA's boundaries, the capability of users to connect to the network must be restricted, in line with the access control requirements of systems.
- 3.94 Routing controls must be implemented on FNHA's network to ensure that computer connections and the flow of confidential information does not breach the access control requirements of systems.
- 3.95 Wireless networks must be segregated from internal and private networks, and networking controls must be implemented to maintain that segregation. Wireless controls are defined in the *Identity and Access Management Directive* under *Wireless (WiFi) Network Access*.
- 3.96 Restrictions on connection times must be used to provide additional security for high-risk applications.

### *Operating system access control*

- 3.97 Access to operating systems must be controlled by a secure log-on procedure.
- 3.98 All system passwords must follow standards defined in the *Identity and Access Management Directive*.



# First Nations Health Authority

## Board Policy



- 3.99 Passwords must be protected from unauthorized use or disclosure. Unsuccessful access attempts must be monitored and trigger appropriate system protection mechanisms and response processes, such as user account lock-outs or deactivation.
- 3.100 The use of utility programs that might be capable of overriding system controls must be restricted and tightly controlled.
- 3.101 Inactive sessions must shut down after a defined period of inactivity.
- 3.102 Restrictions on connection times must be used to provide additional security for high-risk applications.

### *Application and information access control*

- 3.103 Access to confidential information and application system functions by users and support personnel must be restricted in accordance with this and the Identity and Access Management Directives. Access restrictions must be based on individual business application requirements.
- 3.104 Systems containing confidential information must have a dedicated (isolated) computing environment.

### *Mobile computing and teleworking*

- 3.105 Appropriate security measures must be adopted to protect against the risks of using mobile computing and communication devices.
- 3.106 Users must not take portable storage devices or media off FNHA's premises without the approval of their immediate supervisor. Approval includes the supervisor knowing what equipment is leaving, for what purpose, and with what data.
- 3.107 Operational plans and procedures must follow the standards defined in the *Acceptable Use Directive* under *Mobile Computing and Device Usage*.

## **Information Security in System Acquisition, Development, and Maintenance**

### *Security requirements of systems*

- 3.108 Business requirements for new systems, or enhancements to existing systems, must specify the security control requirements.
- 3.109 All security requirements must be identified at the requirements phase of a project and be justified, agreed to, and documented as part of the overall business case for systems.
- 3.110 Appropriate controls for auditing or activity logging must be designed into systems. Control requirements must be determined on the basis of a risk assessment.

### *Correct processing in applications*

- 3.111 Application data entry must be validated to ensure the data was entered correctly and is appropriate.
- 3.112 Validation checks must be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.
- 3.113 Requirements for ensuring authenticity and protecting message integrity in applications must be identified and appropriate controls implemented.

# First Nations Health Authority

## Board Policy



First Nations Health Authority  
Health through wellness

### *Cryptographic controls*

- 3.114 Encryption must be used in appropriate circumstances to protect confidential information from unauthorized disclosure. If storage or transmission of confidential information is required for business needs, the information must be encrypted using FNHA's encryption/cryptographic standard to render it unreadable.
- 3.115 The use of cryptographic controls must be determined by a STRA as described in the *Compliance Directive* under *Security Threat and Risk Assessment*.
- 3.116 As necessary, appropriate key management systems must be in place to support the use of cryptographic techniques across FNHA.

### *Security of system files*

- 3.117 Procedures must be in place to control the installation of software on operational systems.
- 3.118 Test data must be selected carefully, and protected and controlled. 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 modified beyond recognition before use.
- 3.119 Access to system files and source code must be controlled and restricted only to authorized users based on their roles and responsibilities following the principle of "least privilege".

### *Security of development and support processes*

- 3.120 The implementation of changes must be controlled by a formal change control procedure.
- 3.121 When operating systems are changed, business-critical applications must be reviewed and tested to ensure there is no adverse impact on FNHA's operations or security.
- 3.122 Modifications to software packages must be limited to necessary changes, and all changes must be strictly controlled.
- 3.123 Information leakage must be prevented by:
- a) scanning outbound media and communications for hidden information;
  - b) masking and modulating system and communications behavior to reduce the likelihood of an external party being able to deduce information from such behavior;
  - c) making use of systems and software that are considered to be of high integrity, e.g., using evaluated products;
  - d) regular monitoring of staff usage and system activities, where permitted under existing legislation or regulation; and
  - e) monitoring resource usage in systems.
- 3.124 Outsourced software development must be supervised and monitored by FNHA, as appropriate.

### *Technical vulnerability management*

- 3.125 An STRA must be conducted prior to deploying a system in production to ensure technical vulnerabilities are identified and the risk exposure is evaluated so appropriate measures can be implemented to address the associated risks.

3.126 Systems must be patched regularly as described in the *Operational Security Directive* under *Software Patch Management*.

3.127 Systems must be scanned for vulnerabilities before being deployed in production and when changes which may affect the system security are made. Identified vulnerabilities must be prioritized and addressed for remediation considering each threat and its potential impact on FNHA. Vulnerability remediation may include correcting the vulnerable configuration, applying a software patch, or implementing alternative compensatory controls. Critical systems, such as externally facing network devices and firewalls, must be scanned for vulnerabilities on a regular and ad hoc basis.

### ***Information Security Incident Management***

#### *Reporting of information security events and weaknesses*

3.128 All staff and users of systems are required to report any observed or suspected security breaches to their immediate manager or supervisor.

3.129 Information security events must be reported to FNHA's Helpdesk, Information Security Manager and Information Privacy Office as quickly as possible.

3.130 All staff and users of systems are required to report to the FNHA Helpdesk and Information Security Manager any observed or suspected security weaknesses in systems.

#### *Management of information security incidents and improvements*

3.131 Management responsibilities and procedures must be established to ensure a quick, effective, and orderly response to information security incidents.

3.132 FNHA's Senior Executive Team is accountable for decisions relating to significant security incidents affecting revenue, reputation, or legal liability.

3.133 Security incidents must be logged and tracked, and summary reports of the incidents must be presented to FNHA's Information Privacy Office.

### ***Disaster Recovery and Business Continuity Planning***

#### *Information security aspects of business continuity management*

3.134 A managed process must be developed and maintained that identifies the information security requirements needed for business continuity. Events that can cause interruptions to business processes must be identified, along with the probability and impact of such interruptions and their consequences for information security.

3.135 Plans must be developed and implemented to maintain or restore operations and to ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.

3.136 A single point of reference for business continuity plans must be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.

3.137 Business continuity plans must be tested and updated regularly to ensure they are effective.

# First Nations Health Authority

## Board Policy



First Nations Health Authority  
Health through wellness

### ***Policy Monitoring***

#### *Compliance with legal requirements*

- 3.138 All relevant statutory, regulatory and contractual requirements, and FNHA's approach to meeting these requirements, must be defined, documented, and kept up-to-date.
- 3.139 Appropriate procedures must be implemented to ensure compliance with legislative, regulatory and contractual requirements regarding the use of material in respect of which there may be intellectual property rights and regarding the use of proprietary software products.
- 3.140 Important records must be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual and business requirements. Retention requirements for FNHA's confidential information are defined in the *Records and Information Management Policy* and the *FNHA Retention Schedule*.
- 3.141 Data protection and privacy controls must be implemented as required by relevant legislation, regulations, and, if applicable, contractual clauses.

#### *Compliance with security policies and standards, and technical compliance*

- 3.142 Staff are accountable for complying with this policy and related directives. All deviations and non-compliance with this policy and related directives must be recorded, including the specific actions taken through an exceptions authorization process.
- 3.143 Managers are required to ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with this policy and related directives.
- 3.144 Systems must be regularly checked for compliance with security implementation standards.
- 3.145 Failure to comply with this policy and related directives may result in disciplinary action including, but not limited to, loss of computing privileges and/or the termination of employment.
- 3.146 FNHA will take reasonable measures to comply with this policy and related directives. Where technical controls or existing resources are incapable of enforcing all conditions outlined in this policy, compensatory controls will be put in place to achieve the control objectives of this policy.

#### *Information systems audit considerations*

- 3.147 Audit requirements and activities involving checks on operational systems must be carefully planned to minimize the risk of disruptions to business processes.
- 3.148 Access to system audit tools must be protected to prevent any possible misuse or compromise.
- 3.149 On-going planned and ad hoc compliance reviews for FNHA and its partners and service providers must be conducted. Consent of the asset owner or facility manager is not needed by IIMS. All systems are subject to inspection at any time.
- 3.150 A periodic information security risk assessment, and review of implemented security controls, will be performed to ensure that existing information security policies and controls adequately address changes to business requirements and priorities, and to consider new threats and vulnerabilities to FNHA.

#### *Exceptions*

- 3.151 Exceptions to this policy are permitted only in extraordinary circumstances for approved business or clinical purposes and where the exception is supported by a security threat risk assessment.

# First Nations Health Authority

## Board Policy



First Nations Health Authority  
Health through wellness

- 3.152 Exceptions to this policy must be approved by the Information Security Manager in consultation with the IT Risk and Compliance Committee.
- 3.153 Any approved exceptions must be re-evaluated whenever a material change to the control environment occurs. The business sponsor is responsible for notifying the Information Security Manager of any changes to the control or operating environment described in an approved exception.

### 4.0 Responsibilities

Board of Directors, Chief Information Officer (CIO), and Director, Project Risk Management Services: Are responsible for information security governance of FNHA and the organization's information assets and their criticality to the ongoing business operations.

Information Security Manager: Defines and manages the Information Security Program, and monitors ongoing compliance with the *Information Security Policy* and its associated directives.

FNHA Staff and System Users: Are responsible for complying with this policy and associated directives.

### 5.0 Definitions

Clients: All people receiving services from FNHA, including patients and residents or their authorized or legal representative.

Confidential Information: Includes information and data, in any form or medium, relating to FNHA, its business, operations, activities, planning, personnel, labour relations, suppliers, and finances that is not generally available to the public, including personal information and information that is identified as "confidential information" in accordance with FNHA's policies.

Control: Any method of managing risk, including policies, procedures, guidelines, practices, or organizational structures, which can be of an administrative, technical, management or legal nature. Control is also used as a synonym for "safeguard" or "countermeasure".

External Party: Any FNHA business partner entity or other non-FNHA entity.

External User: A user of a system who is not a member of FNHA personnel.

Firewall: A system which controls network access between two or more networks or networked devices.

IIMS: Innovation and Information Management Services

Information Security: The preservation of the confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

Information Security 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 a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

Least Privilege: The security principle that ensures that a user must have only those privileges required for the task at hand and no more.

# First Nations Health Authority

## Board Policy



Malicious Code: Software designed to exploit, infiltrate, or damage a system without the informed consent of the computer user. The software is also referred to as “malware” and includes computer viruses, worms, Trojan horses, rootkits, spyware, dishonest adware, and other unwanted software.

Material Change: A change to existing practices that significantly increases the level of risk to FNHA.

Media: Any technology or device that stores or is capable of storing information.

Mobile Code: Software obtained from remote systems, transferred across a network, and then downloaded and executed on a local system without explicit installation or execution by the user.

Password: A form of secret authentication data that is used in combination with a user-ID to control access to a system.

Publicly Available: A domain that is available for public use.

Remote Access: Accessing a system from outside of an organization’s facility or site.

SET: Senior Executive Team.

Staff: All officers, directors, employees, contractors, consultants, physicians, health care professionals, students, volunteers, and other service providers engaged by FNHA or organizations with which FNHA has concluded a network services agreement or any other authorized User”.

Worker(s): Includes individuals employed, privileged, or contracted with First Nations Health Authority (FNHA) while engaged in an FNHA work activity, specifically: FNHA Board of Directors; employees (union, non-union, full-time, part-time, permanent, term, casual); people working at FNHA through an Interchange Agreement; people paid via third-party agencies (temps); contractors; consultants; students; and volunteers.

System: Any of FNHA’s respective information systems, including shared electronic information systems.

Threat: A potential cause of an unwanted incident, which may result in harm to a system or FNHA.

User: Any individual who has been authorized to access and use a system.

User-ID: A code or string of characters used to uniquely identify a user on a system.

Vulnerability: A weakness of a system that can be exploited by one or more threats.

## 6.0 Related Documents

### Legislation and Regulations

Information Security Branch  
Office of the Chief Information Officer  
Ministry of Technology, Innovation and Citizens’ Services, Province of British Columbia:  
[http://www.cio.gov.bc.ca/local/cio/informationsecurity/policy/summaries/7\\_sec\\_threat\\_risk.pdf](http://www.cio.gov.bc.ca/local/cio/informationsecurity/policy/summaries/7_sec_threat_risk.pdf)

Payment Card Industry Security Standards Council  
Payment Card Industry Data Security Standard (PCI-DSS) v3.0:  
[https://www.pcisecuritystandards.org/security\\_standards/documents.php?document=pci\\_dss\\_v3-0#pci\\_dss\\_v3-0](https://www.pcisecuritystandards.org/security_standards/documents.php?document=pci_dss_v3-0#pci_dss_v3-0)



# First Nations Health Authority

## Board Policy



ISO 27002 Standards: Code of Practice for Information Security Management:

<http://www.27000.org/iso-27002.htm>

ITIL (Information Technology Infrastructure Library): <http://www.itil-officialsite.com/home/home.aspx>

COBIT: Framework for IT Governance and Control

<http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx>

### **FNHA Documents**

Acceptable Use Directive

Asset Management Directive

Compliance Directive

Disaster Recovery and Business Continuity Plan

Identity and Access Management Directive

Information Privacy and Confidentiality Policy

Communications (Network) Security Directive

Operational Security Directive

Physical Security Directive

Records and Information Management Policy

### **7.0 Rescind and Conflict Statements**

- 7.1 With the approval of this policy, older versions are considered to be replaced and/or rescinded and are no longer in effect.
- 7.2 Where there is a conflict or overlap within policy documents, the most recent board policy, executive directive, or procedure will prevail. Where clarity still cannot be established, the CEO has sole discretion to provide direction and, where applicable, to report the situation to the Chair of the Board Governance and Human Resources Committee.

### **8.0 Revision History**

Approval Date	Document #   Name	Key Changes / Comments
	new	

### **9.0 Attachments**

None