Wireless Access Point Standard

Objective

In accordance with the Information Security and Acceptable Use Policy, all systems owned or managed by the University of Texas at Dallas must be adequately protected to ensure confidentiality, integrity, availability, and accountability of such systems. Wireless access points are used to extend University network segments and provide access to networked hosts via wireless connection methods. As a result, wireless access point might be accessible from beyond physically secured University buildings and properties.

Physical Location

Wireless access points should be installed in inconspicuous locations and be appropriately secured to limit the possibility of theft or tampering. Installation in a physically secured office suite provides adequate security; access points located in public-use areas may benefit from additional security measures such as locks.

Support Requirements

When feasible, all access points should be provided and centrally maintained by the Office of Information Resources. All wireless access points must have a valid support contract or, in the case of open-source software, be commercially or community supported.

Patching

Security patches and/or device firmware for all wireless access points must be installed in a timely manner, depending on the likelihood and impact of vulnerability exploitation.

Configuration

- **Authentication**: IEEE 802.1x or similar user authentication, based on UTD NetID, is required for wireless access points connected to UTD’s internal networks where Confidential or Controlled Data is accessible. Guest networks configured to provide general Internet access only do not require authentication.

- **Encryption**: WPA2 or stronger encryption is required. WEP and WPA are not sufficiently secure and must not be used.

- **Default Settings**: Default settings for encryption keys, SNMP passwords, pre-shared keys, and passphrases must be changed prior to wireless access point implementation.
**Server Registration**

All wireless networks and access points must be recorded with the Information Security Office’s Server Registry application.

The University wired network may not be extended using unauthorized and/or consumer-grade hardware without the review and authorization of the Office of Information Resources.

**Logging**

Activity must be logged and retained for a minimum of 90 days to facilitate troubleshooting and investigations. The following types of activities must be logged:

- Successful and unsuccessful login attempts
- Any device modification operation
- Rejected connection attempts. Logging of allowed connections is recommended when feasible.

Logs should also be sent to a centralized logging server to reduce storage requirements on local systems and reduce feasibility of log tampering.

**Incident Management**

System owners are required to report any suspicious activity to the Information Security Office for investigation.

**Backup / Recovery**

Backup and recovery procedures must be established to ensure that wireless networks can be rebuilt in the event of a disruptive event. Further, configuration backups should be captured before significant configuration changes to ensure a method of failing back after an unexpected disruption. Backup media should be encrypted if transported or stored outside of a UTD facility.

**Exemptions**

In the event that compliance with this standard cannot be met, please contact infosecurity@utdallas.edu to submit an exemption request which will be approved or denied by the CISO. Denied exemption requests may be appealed to the UTD President for final decision.