Insert the organization logo by clicking on the image icon

Wireless Security Policy Template

Date:

**Document Control**

|  |  |
| --- | --- |
| **Document Title:** | Wireless Security Policy Template |
| **Document ID:** |  | Version: | 0.1 |
| **Status:** | Draft |  |
| **Publish Date:** |  |

**Document Review**

|  |  |  |  |
| --- | --- | --- | --- |
| Version No. | Date | Reviewer(s) | Remarks |
|  |  |  |  |
|  |  |  |  |

**Table of Contents**

[1. Objective 4](#_Toc97463415)

[2. Scope 4](#_Toc97463416)

[3. Policy 4](#_Toc97463417)

[3.1 General Requirements 4](#_Toc97463418)

[3.2 Authorization 4](#_Toc97463421)

[3.3 Authentication of Wireless Clients 4](#_Toc97463422)

[3.4 Encryption 5](#_Toc97463431)

[3.5 Wireless Access Control. 5](#_Toc97463433)

[3.6 Wireless Client Security Standard 5](#_Toc97463434)

[3.7 Wireless Physical Security 5](#_Toc97463435)

[3.8 Wireless Logical Security 6](#_Toc97463436)

[3.9 Inventory Monitoring and Audit 6](#_Toc97463437)

[3.10 Guests and Visitors wireless access 6](#_Toc97463438)

[3.11 Deployment and Configuration 7](#_Toc97463439)

[4. Policy Enforcement 7](#_Toc97463440)

1. **Objective**

The objective of this policy is to minimize risks associated with using wireless network access, and defines controls against the threats of unauthorized access, theft of information, theft of services, and malicious disruption of services.

1. **Scope**

This policy applies to employees, contracted personnel, trainees and any third parties’ representatives who have been provided access to wireless services at the organization/ entities.

1. **Policy**

## General Requirements

1. Designated Security Team (DST) should ensure that all wireless LAN accesses have approved security configurations.
2. DST should Use approved encryption protocols.
3. Information Technology (IT) team should maintain a hardware address (MAC address) that can be registered and tracked.
4.
5.

## Authorization

* + 1. All deployments of wireless network should be controlled and approved by DST.

## Authentication of Wireless Clients

* 1.
	2.
	3.
1.
2. 1.
	2.
	3.
3. All access to wireless networks must be authenticated by leveraging the AAA infrastructure established by the <entity name>.
4. The strongest form of wireless authentication permitted by the client device shall be used. For most wireless devices, WPA or WPA2 with 802.1x/EAP-PEAP, Extensible Authentication Protocol – Transport Layer Security (EAP / TLS) must be used. WPA2 is preferred wherever possible unless there is a technological limitation. Minimum of 128-bit encryption must be used. Technological Limitations should be resolved as soon as possible, and periodic review and monitoring should be performed.
5. WPA keys shall be changed, after a known or suspected compromise, or when there are personnel changes.
6. Factory default WPA keys shall be changed before deployment.

## Encryption

* 1.
1. The strongest form of wireless encryption permitted by the client device shall be used, WPA using TKIP encryption or WPA2 using AES-CCM encryption must be used.
2. Wireless equipment that does not support at least 128-bit key encryption shall not be used.

## Wireless Access Control.

1. Direct or remote access to the <entity name> network should be in accordance with Access Control and physical Security Policy.
2. Unnecessary protocols shall be blocked.
3. File sharing on wireless client devices shall be disabled.
4. Service set IDs (SSIDs) must be changed from the factory default to something that is meaningless to outsiders. SSID character strings must not reflect company Name, location, or product being used.
5. Broadcast mode of SSIDs shall be disabled.
6. The wireless network shall be configured with the longest beacon interval.
7. The wireless solution connected to the <entity name> network should be secured by network firewall.

## Wireless Client Security Standard

1. <entity name> team should ensure that all wireless clients must have security-related operating system patches applied.
2. The wireless client must comply with <entity name> security policy before network access granted by implementing a Network Access Control (NAC).
3. The wireless solution should secure in such a way that can:
* Detect and Disable Rogue APS.
* Protect from Denial of Service and Impersonation
* Protect Man-in-Middle.

## Wireless Physical Security

1. The physical area where the wireless LAN is to be deployed should be identified and documented.
2. Access points shall be physically secured upon proper configuration to prevent tampering and reprogramming (i.e., to prevent unauthorized physical access).
3. Access points shall be placed in secure areas, such as high on a wall, in a wiring closet, or in a locked enclosure to prevent unauthorized physical access and user manipulation. Access points shall not be placed in easily accessible public locations.
4. In areas where utilization is not required on 24/7 basis, access points shall be turned off during all hours during which they are not used (e.g., after hours and on weekends) to minimize potential exposure to malicious activity.
5. In the event of resetting function for an access point is used, the device must be restored to the latest security settings.
6. All security settings and baseline configurations shall be backed up and stored securely.
7. Access points signals range must be undetectable outside the <entity name> premises boundaries.

## Wireless Logical Security

1. All insecure and nonessential management protocols such as (Hypertext Transport Protocol (HTTP) and Simple Network Management Protocol (SNMP)) shall be disabled.
2. If SNMP is turned on for management purposes, the SNMP community strings must be changed from their manufacturer default to unique and difficult to guess strings. SNMPv3 and/or SSL/TLS for Web-based management of access points should be utilized
3. When disposing any wireless equipment, it shall be ensured that all configurations and security settings are erased completely.
4. Placement of access points and channel assignments shall be such that coverage/throughput is maximized while interference (denial of service) is kept to a minimum between different access points or WLANs.

## Inventory Monitoring and Audit

1. All wireless connections shall be routinely monitored, and security audits performed to verify the compliance with this policy, access points and wireless devices are authorized, and to identify unauthorized activity.
2. Access logs and system audit trails shall be enabled at the access point and reviewed regularly.
3. Intrusion Detection Systems (IDS) should be deployed on the wireless network to report [suspected activities](https://medium.com/%40tnbizacct/think-like-the-adversary-2bc304a0afe6).
4. Network vulnerability scanner should be deployed on the wireless network to report threats and vulnerability.

## Guests and Visitors wireless access

1. Deploy an untrusted wireless access point for guests and visitors not connected to <entity name> network.
2. Deploy for a Virtual Local Area Network (VLAN) separated and unrouted in the <entity name> network for the guests and visitor’s wireless network.
3. Allow guests and visitors to access internet only.

## Deployment and Configuration

1. Wireless access points (WAP’s) should be deployed and setup by the IT team and approved by DST.
2. **Policy Enforcement**
3. Policy document sponsor and owner: <Head of Cyber Security Department>.
4. Policy implementation and enforcement: <Department Concerned with Information Technology>.
5. Any violation of this policy may subject the offender to disciplinary action as per the procedures followed in <entity name>.

-End of the Document-