1. POLICY INTENT

The document establishes the policy for Radio Frequency (RF) devices used to transmit voice communications and medical data and telemetry at San Francisco Department of Public Health (SFDPH) facilities as well as to-and-from radio equipped vehicles (e.g., ambulances). It defines standards and guidelines to defend SFDPH resources and data from security threats associated with RF and wireless transmission and connection, to improve incident response for RF issues and regulate Radio Frequency (RF) access to and from the SFDPH Enterprise Network. This policy is intended to comply with those sections of the Code of Federal Regulations that govern HIPAA requirements for Information Security. The sections that relate to Wireless Network Devices (as a subset of Network Security in general) are CFR 164.310(b) and (c), the 2010 ‘HITECH act specifies the Federal enforcement and penalty aspects of this policy.

BACKGROUND: This Policy document is a revised version of the Radio Frequency-related policy previously in force. RF equipment uses lower frequency (<2.9 GHz) analog signals for on-site communications, emergency communications, vehicle dispatch etc. and from fixed-site digital wireless systems (e.g. monitors and telemetry) used in parallel with and as part of normal wired networks.

Due to advances in portable digital wireless capabilities (e.g., smart phones, palm tops, smart pads and laptops) with the capability to both transmit on the 3-4 Giga Hertz bands (3G and 4G) and to act as wireless access points (WAPs). This treated in a separate policy, and is referred to hereinafter as Wi-Fi refer to the DPH Wi-Fi Device and Information Transmission Security policy.

Inclusion by Reference: This policy is an annex to the SFDPH Data Network Policy. All of the principles, standards, guidelines and responsibilities described in the Data Network Policy are included as part of this document by reference. The purpose of this document is to further extend, refine and define how Data Network security, use and control principles apply in the wireless voice and data transmission context. For information on policy and standards for secure Remote Access to the SFDPH Data Network, refer to the Remote Access Policy.
For information on policy and standards for secure access to and use of wireless devices and for security of information stored in wireless devices, refer to the Workstation Policy and the Portable Computer Policy.

**Wireless connectivity cannot be guaranteed.** Frequency conflicts and signal interference can have a negative effect on the integrity of health information and telemetry transmitted wirelessly. Although this is a SFDPH security issue, technical and broader management considerations require that the issues of frequency management and assignment, as well as the prioritizing of frequency use and mitigating interference, among wireless technologies be addressed in a separate City-wide Wireless Access Controls policy or section.

2. **POLICY STATEMENTS**

2.1. **Planning and Approval:** All RF systems intended to or actually connected to the Enterprise Network are subject to the planning and approval process as defined in the Network Security Policy, Facilities Planning policies and Enterprise Wireless policy and such other SFDPH policies. Refer to the requirements for review and approval by other divisions and departments in the Data Network Policy.

2.2. **Wireless technology will only be used where appropriate.**

2.2.1. RF technology will not be used in areas where its emissions will interfere with the function of patient care technology and equipment.

2.2.2. RF technology will not be used as the primary or sole form of network connection where failure of the wireless technology will have serious consequences impairing safety, patient care, critical operational functions etc.

2.3. **Frequency and Deployment Rules** – All provisions of this policy are in addition to the requirements of the overall SFDPH Enterprise and CCSF Frequency Assignment, Deployment and Conflict Resolution policies and/or guidelines. Where the provisions of this policy and the Enterprise policies are in conflict, the Enterprise Policy takes precedence over this policy.

2.4. **Registration of Wireless Devices**
2.4.1. All wireless network access points and wireless devices must be registered with the Wireless Device Database managed by the SFDPH Information Technology (DPH-IT) Department at the time of device deployment.

2.4.2. DPH-IT will establish general risk mitigation strategies for RF devices, and standards for encryption, virus protection, password setting, signal interception avoidance and other preventative measures.

2.4.3. Prior to deployment, access points must meet the DPH-IT current wireless security standards. Refer to section 3.5 for details.

2.4.4. Only approved and registered access points are permitted for deployment within the SFDPH.

2.4.4.1. SFDPH will monitor networks for connection of unapproved (rogue) devices.

2.4.4.2. When detected, unapproved (rogue) devices will be removed from service by DPH-IT, and the person(s) responsible for the devices will be subject to disciplinary action.

2.5. Management and Security of Access Points

2.5.1. Management Tool Compatibility – All installed devices shall be compatible with the SFDPH standard for Network and Wireless Management Products.

2.5.2. Physical Security: Access points shall be properly secured within a safe, adequately monitored space to prevent theft, unauthorized access and physical tampering.

2.5.2.1. Fixed access points shall be regularly inspected at scheduled intervals to confirm that they are physically secure.

2.5.2.2. The network shall be regularly inspected at scheduled intervals to detect and remove unauthorized wireless access points.

2.5.3. Configuration Management: All wireless access devices must be secured using an administrative password that complies with the password requirements in the DPH-IT Password Policy.
2.5.3.1. Administrators must ensure all vendor default usernames and passwords are removed from devices as part of the registration process.

2.5.3.2. Administration of the devices will be accomplished via approved secure pathways.

2.6. **Broadcast Interference:** SFDPH reserves the right to limit or control the signal strength and propagation of all RF devices or classes of devices that fall within its jurisdiction or are used on its premises.

2.7. **Broadcast Security and Encryption**

2.7.1. DPH-IT will provide and maintain an up-to-date standards list that will include approved RF technologies, current minimum encryption standards, and best practices for secure installations.

2.8. **Access to SFDPH Facilities and Data**

2.8.1. Once a device is authenticated to an access point, users and devices must either be routed outside the SFDPH firewalls, or authenticate to the SFDPH network. Just as with a wired network, SFDPH network authentication must satisfy prescribed login/password standards before using SFDPH resources that are not normally accessible by nodes outside the SFDPH firewalls.

2.8.2. Access control mechanisms such as firewalls should be deployed to separate the RF network from the internal wired network.

2.8.3. As the technology permits, RF networks should employ a combination of layered authentication methods to protect Restricted sensitive, proprietary and patient information.

2.9. **Naming Conventions**

2.9.1. Final device names/call-letters are assigned during the registration process to avoid conflicts and confusion, and to aid DPH-IT in identifying, authenticating and locating wireless devices.
2.9.2. If technology allows for the broadcast of a device name, standardized names shall appear in the broadcast description, along with any unique identifiers assigned to the unit.

2.10. **Disruption and Interference**

2.10.1. All newly deployed RF technologies must satisfy all existing and future standards as required by law or established by DPH-IT.

2.11. **Accountability for Wireless Data Network Devices:** All additions and changes to SFDPH Data Networks, including RF and fixed network access points etc. will be documented in such a way that preserves an audit trail of the evolution of the network connections and of the persons performing and responsible for approving modifications.

3. **STANDARDS AND GUIDELINES**

3.1. **Compatibility and Compliance:** All deployed wireless technologies must satisfy all existing and future standards as required by law or established by the DPH-IT.

3.2. **Registration** - At the time of deployment, all wireless devices will be registered in the Central Wireless Device Database. DPH-IT will provide a secure interface for DPH-IT designated personnel to add, change and remove wireless devices on any SFDPH connected network. Registration information will include, but is not limited to, the following information:

- Contact information for owner and responsible parties, including the authorizing supervisor or manager.
- Locations where device is normally used and where it is stored when not in use
- Intended use and geographic coverage area
- Type of wireless technology deployed
- Manufacturer name and model number
- Device description
- SSID/ESSID (or equivalent)
- Hopping sequence (if applicable)

3.3. **Authentication** shall require at least two factors: A device’s registration code and the user’s logon/ID code. (see also 3.5.6 below)
3.4. **Periodic audits** of the wireless network will take place at scheduled intervals:

3.4.1. Physical security and technical vulnerability audits of wireless gateways and access points shall be performed no less than annually.

3.4.2. Unannounced sweeps for “rogue” access points are to take place at no less than six month intervals and will be conducted by *(Responsible unit to be determined)*

3.5. **Technology Standards** (NOTE: All standards in this section are effective as of the publication date of this policy, and are subject to revision as the technology evolves).

3.5.1. All factory default settings will be examined and reset to remove known vulnerabilities.

3.5.2. Transmitter frequency standard is 2.4 GHz.

3.5.3. Channels will be assigned by site and will not be changed without authorization.

3.5.4. Minimum Firmware Configuration requirements *(Also see Site Type Definitions in Section 6)*:

3.5.4.1. For SOHO (Small Or Home Office) and Consortium locations: Non Broadcast SSID and 128-bit static WEP encryption.

3.5.4.2. For Remote Sites and Major Sites: Non-Broadcast SSID, and either

  - EAP/TLS = TKIP = 802.11x. OR
  - Wireless Protected Access (WPA)

3.5.5. Access point hardware standards:

3.5.5.1. All sites (except SOHO) = Cisco AP1120B or 1230B

3.5.5.2. SOHO sites may use any access point hardware that permits proper configuration as defined in 3.5.4.1 above.

3.5.6. Authentication:

3.5.6.1. SOHO and Consortium sites will use access point authentication.

3.5.6.2. Remote and Major Sites will use centralized 802.11x authentication.

3.6. **Accountability for Wireless Portions of Data Network**: In addition to the specifications of the **Data Network Policy**, the following specifics for wireless access and devices apply.

3.6.1. **Activities to be Documented**:
4. RESPONSIBILITIES

4.1. **SFDPH Executive Management:**

4.1.1. Approves policy, standards and guidelines for the use of RF access to the SFDPH Data Network.

4.1.2. Directs the development and deployment of training in the appropriate and secure use of RF devices.

4.2. **The SFDPH CIO/CISO** is responsible for:

4.2.1. Implementing SFDPH-wide policy for RF devices and is ultimately responsible for the safety and security of the SFDPH Enterprise Network. The SFDPH CIO or designee must approve all exceptions to this policy.

4.2.2. Advocating and supporting DPH-IT security needs, concerns and projects to ‘Chief Officer’ and ‘Division Director’ level Senior management

4.2.3. Development, deployment and maintenance of policies for appropriate and secure use of RF network devices.

4.2.4. Directing the development and promulgation of training and orientation materials to enable and encourage employee awareness of the security problems and issues involved in the use of RF devices.

4.2.5. Directing the monitoring, and analysis of the state of compliance and risk-management of existing programs and procedures.

4.3. **DPH-IT:**

4.3.1. Develops and supports standards and procedures for the centralized registration of authorized devices and access points.

4.3.2. Develops and supports the procurement, implementation and maintenance of data-network RF intrusion and unauthorized use prevention technologies.
4.3.3. Will resolve any conflicts between RF devices in accordance with the guidelines in the SFDPH Wireless Frequency Management Policy. Priority is granted to fully supported and registered RF installations, except as appropriate in the case of medical, safety, or emergency devices.

4.3.4. Supports the regular scanning of the Radio Frequency spectrum at all SFDPH sites for vulnerable and/or unregistered wireless devices and will coordinate response with the SFDPH Technical Team in the event of a possible system intrusion or compromise.

4.4. **Responsible Unit to be determined** is responsible for:

4.4.1. Maintaining the list of acceptable RF frequencies and wireless technologies.

4.4.2. Assignment of frequencies and allocation of channels to individual sites.

4.4.3. Resolving conflicts between incompatible wireless devices.

4.4.4. Conducting periodic spectrum analysis to assess the potential impact of electromagnetic interference (EMI) from transmitters and the impact of electromagnetic emissions from wireless devices.

5. **PENALTIES FOR VIOLATIONS:**

5.1. **County of San Francisco General Workforce Violations:** Violation of published Information Security Policy, standards, guidelines, rules or procedures are subject to the same progressive discipline processes and sanctions as any other violation of the terms and conditions of employment at SFDPH.

5.2. **Individual Non-Employee and Third Party Workforce Violations:** Violation of published Information Security Policy, standards, guidelines, rules or procedures by persons employed through a third party or otherwise not subject to the progressive discipline processes and sanctions of the terms and conditions of employment at SFDPH are subject to the sanctions provided under the terms and conditions of the agreement(s) whereby their services are provided.

5.3. **Contractor and Third Party Entity Violations:** In addition to the individual sanctions noted in 2.1 and 2.2 above, third party organizations, business entities and others who are contractually required to comply with SFDPH Security Policies and standards may be subject to specified monetary fines or penalties or termination of the agreement as required for by the written contract and criminal penalties provided for in the applicable laws and regulations.
5.4. **Trusted Workforce Member Violations**: Managers, System Engineers, System Administrators and other classifications who are given greater than routine access to and control of critical information systems and data may be subject to stricter standards of security behavior and more abrupt and stringent penalties in the case of violations.

### 6. EXAMPLES AND ATTACHMENTS

#### 6.1. Site Type Definitions

- Single remote user located at home or private office
- Primary function of site is unrelated to SFDPH business or is a temporary or small, dedicated SFDPH site.
- Occasional access to SFDPH systems via VPN or Citrix Portal, fallback to dial-up
- Connectivity to SFDPH systems provided on a best-effort basis
- Large variation in PC, LAN, Firewall, DSL/Cable modem, and Wi-Fi equipment
- Consumer-grade, unmonitored, always-on Internet connection via DSL or Cable
- Minimal SFDPH support provided for only VPN or Portal connectivity to specific SFDPH applications

6.1.2. Consortium Site (Also refer to the Remote Access Policy).
- Small number of remote users located at an affiliated office
- Primary function of site is related to SFDPH business by affiliation
- Regular access to SFDPH systems via VPN or Citrix Portal, fallback to dial-up
- Connectivity to SFDPH systems provided on a best-effort basis
- Large variation in PC, LAN, Firewall, and DSL router equipment; minimum SFDPH requirements for standardized VPN, Firewall, and Wi-Fi hardware and software
- Business-grade, monitored, low-priority, always-on Internet connection via DSL
- Minimal SFDPH support provided for only VPN or Portal connectivity to specific SFDPH applications
6.1.3. SFDPH Remote Site (Also refer to the Remote Access Policy).

- Small to medium number of remote users located at an SFDPH clinic or office
- Primary function of site is SFDPH business
- Continuous access to SFDPH systems via dedicated circuit with built-in ISDN backup
- Connectivity to SFDPH systems provided on a guaranteed basis
- Standardized equipment provided and installed by SFDPH
- Business-grade, monitored, high-priority, dedicated private WAN connection
- Full SFDPH support provided for network connectivity (LAN/WAN) to SFDPH applications
6.1.4. Major Site

- Large number of users located at SFGH, 1380 Howard, 101 Grove, LHH, etc.
- Primary function of site is SFDPH business
- Continuous access to SFDPH systems via redundant WAN and high-availability LAN
- Connectivity to SFDPH systems provided on a guaranteed basis
- Standardized equipment provided and installed by SFDPH
- Business-grade, monitored, high-priority, dedicated, and redundant private WAN connections
- Full SFDPH support provided for network connectivity (LAN/WAN) to SFDPH applications

6.2. Policies to be Developed or Included:

6.2.1. Obtaining Authorization to Install, Move, Remove or Change Wireless Network Devices.

6.2.2. CCSF Frequency Assignment, Deployment and Conflict Resolution policies and/or guidelines