Security Standard – Wireless Network (SS-019)

Chief Security Office

Date: 24/04/2025

This Wireless Network Security Standard is part of a suite of standards, designed to promote consistency across the Department for Work and Pensions (DWP), and supplier base with regards to the implementation and management of security controls. For the purposes of this standard, the term DWP and Department are used interchangeably.

Technical security standards form part of the DWP Digital Blueprint which is a living body of security principles, architectural patterns, code of practice, practices and radars, that aim to support Product Delivery Units (PDUs) and suppliers in delivering the DWP and HMG Digital Strategy. Security standards and policies considered appropriate for public viewing are published here:

Government Publications Security Policies and Standards

Technical security standards cross-refer to each other where needed, so can be confidently used together. They contain both mandatory and advisory elements, described in consistent language (see table below).

(Important note for screen reader users.) Paragraphs that contain a **'must'** statement, and therefore denote a mandatory requirement, will contain the following statement after the heading:

(Important) this paragraph contains 'must' activities.

Table 1 – Terms

Term	Intention
must	denotes a requirement: a mandatory element.
should	should denotes a recommendation: an advisory element.
may	denotes approval.
might	denotes a possibility.
can	denotes both capability and possibility.
is/are	is/are denotes a description.

1. Contents

2. Revision history

Version	Author	Description	Date
1.0		First published version	04/07/2017
2.0		Full update in line with current best practices and standards; • Updated Intro, purpose, audience, scope; added reference to CIS security controls • Added NIST CSF references 11.1.4 New requirement about maintaining documentation 11.1.5 New requirement about hardware disposal 11.2.1 WPA requirements clarified 11.2.2 Added reference to SS-007, clarified position regarding HMAC and SHA-1 11.2.3 Added logging requirement 11.2.5 Added distinction between Authority and non-Authority devices 11.2.6 Added exclusions for SNMP protocols, clarified position on SNMPv3	27/02/2023

		11.2.7 Added requirements for https traffic and application awareness 11.2.10 Removed reference to pre-shared keys, added reference to SS-007 11.2.14 Added reference to automated auditing 11.4.9 Added requirement for WLAN authentication resilience 11.5.2 Detection of rogue APs 11.5.3 Disable adhoc mode 11.6.4 Added reference to AUP 11.7.1 Must require authentication 11.8.2 Replaced access points with Wi-Fi service 11.8.3 Guest/partner bandwidth is limited; testing changed to traffic monitoring 11.8.5 Automated auditing; added ref to Protective Monitoring 11.9.1 Added reference to SS-001 pt.2 11.10.1 Added reference to SS-001 pt.2 11.11.1 Changed reference to Security Incident Mgmt. Policy	

2.1		All NIST references reviewed and updated to reflect NIST 2.0 All security measures reviewed in line with risk and threat assessments Approval history - Review period changed to up to 2 years 11.1.1 Must changed to a should 11.1.2 Suppliers and third parties 11.1.4 Ref added to Network Security Design Standard 11.2.1 WPA3 11.2.3 & 11.2.4 Except guest devices; Ref added to PKI standard 11.2.6 Unneeded protocols, Wi-Fi gateways/controllers 11.2.7 Duplicated statements removed; Refs added to Protective Monitoring, Network Security Design and Malware standards 11.2.8 Private network operated by the Authority; Refs added to Security Boundaries and Network Security Design standards 11.2.9 SNMP not permitted via wireless-facing interfaces 11.2.10 Must; IoT devices and pre-shared keys 11.2.11 Ref added to PKI standard and X.509 Policy	24/04/2025

		11.2.13 & 11.2.14 Must changed to a should 11.2.15 Other compensating controls; Ref added to Security Testing standard 11.3.3 Authority private network 11.3.6 Mgmt interface access disabled from Wi-Fi or external networks 11.3.8 & 11.3.9 At installation 11.3.10 Patching Access Points 11.4.1 Windows and Linux OSs; Gold builds and CIS hardening 11.4.3 Must 11.4.5 TLS; ref added to DWP Cryptographic Algorithms 11.4.10 Authority certificate authority 11.5 Private Network operated by the Authority 11.5.2 Ref added to Glossary 11.6 Guest definition added 11.6.1 private network operated by the Authority 11.6.2 ‘network’ removed 11.6.7 Logged and ingested by SIEM; Added ref to Desktop OS standard 11.7.1 Partner Users and 3rd parties in line with Acceptable Use and Physical Security Policies.	

		11.8.2 Refs to VPNs and firewalls removed as these are described in other standards 11.8.3 Must 11.8.4 Must; jamming bullet removed; non-managed endpoints 11.8.6 Log ingestion 11.9.1. Initial provisioning and maintenance; 'and' 11.9.2 Ref added to Access & Authentication standard 11.9.3 Privileged Users; Ref added to Privileged User Access standard 11.10.3 Encrypted communications; ref added to DWP Cryptographic Algorithms 11.10.4 ref added to DWP Cryptographic Algorithms 11.10.5 Management interfaces; restricted subnets 11.11.1 Must; Internal References – Physical Security Policy; X.509 certificate policy; Desktop OS policy Glossary - IoT devices; Rogue APs; SIEM	

3. Approval history

Version	Name	Role	Date
1.0		Chief Security Officer	04/07/2017
2.0		Chief Security Officer	27/02/2023
2.1		Chief Security Officer	24/04/2025

This document is continually reviewed to ensure it is updated in line with risk, business requirements, and technology changes, and will be updated at least every 2 years - the current published version remains valid until superseded.

4. Compliance

Compliance with this standard will be verified through various methods, including but not limited to;

- controls tests performed by 1st line teams and by 2nd line activities (e.g. security testing teams)
- security assurance activities to ensure that Architectural Design and delivery are appropriate and aligned to applicable Authority Security Standards. [See Security Assurance Strategy – Ref. D].
- independent external audit

Results of these will be fed back to the appropriate Authority Risk and System Owners.

5. Exceptions Process

(Important) this paragraph contains ‘must’ activities.

In this document the term **“must”** is used in bold letters to indicate a mandatory security measure. Any exceptions to the application of this standard, or where specific security measures cannot be adhered to, **must** be presented to the Authority. This **must** be carried out prior to deployment and managed through the design caveats or exception process.

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

Exceptions to the standard **must** be maintained on a risk register for accountability, traceability, and security governance reporting to senior management.

6. Audience

This document is intended for, but not necessarily limited to, technical architects, engineers, developers, security teams, project teams, including suppliers engaged in the design, development, implementation and operation of systems, services and applications for the purposes of delivering applications and services that handle Authority data.

7. Accessibility statement

(Important) this paragraph contains ‘must’ activities.

Users of this standard **must** consider accessibility design requirements as appropriate. Further information on accessibility standards can be found in Appendix F.

8. Introduction

(Important) this paragraph contains ‘must’ activities.

This Wireless Network Security Standard defines the minimum technical security measures that **must** be implemented to secure IEEE 802.11 wireless networks for use within the Authority.

As this standard only provides minimum measures, they **should** be exceeded as appropriate depending on the threats and risks that need to be addressed, the sensitivity of the data, and in keeping with latest security enhancements.

The security measures are derived from industry best practice i.e. guidance published by NIST, CIS and OWASP (see Appendix C for full list of external references) and support the implementation of appropriate security controls as selected by the Authority or our third party providers, such as the CIS Critical Security Controls set. [see External References]

Every effort has been made to ensure the security measures are vendor and technology agnostic as far as possible; this is to ensure greater applicability of the standard regardless of the technologies used. The security measures **may** be implemented in different ways, depending on the technology choices and business requirements in question.

The aim of this standard is to:

- ensure security controls that are applicable to wireless networking are implemented consistently across the Authority and by third party providers where applicable.
- mitigate risks from common threats and vulnerabilities associated with wireless networking, to an acceptable level for operation.
- support the achievement of security outcomes described in Appendix A.

Technical security standards ultimately support the achievement of security outcomes sought by the Authority. They set the expectations for what needs to be done to achieve them and why, and provide an objective, measurable statement of the Authority's existing security posture in a number of important areas. The outcomes are based on the official NIST sub-categories where possible to ensure close alignment with the NIST Cyber Security Framework (CSF). Those relevant to the subject of each standard can be found in Appendix A of every technical security standard.

9. Purpose

The purpose of this standard is to ensure that Authority systems and services are designed, configured, deployed, and managed consistently to protect against typical threats at the OFFICIAL tier.

This standard also serves to provide a baseline in which assurance and compliance activities can be carried out, so that the Authority can be assured that security obligations are being met or exceeded.

10. Scope

(Important) this paragraph contains ‘must’ activities.

This standard applies to all IEEE 802.11 wireless network deployments that are provisioned within the Authority and supplier base (contracted third party providers), for the purposes of delivering applications and services that handle Authority data. It does not cover wireless network deployments for remote working e.g. for staff working from home. The requirements will be applied to new and existing installations.

Any queries regarding the security measures laid out in this standard **should** be sent to the Authority.

11. Minimum Technical Security Measures

(Important) this paragraph contains ‘must’ activities.

The following section defines the minimum security measures that **must** be implemented to achieve the security outcomes described in Appendix A. For ease of reference, the official NIST sub-category ID is provided against each security measure e.g. PR.PT-3, to indicate which outcome(s) it contributes towards. Refer to Appendix A for full description of outcomes.

11.1. Policy and Procedures

(Important) this table contains ‘must’ activities.

Reference	Minimum Technical Security Measures	NIST ID
11.1.1	A wireless network usage policy **should** 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 authorised to use WLAN technology and for what purposes • user responsibilities for the hardware, software and data in relation to the network and its security.	PR.AA-05 PR.AT-02
11.1.2	The Authority (including suppliers / third parties contracted to provide network services to the Authority) **must** enforce the wireless security policies through the appropriate security controls.	PR.AA-05 PR.IR-01

11.1.3	There **must** be appropriate knowledge and training in the introduction of new wireless network systems and updated security practices, controls, procedures, and architectures.	PR.AT-01 PR.AT-02
11.1.4	Wireless network infrastructure documentation **must** be kept up-to-date, and diagrams describing current state are updated, in line with SS-018 Network Security Design Standard [Ref. C].	ID.AM-03
11.1.5	All WLAN components **must** be disposed of according to SS-036 - Secure Sanitisation and Destruction Security Standard [Ref. L] – all configurations **must** be removed before disposal.	ID.AM-08

11.2. Wireless Network General Requirements

(Important) this table contains ‘must’ activities.

Reference	Minimum Technical Security Measures	NIST ID
11.2.1	All products (e.g. access points, servers, equipment & software) **must** support WPA2 or successor standards (e.g. WPA3). They **must** have been assured/validated prior to purchase, certified WPA-Enterprise, and use certified cryptographic modules as stated in SS-007 Use of Cryptography Security Standard [Ref. B].	PR.DS-02

11.2.2	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, in line with SS-007 Use of Cryptography Security Standard [Ref. B]. Although SHA-1 has been deprecated, it is still valid for use with HMAC, but users **must** consider that this minimum requirement may have changed	PR.DS-02
11.2.3	All endpoint devices (except 'Guest' devices, which can only be logged) that attempt to wirelessly connect to an Authority network **must** be authenticated and logged. If the authentication method uses digital certificates, SS-002 PKI & Key Management security standard [Ref. G] **must** be followed.	PR.AA-03
11.2.4	The authentication method chosen for Authority wireless networks **must** be assessed as suitable for deployment by the Authority. If the authentication method uses digital certificates, SS-002 PKI & Key Management security standard [Ref. G] **must** be followed.	PR.AA-03
11.2.5	For Authority devices, all network components **must** be configured to reduce the risk of being compromised as per SS-018 Network Security Design Standard [Ref. C]. There **must** be standardised security configurations for common WLAN components, such as client devices and Access Points (APs). For non- Authority devices, this approach is strongly recommended.	PR.IR-01

11.2.6	Unneeded network connections, network services, protocols and ports on managed endpoints, access points, Wi-Fi gateways / controllers and authentication servers **must** be disabled to reduce attack surface.	PR.IR-01
11.2.7	There **must** be security functions on the external gateway to protect the Wi-Fi service and supplement the controls on the end user devices. See SS-018 Network Security Design security standard [Ref. C], SS-015 Malware Protection security standard [Ref. R] and SS-012 Protective Monitoring Standard [Ref. A] for further information.	PR.IR-01
11.2.8	To ensure the separation and protection of WLANS, there **must** be a robust boundary (with network security enforcing components) between each WLAN and any private network operated by the Authority / the internet. See SS-006 Security Boundaries [Ref. D] and SS-018 Network Security Design [Ref. C] standards for further information.	PR.IR-01
11.2.9	Although SNMPv3 contains additional security capabilities, the risk of compromise still exists, thus SNMPv1, SNMPv2 & SNMPv3 protocols **must** not be permitted on the wireless-facing interfaces.	PR.IR-01

11.2.10	The WLAN infrastructure **must** be based on IEEE 802.1X/EAP authentication without the use of pre-shared keys, however 'Internet of Things' (IoT) devices using device-specific pre-shared keys are permitted. Also, the WLAN **must** use CCMP leveraging a FIPS-validated AES encryption module, see SS-007 Use of Cryptography Security Standard [Ref. B].	PR.DS-02 PR.IR-01
11.2.11	Any certificates on the endpoints and the servers used for wireless authentication **must** be periodically updated in accordance with the DWP X.509 Certificate Policy [Ref. U] and SS-002 PKI & Key Management security standard [Ref. G].	PR.DS-02 PR.IR-01
11.2.12	Access Points, Authentication Servers other wireless infrastructure components **must** be subject to the requirements in SS-033 Security Patching Security Standard [Ref. E].	PR.PS-02 PR.PS-03 PR.IR-01
11.2.13	Risk assessment **should** 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.	ID.RA-05
11.2.14	There **should** 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 or with an appropriate Authority security configuration. Automated auditing tools should be considered.	PR.PS-01

11.2.15	There **must** be comprehensive WLAN security assessments (e.g. IT Health Check) at regular intervals, preferably at least annually. Any detected vulnerabilities **must** be fixed by patching applications, OS and devices or by using secure configurations, hardening devices, or other compensating controls. See SS-027 Security Testing Standard [Ref. Q] for further information.	ID.RA-01 PR.PS-01 PR.PS-02 PR.PS-03 PR.IR-01

11.3. Access Points (Aps)

(Important) this table contains 'must' activities.

Reference	Minimum Technical Security Measures	NIST ID
11.3.1	WEP and TKIP **must** be disabled in the configuration of each AP.	PR.IR-01
11.3.2	The Service Set Identifier (SSID) of the Access Point (AP) **must** be changed from its default.	PR.IR-01
11.3.3	Access points (APs) **must** not be connected directly to any private network operated by the Authority as this could provide an unprotected route into the network. The wireless infrastructure **must** be separate from any private network operated by the Authority.	PR.IR-01
11.3.4	Access Points **must** terminate associations after a configurable time period (as assessed suitable by risk assessment).	PR.IR-01
11.3.5	A Group Master Key (GMK), where applicable, **must** be configured on the AP with a maximum lifetime (not to exceed 24 hours).	PR.IR-01

11.3.6	The management interface **must** be disabled from being accessible from the Wi-Fi or external networks.	PR.IR-01
11.3.7	The standard security configuration **must** be re-applied to an AP whenever its reset function is used.	PR.IR-01
11.3.8	There **must** be a site survey at installation 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.	PR.AA-06
11.3.9	Access Points (APs) **must** be physically inaccessible to unauthorised users as far as possible, and **must** be properly installed e.g. above desk height, not on the floor etc.	PR.AA-06
11.3.10	Access Point firmware **must** be either automatically updated using cryptographically signed vendor update mechanisms or manually updated in accordance with SS-033 Security Patching Security Standard [Ref. E].	PR.PS-02

11.4. Authentication Servers

(Important) this table contains ‘must’ activities.

Reference	Minimum Technical Security Measures	NIST ID
11.4.1	The security of any authentication server **must** be established in accordance with SS-008 Server Operating System Security Standard [Ref F]. Where Authentication Servers are installed on top of Authority -maintained Windows or Linux operating system instances, they **must** adopt Gold Images and be conformant to Authority CIS Hardening Benchmarks.	PR.AA-03 PR.AA-06 PR.IR-01

11.4.2	Managed endpoints **must** be configured to specify valid Authentication Servers (ASs) by name.	PR.AA-03 PR.IR-01
11.4.3	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 **must** also be configured to accept certificates only from the CA that signed the server certificates (see SS-002 PKI and Key Management Security Standard [Ref. G] for further requirements for certificates).	PR.AA-03 PR.IR-01
11.4.4	A Public Master Key (PMK), where applicable, **must** be configured on the Authentication Server with a maximum lifetime, preferably to not exceed eight hours.	PR.AA-03 PR.IR-01
11.4.5	Any communications between each Access Point (AP) and its corresponding Authentication Servers (AS) **must** be protected by TLS in line with the DWP Approved Cryptographic Algorithms document [Ref. S].	PR.DS-02
11.4.6	The cryptographic software on the authentication server **must** be deployed in accordance with SS-007 Use of Cryptography Security Standard [Ref. B].	PR.DS-02
11.4.7	The Authentication Server **must** be configured to use authorised methods only, as assessed suitable for deployment by the Authority.	PR.AA-03 PR.IR-01
11.4.8	Authentication Servers **must** only grant authorisations for a configurable time period (as assessed suitable by risk assessment).	PR.AA-03 PR.IR-01

11.4.9	WLAN authentication mechanisms **must** be resilient / fault tolerant to ensure continuity of service in case of failures.	PR.AA-03 PR.IR-01
11.4.10	All Authentication Servers **must** be enrolled with the Authority's PKI Chain of Trust through installation of an Authority PKI Certificate Authority Certificate.	PR.DS-02 PR.IR-01

11.5. Private Network operated by the Authority

(Important) this table contains 'must' activities.

Reference	Minimum Technical Security Measures	NIST ID
11.5.1	Access to enterprise resources from a mobile wireless device **must** be in line with SS-016 Remote Access Security Standard [Ref. H].	PR.AA-01 PR.AA-02 PR.AA-03
11.5.2	Detection mechanisms **must** be in place to detect and report on rogue APs (see Glossary).	DE.CM-01
11.5.3	All devices connected to the network **must** be configured with ad hoc mode disabled.	PR.IR-01

11.6. Guest Wi-Fi

(Important) this table contains ‘must’ activities.

Guest users and devices are defined as those that are not Authority users or corporate devices, but are external users and devices that are authorised to use Authority WIFi.

Reference	Minimum Technical Security Measures	NIST ID
11.6.1	Guest users **must** not have access to any private network operated by the Authority or the Authority intranet via the wireless network.	PR.AA-05 PR.IR-01
11.6.2	There **must** be physical or logical segregation between all guest traffic and corporate traffic.	PR.IR-01
11.6.3	Guest users **must** authenticate with the guest Wi-Fi before being permitted access to Internet services.	PR.AA-01 PR.AA-02 PR.AA-03
11.6.4	There **must** be technical controls in place to control what can be accessed, in line with the DWP Acceptable Use Policy [Ref. M].	PR.AA-05
11.6.5	Guest user sessions **must** have a timeout period configured (as assessed suitable by risk management).	PR.IR-01
11.6.6	Guest credentials **must** be unique and attributable to each guest user.	PR.AA-02
11.6.7	Internet activity for guest devices **must** be logged and ingested by the Authority SIEM solution and attributable to authenticated users such that an investigation can be successfully completed should the internet feed be used for malicious purposes. Security requirements for corporate devices can be found in SS-010 Desktop Operating System Security Standard [Ref. V].	DE.CM-01 DE.CM-03

11.6.8	In the case of a web based authentication for the guest Wi-Fi, then it **must** be configured and tested to ensure compliance with good web application design and implementation (in accordance with SS-029 Securely Serving Web Content Security Standard [Ref. I]).	PR.AA-03
11.6.9	Guest users **must** be made aware of terms and conditions (DWP Acceptable Use Policy [Ref. M]) which they **must** accept before accessing the Wi-Fi, including but not limited to: • no level of confidentiality is offered to traffic passing over the wireless infrastructure. • all usage and attempts to use the Wi-Fi are monitored and this may be used for an investigation to any misuse or abuse of the system	GV.OC-03 PR.AT-01 PR.AT-02

11.7. Partner Users

Reference	Minimum Technical Security Measures	NIST ID
11.7.1	The Authority will permit partner users (including contracted third parties) to access their organisation's VPN gateway where it is compatible with the Wi-Fi and Internet services that the Authority provides, and in line with Authority security policies, in particular the DWP Acceptable Use Policy [Ref M] and the DWP Physical Security Policy [Ref T].	PR.AA-03

11.8. Auditing and Monitoring

(Important) this table contains ‘must’ activities.

Reference	Minimum Technical Security Measures	NIST ID
11.8.1	Audit and monitoring **must** be done in compliance with SS-012 Protective Monitoring Security Standard [Ref. A].	PR.IR-01 PR.PS-04
11.8.2	Audit and monitoring information **must** be taken from the components within the architecture. Example events that **must** be recorded include: • Centralised logging on the Wi-Fi service **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.	PR.IR-01 PR.PS-04 DE.AE-03

11.8.3	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 • An Acceptable Usage Policy (AUP) for guest access **must** be developed that defines acceptable use of the wireless network. Guest activity **must** be monitored to ensure compliance with this AUP. • Changes to the configuration of a captive portal/Guest Wi-Fi **must** be logged together with the user carrying out the change. Unauthorised changes **must** be investigated • Traffic monitoring **must** be undertaken, with appropriate thresholds and alerting, to ensure that logged traffic flows can be attributed to individual user credentials in case malicious use needs to be investigated. • Guest/partner bandwidth may be throttled if necessary.	PR.IR-01 PR.PS-04 DE.AE-03

11.8.4	There **must** be both attack monitoring and vulnerability monitoring to support WLAN security. The monitoring solutions for the wireless network **must** provide the following detection capabilities: <u>ATTACKS</u> • Unauthorised WLAN devices, including rogue APs and unauthorised 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 denials 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 <u>VULNERABILITIES</u> • WLAN devices (excluding non-managed endpoints) that are misconfigured or using weak WLAN protocols and protocol implementations.	PR.IR-01 PR.PS-04 DE.AE-03

11.8.5	There **must** be wireless security audit processes and procedures (which can be automated) that identify the types of security relevant events that should be captured and determine how audit records will be securely stored for subsequent analysis, in line with SS-012 Protective Monitoring Security Standard [Ref. A].	PR.IR-01 PR.PS-04 DE.AE-03
11.8.6	Logs **must** be ingested into the Authority's SIEM solution for analysis.	DE.AE-02

11.9. Access Control

(Important) this table contains 'must' activities.

Reference	Minimum Technical Security Measures	NIST ID
11.9.1	Access points **must** never be managed individually while deployed within the live network apart from during initial provisioning or maintenance, but via centralised management facilities (to enable single admin account access), and **must** have strong authentication enabled in line with SS-001 pt.2 Privileged User Access Security Standard [Ref. N], and unique administrative passwords (changed from default) in accordance with DWP User Access Control Policy [Ref. J].	PR.AA-03
11.9.2	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, in line with SS-001 pt.1 Access and Authentication Security Standard [Ref. K].	PR.AA-03 PR.AA-05

11.9.3	Administrative or other privileged users **must** only be granted access in line with SS-001 pt.2 Privileged User Access Security Standard [Ref. N].	PR.AA-05

11.10. Administration

(Important) this table contains 'must' activities.

Reference	Minimum Technical Security Measures	NIST ID
11.10.1	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, appropriately trained and cleared administrators, in line with SS-001 pt.2 Privileged User Access Security Standard [Ref. N].	PR.AA-05 PR.AT-02
11.10.2	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 [Ref. B]).	PR.AA-05 PR.DS-02
11.10.3	Network management information between APs/ASs and network management servers or consoles **must** be secured with encrypted communications e.g. TLS in line with the DWP Approved Cryptographic Algorithms document [Ref. S].	PR.DS-02
11.10.4	Access points (APs) **must** support authentication and data encryption for administrative sessions (e.g. SSL/TLS support for web-based administration and secure shell (SSH) for command-line administration) in line with the DWP Approved Cryptographic Algorithms document [Ref. S].	PR.AA-03 PR.DS-02

11.10.5	Access to management interfaces from wireless networks **must** be disabled. Devices **must** restrict the subnets that can send or receive management traffic.	PR.AA-03 PR.DS-02

11.11. Incident Management

(Important) this table contains ‘must’ activities.

Reference	Minimum Technical Security Measures	NIST ID
11.11.1	Any security incidents relating to Authority wireless networks **must** be managed in accordance with SS-014 Security Incident Management Standard [Ref. O].	ID.IM-04 DE.AE-08

12. Appendices

Appendix A - Security Outcomes

The minimum security measures defined in this standard contribute to the achievement of security outcomes described in the table below. For consistency, the official NIST Sub-category IDs have been carried through to the standards.

Table 2 – List of Security Outcomes Mapping

Ref	Security Outcome (sub-category)	Related security measures
GV.OC-03	Legal, regulatory, and contractual requirements regarding cybersecurity - including privacy and civil liberties obligations - are understood and managed	11.6.9
ID.AM-03	Representations of the organisation's authorised network communication and internal and external network data flows are maintained	11.1.4
ID.AM-08	Systems, hardware, software, services, and data are managed throughout their life cycles	11.1.5
ID.RA-01	Vulnerabilities in assets are identified, validated, and recorded	11.2.15
ID.RA-05	Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritisation	11.2.13
ID.IM-04	Incident response plans and other cybersecurity plans that affect operations	11.11.1

	are established, communicated, maintained, and improved	
PR.AA-01	Identities and credentials for authorised users, services, and hardware are managed by the organisation	11.5.1, 11.6.3
PR.AA-02	Identities are proofed and bound to credentials based on the context of interactions	11.5.1, 11.6.3, 11.6.6
PR.AA-03	Users, services, and hardware are authenticated	11.2.3, 11.2.4, 11.4.1, 11.4.2, 11.4.3, 11.4.4, 11.4.7, 11.4.8, 11.4.9, 11.5.1, 11.6.3, 11.6.8, 11.7.1, 11.9.1, 11.9.2, 11.10.4
PR.AA-05	Access permissions, entitlements, and authorisations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	11.1.1, 11.1.2, 11.6.1, 11.6.4, 11.9.3, 11.10.1, 11.10.2
PR.AA-06	Physical access to assets is managed, monitored, and enforced commensurate with risk	11.3.8, 11.3.9, 11.4.1
PR.AT-01	Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind	11.1.3, 11.6.9
PR.AT-02	Individuals in specialised roles are provided with awareness and training so that they possess the knowledge and skills to perform	11.1.1, 11.1.3, 11.6.9, 11.10.1

	relevant tasks with cybersecurity risks in mind	
PR.DS-02	The confidentiality, integrity, and availability of data-in-transit are protected	11.2.1, 11.2.2, 11.2.10, 11.2.11, 11.4.5, 11.4.6, 11.4.10, 11.10.2, 11.10.3, 11.10.4
PR.IR-01	Networks and environments are protected from unauthorised logical access and usage	11.1.2, 11.2.5, 11.2.6, 11.2.7, 11.2.8, 11.2.9, 11.2.10, 11.2.11, 11.2.12, 11.2.15, 11.3.1, 11.3.2, 11.3.3, 11.3.4, 11.3.5, 11.3.6, 11.3.7, 11.4.1, 11.4.2, 11.4.3, 11.4.4, 11.4.7, 11.4.8, 11.4.9, 11.4.10, 11.5.3, 11.6.1, 11.6.2, 11.6.5, 11.8.1, 11.8.2, 11.8.3, 11.8.4, 11.8.5
PR.PS-01	Configuration management practices are established and applied	11.2.14, 11.2.15
PR.PS-02	Software is maintained, replaced, and removed commensurate with risk	11.2.12, 11.2.15, 11.3.10
PR.PS-03	Hardware is maintained, replaced, and removed commensurate with risk	11.2.12, 11.2.15
PR.PS-04	Log records are generated and made available for continuous monitoring	11.8.1, 11.8.2, 11.8.3, 11.8.4, 11.8.5

DE.AE-02	Potentially adverse events are analysed to better understand associated activities	11.8.6
DE.AE-03	Information is correlated from multiple sources	11.8.2, 11.8.3, 11.8.4, 11.8.5
DE.AE-08	Incidents are declared when adverse events meet the defined incident criteria	11.11.1
DE.CM-01	Networks and network services are monitored to find potentially adverse events	11.5.2, 11.6.7
DE.CM-03	Personnel activity and technology usage are monitored to find potentially adverse events	11.6.7

Appendix B - Internal references

Below, is a list of internal documents that **should** read in conjunction with this standard.

Table 3 – Internal References

Ref	Document	Publicly Available*
A	SS-012 Protective Monitoring Standard	Yes
B	SS-007 Use of Cryptography Standard	Yes
C	SS-018 Network Security Design Standard	Yes
D	SS-006 Security Boundaries Standard	Yes
E	SS-033 Security Patching Security Standard	Yes
F	SS-008 Server Operating System Standard	Yes
G	SS-002 PKI and Key Management Security Standard	Yes
H	SS-016 Remote Access Standard	Yes
I	SS-029 Securely Serving Web Content Security Standard	Yes
J	DWP User Access Control Policy	Yes
K	SS-001 pt.1 Access and Authentication Security Standard	Yes
L	SS-036 - Secure Sanitisation and Destruction Security Standard	Yes
M	DWP Acceptable Use Policy	Yes
N	SS-001 pt.2 Privileged User Access Security Standard	Yes
O	SS-014 Security Incident Management Standard	Yes

P	DWP Security Assurance Strategy	No
Q	SS-027 Security Testing Standard	No
R	SS-015 Malware Protection Security Standard	Yes
S	DWP Approved Cryptographic Algorithms	No
T	DWP Physical Security Policy	Yes
U	DWP X.509 Certificate Policy	No
V	SS-010 Desktop Operating System Security Standard	Yes

*Request to access to non-publicly available documents **should** be made to the Authority.

Appendix C External references

The following publications and guidance were considered in the development of this standard and **should** be referred to for further guidance.

Table 4 – External References

External Documents List
CIS Critical Security Controls set
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

Appendix D Abbreviations

Table 5 – Abbreviations

Abbreviation	Definition
PDU	Product Delivery Unit
AP	Access Point
AS	Authentication Server
AUP	Acceptable Use Policy
CCMP	Counter Mode with Cipher Block Chaining (CBC) Message Authentication Code (MAC) Protocol
DOS	Denial of Service
DDA	Digital Design Authority
DWP	Department for Work and Pensions
GMK	Group Master Key
IEEE	Institute of Electrical and Electronics Engineers
PMK	Pairwise Master Key
PSK	Pre-shared Key

Abbreviation	Definition
SIEM	Security Incident Event Monitoring
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

Appendix E Definition of Terms

Table 6 – Glossary

Term	Definition
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 organisation'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
Internet of Things (IoT) devices	IoT devices are pieces of hardware, such as sensors, actuators, appliances, or machines, that are programmed for certain applications and can transmit data over the internet or other networks.
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.

Rogue AP	A rogue AP is an AP outside of the Authority's administrative control that is 1) physically connected to an Authority network or 2) that bridges or routes between an Authority Wi-Fi network and network not controlled by the Authority.
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.

Appendix F - Accessibility artefacts

A variety of accessibility guidance is available from the below URL, that includes:

Guidance and tools for digital accessibility

Understanding accessibility requirements for public sector bodies