Date: 03/28/19

Version 1.0

Wi-Fi Policy Template

# 1. 0 Purpose

To provide adequate security and privacy protections for data transmitted on all wireless connections involving Business’s and its Affiliates' (collectively, Business’s) network.

# 2.0 Policy

A. Wireless access to Business’s network and data shall be permitted only as set forth in this policy. For the purposes of this policy, wireless access is defined as wireless connections using the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standard.

B. Guest networks shall be segregated from the Business’s internal network. Therefore, this policy does not apply to wireless networks installed for guests.

C. Any wireless device connected to Business’s network that does not meet these requirements is unauthorized and subject to immediate removal from the network and confiscation of equipment.

D. Wireless networks shall be monitored to detect intrusions by unauthorized wireless devices.

E. Any exception, change or deviation from this policy must be reviewed and approved by IT services.

## 3.0 Physical Location Standard

A. Wireless Access Points (WAP) shall be strategically placed to limit bandwidth coverage to the minimum necessary for the operation of wireless devices (e.g., center of the room, avoid windows). If such placement is not possible, the power radiated by the WAP shall be adjusted to minimize leakage into areas outside Business’s facilities.

B. Physical access to WAPs shall be restricted.

C. WAPs shall be monitored by our IT services team. Alerts shall be generated when devices become unresponsive due to power outage or theft or when rogue WAPs are connected.

## 4.0 Installation Standard

A. All wireless infrastructure devices (e.g., WAPs, wireless controllers and wireless monitoring tools) shall be configured by our IT services team or their authorized representative before accessing the physical network.

Date: 03/28/19

Version 1.0

Wi-Fi Policy Template

B. The installation of all wireless devices shall ensure authorized use and data encryption.

C. All wireless devices shall be purchased through IT services or procurement department.

D. Wireless devices shall maintain a hardware address that can be registered and tracked by IT services.

E. A WAP may have multiple logical networks defined (Virtual Local Area Networks, or VLANs). Each VLAN may have different levels of security. Wireless service set identifiers (SSID) that grant access to Business’s corporate network and support the Access Control and Encryption Standards below (e.g. Enterprise WPA and PEAP) or stronger may be broadcast. Any SSID that does not meet these criteria shall not be broadcast.

F. All WAPs must be attested to by the IT services group and inventory records maintained within the organization's asset management personnel. Vendor defaults on WAPs must be changed from supplied settings before deployment into the Business’s environment.

## 5.0 Encryption Standard

A. All wireless communication shall be encrypted.

B. For devices that cannot support the encryption standard outlined immediately above, a policy exception must be filed. Prior to connecting these devices to Business’s network, configurations shall be made to support the highest level of encryption the device can support and mitigating controls shall be put in place (e.g. restrict connections using the weaker encryption method to only approved devices based on Machine Authentication Code [MAC] address).

## 6.0 Monitoring Standard

A. Wireless networks shall be monitored to detect intrusions by unauthorized wireless devices. This shall be accomplished either through a wireless control system that identifies unauthorized devices in real-time, or via periodic scans for rogue WAPs. These scans shall be documented to provide evidence of the date of the scan, results of the scan, and any actions that were taken as a result of the scan.

# 7.0 Applicability

A. This policy is applicable to all users - employees, customers and affiliates who are on site.

# 8.0 Other Applicable Policies

A. None