Security Standard Wireless Network (SS-019)

Chief Security Office

Date: March 2020

Department for Work & Pensions

1. Revision History

Version	Author	Description	Date
0.0a		First Draft	05/04/17
0.0b		Amended to include initial review feedback	25/04/17
0.0c		Amended to include feedback from Standard & Pattern Team	05/05/17
0.0d		Amended to include additional feedback from Standard & Pattern Team and controls mapping added	11/05/17
0.0e		Amended to include SME feedback	23/05/17
0.0f		Issued for CSO sign-off	14/06/17
1.0		First published version	04/07/17
1.1		Version for external publication	30/03/20

2. Distribution

Version	Role/Area	Role	Date

3. Approval History

Version	Approver Title	Role	Date
1.0		Chief Security Officer	04/07/17
1.1		Chief Security Officer	30/03/20

This document will be reviewed for continued completeness, relevancy and accuracy within 1 year of being granted "final" status, and at yearly intervals thereafter.

Contents

4. Introduction

4.1. This Wireless Network Security Standard provides the list of controls that are required to secure IEEE 802.11 wireless networks to an Authority approved level of security. This standard provides a list of security controls to protect citizen and operational data. It is to minimise the risk from known threats both physical and logical to an acceptable level for operations.

4.2. Furthermore, the security controls presented in this standard are taken from the international best practice for Wireless Security and have been tailored for Authority suitability.

5. Purpose

5.1. The purpose of this document is to enable Suppliers to work to a defined set of security requirements which enable solutions to be developed, deployed and managed to Authority security standards, which are based upon international best practice for Wireless Network deployments.

5.2. For further clarity and relevance, the security standard is intended to provide secure configuration advice to projects for wireless local area network deployment.

5.3. Secondly, this standard provides a means to conduct compliance based technical security audits.

6. Exceptions

6.1. Any exceptions to the application of this standard or where controls cannot be adhered to MUST be presented to the Authority where appropriate. This MUST be carried out prior to deployment and managed through the design caveats or exception process.

6.2. Such exception requests may invoke the Risk Management process in order to clarify the potential impact of any deviation to the configuration detailed in this standard.

6.3. Exceptions to this standard MUST be maintained on a risk register for accountability, traceability and security governance reporting to the Authority.

7. Audience

7.1. This standard is intended for Suppliers, solution and technical architects, developers, security groups, and also IT staff such as Security Compliance

Teams, involved in securing environments for Authority systems and applications.

8. Scope

8.1. This standard is to cover systems handling data within the OFFICIAL tier of the Government Security Classification Policy (GSCP). All of the organisation's IEEE 802.11 wireless networks falling within this category will be subject to the requirements specified within this security standard. The requirements will be applied to new and existing installations.

8.2. The security control requirements laid out in this standard are product agnostic and applicable for all wireless network systems that are provisioned for Authority use.

8.3. In the event of uncertainty on the controls laid out in this standard please contact the Authority for guidance and support on items which require clarification.

9. Security Controls Assurance

9.1. Controls presented in this standard or referred to via this standard may be subjected to a formalised IT Health Check or Penetration Test to provide evidence of adequacy and effectiveness.

10. Technical Security Control Requirements

In this document the term MUST in upper case is used to indicate an absolute requirement. Failure to meet these requirements will require a formal exemption (see section [6. Exceptions] above).

10.1. Policy and Procedures

Reference	Security Control Requirement
10.1.1.	A wireless network usage policy MUST be established and reviewed at planned intervals (at least annually). It must, at minimum, specify: • the wireless network user authentication; • access control for both employees and guest or non-employees to the wireless network; • employees accessing other wireless networks outside of the control of the employees • who has the authority to allow access points to connect to the Authority network. • which user communities are authorized to use WLAN technology and for what purposes • user responsibilities for the hardware, software and data in relation to the network and its security.
10.1.2.	The Supplier MUST enforce the wireless security policies through the appropriate security controls.

Reference	Security Control Requirement
10.1.3.	There MUST be appropriate knowledge and training in the introduction of new wireless network systems and updated security practices, controls, procedures, and architectures.

10.2. Wireless Network General Requirements

Reference	Security Control Requirement
10.2.1.	All products (e.g. access points, servers, equipment & software) MUST support WPA2 or successor standards. They must have been assured/validated prior to purchase.
10.2.2.	As a minimum, all WLAN components MUST use CCMP (utilising AES Key Wrap with HMAC-SHA-1-128) to protect the confidentiality and integrity of WLAN communications.
10.2.3.	All endpoint devices that attempt to wirelessly connect to an Authority network MUST be authenticated.
10.2.4.	The authentication method chosen for Authority wireless networks MUST be assessed as suitable for deployment by the Authority
10.2.5.	All network components MUST be configured to reduce the risk of being compromised as per SS-018 Network Security Design Security Standard. There must be standardized security configurations for common WLAN components, such as client devices and Access Points (APs).
10.2.6.	Unneeded network connections, network services and ports on managed endpoints, access points and authentication servers MUST be disabled to reduce attack surface (e.g. if a device is already connected to a wired network access, WLAN access is usually redundant and should be disallowed).
10.2.7.	There MUST be security functions on the external gateway to supplement the controls on the end user devices. This includes all or a combination of: • logging all web access to audit compliance with corporate policy, and provide more situational awareness when an attack is detected elsewhere on the network • anti-malware scans on files and web pages before they are loaded on the end user device • reputational filtering to block potentially malicious sites based on data from cloud anti-malware services • filtering out categories of sites deemed inappropriate for the workplace • applying data loss protection rules to attempt to block sensitive data being accidentally sent to the Internet • preventing the user from installing an untrusted root Certificate Authority's certificate
10.2.8.	There MUST be a robust boundary (with network security enforcing components) between each WLAN and the enterprise network/the internet.
10.2.9.	Boundaries of the wireless network MUST in addition comply with SS-006 Security Boundaries Security Standard.
10.2.10.	Where there has been Authority risk assessment approval for pre-shared keys to be used to establish network associations, they MUST be replaced frequently - at least once every 30 days.
10.2.11.	If PSKs are used to establish network associations, no key MUST be shared across multiple endpoint devices.
10.2.12.	Any certificates on the endpoints and the servers used for wireless authentication MUST be periodically updated.
10.2.13.	Access Points, Authentication Servers other wireless infrastructure components MUST be subject to the Authority SS-033 Patching Security Standard.
10.2.14.	Risk assessment MUST be performed to determine the necessity for additional technical countermeasures required such as wireless location services, passive/active WLAN scanners, wireless intrusion detection and protection systems, and spectrum analysis.

Reference	Security Control Requirement
10.2.15.	There must be regular auditing (at least annually) of the security configurations of the Wi-Fi network components such as the client device and the access points to ensure that they comply with a minimum level of security
10.2.16.	There MUST be comprehensive WLAN security assessments (e.g. IT Health Check) at regular and random intervals, preferably at least once annually. Any detected vulnerabilities must be fixed by patching applications, OS and devices or by using secure configurations and hardening devices.

10.3. Access Points (APs)

Reference	Security Control Requirement
10.3.1.	WEP and TKIP MUST be disabled in the configuration of each AP.
10.3.2.	The Service Set Identifier (SSID) of the Access Point (AP) MUST be changed from its default.
10.3.3.	Access points (APs) MUST not be connected directly to the enterprise network as this could provide an unprotected route into the network. The wireless infrastructure must be separate from the enterprise network.
10.3.4.	Access Points MUST terminate associations after a configurable time period (as assessed suitable by risk assessment).
10.3.5.	A Group Master Key (GMK), where applicable, MUST be configured on the AP with a maximum lifetime (not to exceed 24 hours).
10.3.6.	APs MUST have a logically or physically independent management support interface.
10.3.7.	The standard security configuration MUST be re-applied to an AP whenever its reset function is used.
10.3.8.	There MUST be a site survey to determine the proper location of APs, given a desired coverage area. Preferably, the estimated usable range of each AP should not extend beyond the physical boundaries of the facility.
10.3.9.	Access Points (APs) MUST be physically inaccessible to unauthorised users.

10.4. Authentication Servers (ASs)

Reference	Security Control Requirement
10.4.1.	The security of any authentication server MUST be established in accordance with SS-008 Server Operating System Security Standard.
10.4.2.	Servers MUST be identified by their fully qualified domain name (e.g., as1.xyzAgency.gov) so that the name listed in the Authentication Server's certificate can be compared with the name specified in the managed endpoint device's configuration. Managed endpoints should also be configured to accept certificates only from the CA that signed the server certificates (see SS-002 PKI Security Standard for further requirements for certificates).
10.4.3.	Managed endpoints MUST be configured to specify valid Authentication Servers (ASs) by name.
10.4.4.	A Public Master Key (PMK), where applicable, MUST be configured on the AS with a maximum lifetime, preferably not to exceed eight hours.
10.4.5.	Any communications between each Access Point (AP) and its corresponding Authentication Servers (AS) MUST be protected sufficiently through cryptography (see SS-007 Use of Cryptography Security Standard).
10.4.6.	The cryptographic software on the authentication server MUST be deployed in accordance with SS-007 Use of Cryptography Security Standard.
10.4.7.	The AS MUST be configured to use authorised methods only, as assessed suitable for deployment by the Authority
10.4.8.	ASs MUST only grant authorisations for a configurable time period (as assessed suitable by risk assessment).

10.5. Enterprise Network

Reference	Security Control Requirement
10.5.1.	Access to enterprise resources from a mobile wireless device MUST be in compliance with SS-016 Remote Access Security Standard.
10.5.2.	Users wishing to access enterprise network services MUST be in possession of the credentials required to pass through the VPN gateway. Wireless endpoints MUST authenticate with the VPN gateway after associating with the managed wireless infrastructure.
10.5.3.	The enterprise network MUST be periodically surveyed to confirm that APs have not been attached directly to the enterprise network. The frequency of these surveys will depend on the risk appetite and the information sensitivity of the data passing through the network.

10.6. Partner Users

Reference	Security Control Requirement
10.6.1.	Partner users MUST be able to directly access their organisation's VPN gateway without requiring authentication to the access layer (i.e. bypassing the captive portal).

10.7. Audit and Monitoring

Reference	Security Control Requirement
10.7.1.	Audit and monitoring MUST be done in compliance with SS-012 Protective Monitoring Security Standard.
10.7.2.	Audit and monitoring information MUST be taken from the components within the architecture. Example events that must be recorded include: • Centralised logging on the access points MUST be enabled to record user and event activity such as client access success/failure events, authentication success/failure events, client association history, timestamps, MAC addresses, usernames, type of event, reboots, association/de-associations, identification of rogue access points. • Configuration changes to the service/infrastructure, including VPN gateway and wireless infrastructure. Unauthorised changes must be investigated • Traffic flows through the firewall, ensuring that any configuration errors that could allow flows from the wireless infrastructure to the internet are caught promptly
10.7.3.	In addition, where guest/partner users are permitted to connect to a wireless network, the following MUST be logged or monitored: • Guest users that successfully authenticate to a captive portal/the guest Wi-Fi must be logged. Multiple failed attempts to authenticate to the portal should be investigated • Changes to the configuration of a captive portal/Guest Wi-Fi must be logged together with the user carrying out the change. Unauthorised changes should be investigated • Attempts to access white-listed VPN gateways must be logged. Such logs may be used to investigate an attack on a white-listed gateway from the enterprise wireless infrastructure • Abnormally high bandwidth usage by guests or partners must be logged and investigated further • Tests must be undertaken to ensure that logged traffic flows can be attributed to individual user credentials in case malicious use needs to be investigated
10.7.4.	There MUST be both attack monitoring and vulnerability monitoring to support WLAN security. The monitoring solutions for the wireless network should provide most, if not all, of the following detection capabilities:

Reference	Security Control Requirement
	ATTACKS • Unauthorized WLAN devices, including rogue APs and unauthorized client devices • Unusual WLAN usage patterns, such as extremely high numbers of client devices using a particular AP, abnormally high volumes of WLAN traffic involving a particular client device, or many failed attempts to join the WLAN in a short period of time • The use of active WLAN scanners (e.g. war driving tools) that generate WLAN traffic. The use of passive sensors cannot be detected through monitoring controls. • DoS attacks and conditions (e.g., network interference). Many denial of service attacks are detected by counting events during periods of time and alerting when threshold values are exceeded. For example, a large number of events involving the termination of WLAN sessions can indicate a DoS attack. • Impersonation and man-in-the-middle attacks. For example, some WIDPS are able to detect these • Any radio frequency jamming signal emanating from an attacker or from an accidental source. VULNERABILITIES • WLAN devices that are misconfigured or using weak WLAN protocols and protocol implementations
10.7.5.	There MUST be wireless security audit processes and procedures that identify the types of security relevant events that should be captured, and determine how audit records will be securely stored for subsequent analysis.

10.8. Access Control

Reference	Security Control Requirement
10.8.1.	Access points, that are either managed individually or via centralised management facilities (to enable single admin account access), MUST have strong, unique administrative passwords (changed from default) in accordance with the Authority's SS-001 pt1 Access and Authentication Controls Security Standard and User Access Control Policy.
10.8.2.	Users MUST only be provided with access to the wireless network and wireless network services that they have specifically been authorised to use, with users' access rights being regularly reviewed.
10.8.3.	Access and Authentication must in addition be in accordance with the appropriate controls in SS-001 Access and Authentication Security Standard.

10.9. Administration

Reference	Security Control Requirement
10.9.1.	As part of a privileged user management regime, the allocation and use of privileged access rights of the wireless network infrastructure MUST be restricted and controlled to authorised administrators. They must be appropriately trained and cleared network administrators.
10.9.2.	Management of the wireless infrastructure MUST be carried out over a wired interface. Where this cannot be prevented, such as when diagnosing and correcting Radio Frequency (RF) problems, the wireless management interface should be disabled when not in use.
10.9.3.	Administration and network management of WLAN infrastructure equipment (i.e., APs and ASs) MUST involve strong authentication and encryption of all communication (in accordance with SS-007 Use of Cryptography Security Standard).
10.9.4.	Network management information between APs/ASs and network management servers or consoles MUST be transmitted over a dedicated management VLAN.
10.9.5.	Access points (APs) MUST support authentication and data encryption for administrative sessions (e.g. SSL/TLS v1.2 (or above) support for web-based administration and secure shell (SSH) for command-line administration).

Reference	Security Control Requirement
10.9.6.	All insecure and unused management protocols on the APs MUST be disabled, and configure remaining management protocols for least privilege.

10.10. Incident management

Reference	Security Control Requirement
10.10.1.	Any security incidents relating to Authority wireless networks should be managed in accordance with SS-014 Security Incident Management Security Standard.

11. Compliance

Compliance with this standard MUST occur as follows:

Compliance	Due Date
On-going	From the first day of approval
Retrospective	Within 6 months of the approval of the standard.

12. Accessibility

No user interfaces are included in this standard and accessibility is not applicable as part of this standard. However, it is deemed that Suppliers implementing this standard are obliged to incorporate accessibility functions where necessary.

13. Reference Documents

CESG Architectural Patterns: Wireless Networking, October 2015, Issue No 1.1

NCSC End User Devices Guidance

NIST Special Publication 800-97: Establishing Wireless Robust Security Networks – A guide to IEEE 802.11i

NIST Special Publication 800-153: Guidelines for Securing Wireless Local Area Networks (WLANs)

BS ISO/IEC 27033-6:2016: Information technology – Security techniques – Network security, Part 6 – Securing Wireless IP Network Access

14. Definition of Terms

Access Point (AP)	The access point provides an endpoint with wireless access to services on a wired network. An AP logically connects endpoints with a distribution system (DS), which is typically an organization's wired infrastructure. APs can also logically connect wireless endpoints with each other without accessing a distribution system.
Captive portal	A captive portal presents an authentication page to guest users that require access to the Internet. This may be used to control access and provide auditing capability to support governance.
Enterprise users	Enterprise users are employees of the Authority. They will usually be given use of a managed wireless endpoint.

Endpoints	A wireless endpoint device. Typical examples of endpoints are laptop computers, personal digital assistants (PDA), mobile phones, and other consumer electronic devices with IEEE 802.11 capabilities.
Guest users	Guest users are likely to be users visiting the HMG department requiring Internet access. Guest users will typically be in possession of an unmanaged endpoint.
Hardening	Process of securing a system by reducing its surface of vulnerability
Managed component	A managed component is one that is managed by the enterprise deploying the wireless solution. The enterprise will have increased confidence about the integrity, configuration and maintenance of such components. Managed components should be patched according to an enterprise patching policy and may have additional technical protections designed to protect their confidentiality and integrity.
Partner users	Partner users will typically be employees of a department that has a trust relationship with the HMG department deploying the wireless solution. This, for example may be employees from a different HMG department.
Service Set Identifier (SSID)	The SSID is a text string used to identify a wireless network. SSIDs are usually broadcast from APs.
Unmanaged component	An unmanaged component is one where the enterprise has very little confidence about its integrity, configuration and maintenance because they do not control the component. The lack of confidence in these areas increases the risk of compromise to the networks to which it connects.

15. Glossary

AP	Access Point
AS	Authentication Server
CCMP	Counter Mode with Cipher Block Chaining (CBC) Message Authentication Code (MAC) Protocol
DOS	Denial of Service
DA	Design Authority (DA)
Authority	The Authority refers to the Department for Work and Pensions (DWP)
GMK	Group Master Key
IEEE	Institute of Electrical and Electronics Engineers
PMK	Pairwise Master Key
PSK	Pre-shared Key
SUPPLIER	Is inclusive of Contractor, their employees or any sub-contractors used
TKIP	Temporary Key Integrity Protocol
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WIDPS	Wireless Intruder Detection and Prevention System
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WWAN	Wireless Wide Area Network