Wireless Access Point Policy

Purpose

The purpose of this policy is to limit and restrict the number of wireless access points, within the organization's premises, connecting to Banks DIH Limited's internal network or related technology resources via any means involving wireless technology.

The overriding goal of this policy is to protect Banks DIH Limited's technology-based resources (such as corporate data, computer systems, networks, databases, etc.) from unauthorized use and/or malicious attack that could result in loss of information, damage to critical applications, loss of revenue, and damage to our public image. Therefore, all users employing wireless methods of accessing corporate technology resources must adhere to company-defined processes for doing so, using company-approved access points.

Scope

This policy applies to all Banks DIH Limited employees, including full-time staff, part-time staff, contractors, freelancers, and other agents who utilize mobile devices to access the organization's data and networks via wireless means. Wireless access to enterprise network resources is a privilege, not a right. Consequently, employment at Banks DIH Limited does not automatically guarantee the granting of wireless access privileges.

This policy is complementary to any previously implemented policies dealing specifically with network access and remote access to the enterprise network.

Access Points

Banks DIH Limited is committed to providing authorized users with wireless access to the Internet, Banks DIH Limited networks, and systems, as well as other corporate resources. To make this convenient service available to end users, the IT Department must install "access points" in and around the premises wherever wireless access to company resources is designated. These access points are generally small, antenna-equipped boxes that connect directly to the local area network (LAN), converting the LAN's digital signals into radio signals. The radio signals are sent to the network interface card (NIC) of the mobile device (e.g., tablets, laptop, mobile phones, etc.), which then converts the radio signal back to a digital format the mobile device can use.

- As the number of wireless connections increases, so too does the danger of "rogue" access points be surreptitiously installed. Rogue access points are antennas that are installed without the knowledge or permission of Banks DIH Limited, used by hackers, internal employees, or trespassers to gain illegal access to the company network and Internet connection for the purposes of sabotage, spamming, corporate espionage, personal gain, and so on.

- All wireless access points will be centrally managed by Banks DIH Limited's IT Department and will utilize encryption, strong authentication, and other security methods at IT's discretion. Addition of new wireless access points within corporate facilities will be managed at the sole discretion of IT. Non-sanctioned installations of wireless

equipment, or use of unauthorized equipment within the organizational premises, are strictly forbidden.

Policy Restrictions

1. Banks DIH Limited uses the 802.11b/g/n/ ac/ ax protocols as its wireless network standard, transmitting at the 2.4-5 GHz radio frequency spectrum, with the intention of delivering speeds of up to 400 Mbps to mobile and wireless devices.

2. Banks DIH Limited's IT Department will support only the following devices and equipment for accessing corporate networks and systems wirelessly:

    - Cisco Meraki Access Points.
    - Any 802.11 b/g/n/ ac/ ax wireless NIC cards and/or 10/100/1000 LAN cards.
    - Any compliant laptop, tablet, smartphone, etc.

3. The IT Department will strive to purchase only those access points and equipment that possess the following characteristics and/or features:

    - RADIUS authentication.
    - SNMP.
    - Syslog.
    - WPA encryption or 802.11i-compliant.
    - Power-over-Ethernet (PoE).
    - Backward compliant with 802.11b (if product is 802.11g / ac/ ax)
    - High plenum rating, fire-resistant.
    - Wide temperature range for outdoor use.
    - Anti-theft physical security measures.

4. All wireless clients and devices shall be equipped with a host-based personal firewall and anti-virus software. The user shall update these applications as required and will not reconfigure them in any way.

5. Whenever necessary, the IT Department will conduct a site survey to determine the appropriate placement of new or additional access points. All installations will follow all local safety, building, and fire codes.

6. All wireless access points, including those designated for networking home offices or satellite offices (branch) with the corporate network, must be approved by Banks DIH Limited's IT Manager.

7. All access point broadcast frequencies and channels shall be set and maintained by the IT Department. Any device or equipment found to be interfering with access point signals may be subject to relocation or removal, including cordless phones, microwave ovens, cameras, light ballasts, etc.

8. Use of the wireless network is subject to the same guidelines as Banks DIH Limited's technology and Internet acceptable use policies.

9. All data that traverses the corporate wireless network must be encrypted, using WPA1 and WPA2 at minimum. The IT Department will strive to procure only WLAN equipment that supports WPA and will also provide suitable software for authentication and encryption.

10. Banks DIH Limited's IT Department cannot guarantee 99.999 percent availability of the wireless network, especially during inclement weather. Nevertheless, the IT Department will make all possible network adjustments within the supported radio frequency spectrum.

11. The IT Department will conduct sweeps of the wireless network daily, using tools such as Cisco Meraki dashboard, Cisco Meraki Air marshal, Solar Winds SNMP, to ensure there are no rogue access points present. Empty rooms and offices will also have their network jacks disconnected from the switch to mitigate rogue access point installation.

12. The IT Department reserves the right to turn off without notice any access point connected to the network that it feels puts the company's systems, data, users, and clients at risk.

13. The wireless access user agrees to immediately report to his/her manager and Banks DIH Limited's IT Department any incident or suspected incidents of unauthorized access point installation and/or disclosure of company resources, databases, networks, and any other related components of the organization's technology infrastructure.

14. Any questions relating to this policy, as well as any help desk inquiries, should be directed to the IT Manager or Network Administrator in the IT Department, at 592-225-0917 or 592-226-9584 or helpdesk@banksdih.com.

15. Policy Non-Compliance

Failure to comply with the Wireless Access Point Policy and subsequent agreement may result in the suspension of remote access privileges, disciplinary action, and possibly termination of employment.

Employee Declaration

I, , have read and understand the above Wireless Access Point Policy, and consent to adhere to the rules outlined therein.

_____	_____
Employee Signature	Date
_____	_____
Manager Signature	Date
_____	_____
IT Administrator Signature	Date