AR0300 – WIRELESS (Wi-Fi) NETWORK

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

To set the standards for the deployment, management and use of Wi-Fi Networks within Interior Health facilities.

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.*
Access Point	*A Wireless communications hardware device that allows Wireless devices to connect to a wired network using Wi-Fi, or related communication standards.*
Authentication (Enterprise Grade)	*The process of identifying an individual based on a User name (ID) and Password. In security systems, Authentication is distinct from authorization, which is the process of giving individuals Access to system objects based on their identity. Authentication confirms that the individual is who he or she claims to be, but says nothing about the Access rights of the individual.*
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 a synonym for safeguard or countermeasure.*
Interference	*The degradation of a Wireless communications signal caused by other electromagnetic signals from another source such as cellphones, microwave ovens, medical and research equipment and other devices that generate radio signals.*
Life Safety System	*Robust system put in place to save lives, including but not limited to, fire alarms, nurse call, and code alert systems.*

Password	*A form of Authentication data that is used in combination with a User-ID to Control Access to a System.*
Rogue or Unauthorized Wireless Device	*A device that is not owned, managed or maintained by IH. It could be a personal device, access point or other third-party device that presents a risk to IH Systems and information resources.*
Spectrum	*Bands or frequencies within the electromagnetic Spectrum that have been allocated for wireless communication.*
Staff	*The officers, directors, employees, and physicians employed by Interior Health.*
Threat	*A potential cause of an unwanted incident, which may result in harm to a system or organization.*
User	*Any IH 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.*
Wi-Fi Network	*Any Wi-Fi or wireless network that is connected to IH's network or is created using wireless technology located within IH's facilities.*
Wireless	*Transmission of electromagnetic signals.*
WLAN	*Wireless Local Area Network means a wireless network that is local to an IH facility consisting of one or more access points that provides the capability for other wireless devices to connect to the IH network. A WLAN provides the functionality of a wired LAN without the physical constraints of wiring. A WLAN, by its nature and inherent risks, requires additional security measures to ensure it is protected and interference is minimized.*

3.0 POLICY

3.1 Scope

This policy applies to all Users who Access, use, operate or administer Access to Wi-Fi Networks and Wireless systems. This includes Interior Health (IH) physical locations, both inside building and outdoor areas.

3.2 Principles

Wi-Fi Networks provide increased connectivity, flexibility and mobility for Staff and Users of IH's systems and information.

Appropriate Controls must be in place to minimize the Threat of loss or damage to IH's resources and data.

Wi-Fi Networks and connected endpoints use must be approved by Digital Health.

Wi-Fi Networks and connected devices do not meet the requirements for Life Safety Systems. Wi-Fi connected devices cannot be used in whole or as a fundamental component of a Life Safety System. An example of this is that a fire alarm, which is a Life Safety System, may integrate to a Wi-Fi system for non-critical functionality, while the core functionality of the Life Safety System (e.g., audible alarm and flashing lights), must function without the Wi-Fi component.

Wi-Fi Networks coverage and capacity is provided based on clinical and business requirements as well as available funding and other considerations.

W-Fi Networks are provided in a standardized delivery model with consistent capabilities and feature sets across IH locations.

3.3 Wi-Fi Networks

Digital Health is responsible for authorization, deployment and management of Wi-Fi Networks and Wireless technology including Wi-Fi connected devices. This includes managing the security, monitoring, auditing and integrity of the network. Biomedical Engineering is engaged in the review and approval process for connected medical equipment and as needed.

3.4 Wireless (Wi-Fi) Network Standards

Digital Health manages and maintains a current Wireless (Wi-Fi) infrastructure inventory of approved standards.

Current standards for IH Wireless (Wi-Fi) Networks are based on the IEEE 802.11 specifications. Access requirements are defined and managed by Digital Health. All Wi-Fi Networks must be fully tested and commissioned by Digital Health before deploying into the production environment.

3.5 Encryption

All business and clinical devices, including all devices requiring direct Access to internal systems or transmitting and Accessing personal information, Accessing IH's network through a Wi-Fi Network must deploy enterprise grade levels of Encryption.

3.6 Authentication

All Users and devices Accessing IH's systems and resources through a Wi-Fi Network must be authenticated via Enterprise Grade Authentication prior to Access being granted to IH information resources. Enterprise Grade Authentication includes robust mechanisms involving a suitable combination of credentials, certificates and similar Authentication details provided by endpoint devices. Pre-shared key or simple passphrase Authentication alone does not meet this requirement.

3.7 Coverage and Use Areas

Digital Health deploys Wi-Fi Network coverage to indoor areas of clinical and long-term care facilities as its highest priority. Within these facilities coverage may exist in maintenance, storage and outdoor areas but may not provide suitable performance for all applications. Administrative locations are provided with Wi-Fi coverage to the extent that available funding supports.

3.8 Supported Devices

Devices requiring connectivity to Wi-Fi Networks must be approved by Digital Health. All devices must be maintained and updated to meet current industry standards, including the minimum requirements detailed in Appendix A.

3.9 Interference

The Wireless Spectrum is susceptible to Interference from other devices. Digital Health in collaboration with IH's Facilities and other departments will use the following guidelines to resolve such Interferences:

- If a User, device or piece of equipment is found to be intentionally causing Interference with IH's Wireless (Wi-Fi) Network, Digital Health will work with the department manager or supervisor to determine the appropriate course of action.

- If a User, device or piece of equipment is found to be unintentionally causing Interference with IH's wireless (Wi-Fi) Network, Digital Health will work with the individual or department to remove or minimize the interfering device's impact on the Wireless Network.

3.10 Prohibition of Rogue Wireless Network Devices

No installations of unauthorized parallel wireless infrastructure and/or Rogue Wireless Devices are permitted on IH's network or within its facilities. This includes personal hotspots and patient/public owned devices that may cause wireless Interference.

If an Unauthorized or Rogue Wireless Device is found within IH's Wireless Network, the device will be disabled or removed, and the department manager will be informed. Policy compliance in Section 3.9 may also be enforced.

3.11 Compliance with Policy

Failure to comply with this policy 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.

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 Privacy & Security Office without fear of reprisal. If necessary, complete an incident report in coordination with Information Privacy & Security. All reported breaches are kept strictly confidential.

4.2 Managers / Chief of Staff

4.2.1 Review this policy on an annual basis.

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

4.3 Information Management and Information Technology / Information Privacy and 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 is 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: AR0200 Information Security Policy
2. IH Policy: AR0100 Acceptable Use of Information Systems
3. IH Policy: AR0700 User Identification and Password Policy

4. Information Security Branch, Office of the Chief Information Officer, Ministry of Citizen's Services, Province of British Columbia – Information Security Policy
   a. http://www.cio.gov.bc.ca/cio/informationsecurity/policy/isp_summaries.page
5. Institute of Electrical and Electronics Engineers 802.11 Specifications
   a. http://www.ieee802.org/11/

Appendix A - Minimum Requirements for Wi-Fi Devices

All Wi-Fi devices used in Interior Health must meet the following minimum requirements.

- Support 802.11n or 802.11ac capabilities within 5Ghz Spectrum
- support 802.1x or WPA2-AES Authentication
- Support a minimum of WPA2 Encryption
- Capable of supporting 40MHz channel widths
- Receive consistent software updates including operating system and certificate root stores
- Have a suitable wired or continuity strategy should Wi-Fi not be available or meet operating requirements