Security Standard - Wireless Network (SS-019)

Chief Security Office

Date: 27/02/23

Department for Work & Pensions

This Wireless Network Security Standard is part of a suite of standards, designed to promote consistency across the Authority, 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 Authority 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 Authority and HMG Digital Strategy. Security standards and policies considered appropriate for public viewing are published here:

https://www.gov.uk/government/publications/dwp-procurement-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).

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 v8 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 DWP and non-DWP devices 11.2.6 Added exclusions for SNMP protocols, clarified position on SNMPv3 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	27/02/2023

3. Approval History

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

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

4. Compliance

Security assurance teams will verify compliance with this standard through various methods, including but not limited to, internal and external audits, and feed back to the appropriate Authority Risk and System Owner.

5. Exceptions Process

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.

7. Accessibility Statement

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

8. Introduction

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 v8 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) and are enabled by the implementation of controls from the CIS Critical Security Controls v8 controls set. [see External References]. 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 is intended to be used;

- When developing/procuring a new voice and/or video communication solution for the Authority.
- To assist in providing advice and guidance on secure voice and video communication;
- 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

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

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

Reference	Minimum Technical Security Measures	NIST ID
11.1.1	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 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.AC-1
11.1.2	The Authority **must** enforce the wireless security policies through the appropriate security controls.	PR.AC-3
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-1 PR.AT-2
11.1.4	The Authority **must** ensure wireless network infrastructure documentation is kept up-to-date, and diagrams describing current state are updated.	ID.AM-1
11.1.5	All WLAN components must be disposed according to SS-036 - Secure Sanitisation and Destruction Security Standard [Ref. L] – all configurations must be removed before disposal.	PR.DS-3

11.2 Wireless Network General Requirements

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. 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-2
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 change within the next 12 months.	PR.DS-2
11.2.3	All endpoint devices that attempt to wirelessly connect to an Authority network **must** be authenticated and logged.	PR.AC-7
11.2.4	The authentication method chosen for Authority wireless networks **must** be assessed as suitable for deployment by the Authority.	PR.AC-7
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-DWP devices, this approach is strongly recommended.	PR.PT-4
11.2.6	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). Although SNMPv3 contains additional security capabilities, the risk of compromise still exists, thus SNMPv1, SNMPv2 & SNMPv3 protocols **must** be disabled.	PR.PT-4

11.2.7	There **must** be security functions on the external gateway to protect the wifi service and 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 • preventing the user from installing an untrusted root Certificate Authority's certificate • require the use of HTTPS for websites where the content requires additional protection • The security function must be application aware	PR.PT-4
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 the enterprise network/the internet.	PR.AC-5 PR.PT-4
11.2.9	Boundaries of the wireless network **must** in addition comply with SS-006 Security Boundaries Security Standard [Ref D].	PR.AC-5 PR.PT-4
11.2.10	The WLAN infrastructure **must** be based on IEEE 802.1X/EAP authentication without the use of pre-shared keys. Also, the WLAN should use CCMP leveraging a FIPS-validated AES encryption module, see SS-007 Use of Cryptography Security Standard [Ref. B].	PR.AC-5 PR.AC-7
11.2.11	Any certificates on the endpoints and the servers used for wireless authentication **must** be periodically updated in accordance with Authority's Certificate Policy.	PR.AC-5 PR.AC-7
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.PT-4

11.2.13	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.	ID.RA-1 ID.RA-5 ID.RA-6
11.2.14	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 or with an appropriate Authority standard security configuration. Automated auditing tools should be considered.	PR.PT-1 PR.PT-4
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 and hardening devices.	PR.PT-4

11.3 Access Points (APs)

Reference	Minimum Technical Security Measures	NIST ID
11.3.1	WEP and TKIP **must** be disabled in the configuration of each AP.	PR.PT-4
11.3.2	The Service Set Identifier (SSID) of the Access Point (AP) **must** be changed from its default.	PR.PT-4
11.3.3	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.	PR.AC-5 PR.PT-4
11.3.4	Access Points **must** terminate associations after a configurable time period (as assessed suitable by risk assessment).	PR.PT-4
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.PT-4
11.3.6	APs **must** have a logically or physically independent management support interface.	PR.AC-5 PR.PT-4
11.3.7	The standard security configuration **must** be re-applied to an AP whenever its reset function is used.	PR.PT-4

11.3.8	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.	PR.IP-5
11.3.9	Access Points (APs) **must** be physically inaccessible to unauthorised users.	PR.IP-5

11.4 Authentication Servers

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].	PR.PT-4
11.4.2	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 and Key Management Security Standard [Ref. G] for further requirements for certificates).	ID.AM-1 ID.AM-2
11.4.3	Managed endpoints **must** be configured to specify valid Authentication Servers (ASs) by name.	PR.AC-1 PR.AC-5
11.4.4	A Public Master Key (PMK), where applicable, **must** be configured on the Authentication Server with a maximum lifetime, preferably not to exceed eight hours.	PR.AC-1 PR.AC-5
11.4.5	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 [Ref. B]).	PR.DS-2
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-2
11.4.7	The Authentication Server **must** be configured to use authorised methods only, as assessed suitable for deployment by the Authority.	PR.AC-5 PR.AC-7

11.4.8	Authentication Servers **must** only grant authorisations for a configurable time period (as assessed suitable by risk assessment).	PR.AC-5 PR.AC-7
11.4.9	WLAN authentication mechanisms **must** be resilient / fault tolerant to ensure continuity of service in case of failures.	PR.AC-5 PR.AC-7

11.5 Enterprise Network

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.AC-3
11.5.2	Detection mechanisms **must** be in place to detect and report on rogue APs.	DE.AE-1 DE.AE-2
11.5.3	All devices connected to the network **must** be configured with ad hoc mode disabled.	PR.PT-3 PR.PT-4

11.6 Guest Wi-Fi

Reference	Minimum Technical Security Measures	NIST ID
11.6.1	Guest users **must** not have access to the enterprise network or the Authority intranet via the wireless network.	PR.AC-5 PR.PT-4
11.6.2	There **must** be physical or logical network segregation between all guest traffic and corporate traffic.	PR.AC-5 PR.PT-4
11.6.3	Guest users **must** authenticate with the guest Wi-Fi before being permitted access to Internet services.	PR.AC-4 PR.AC-6 PR.AC-7
11.6.4	There **must** be technical controls in place to control what can be accessed, in line with the Authority's Acceptable Use Policy [Ref. M].	PR.AC-4 PR.DS-1 PR.DS-2
11.6.5	Guest user sessions **must** have a timeout period configured (as assessed suitable by risk management).	ID.RA-1 PR.DS-5
11.6.6	Guest credentials **must** be unique and attributable to each guest user.	ID.AM-6 PR.AC-6

11.6.7	Internet activity **must** be attributable to authenticated users such that an investigation can be successfully completed should the internet feed be used for malicious purposes.	DE.CM-1 DE.CM-3
11.6.8	Network controls **must** protect the guest Wi-Fi from network bound attacks from the Internet	PR.AC-5 PR.PT-4
11.6.9	If it is 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.AC-3 PR.AC-5
11.6.10	Guest users **must** be made aware of terms and conditions (Authority 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	ID.GV-1 ID.GV-3

11.7 Partner Users

Reference	Minimum Technical Security Measures	NIST ID
11.7.1	Partner users **must** be able to directly access their organisation’s VPN gateway but **must** authenticate to the access layer (i.e. bypassing the captive portal).	PR.AC-6 PR.AC-7

11.8 Auditing and Monitoring

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.PT1
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. • 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.	PR.PT-1 DE.AE-3 DE.CM-1
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 • The Authority **must** have developed an Acceptable Usage Policy (AUP) for guest access that defines acceptable use of the wireless network. Guest activity must be monitored to ensure compliance with the 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 should be investigated • Traffic monitoring **must** be undertaken, with appropriate thresholds and alerting, to ensure that logged traffic flows can be attributed to individual	PR.PT-1 DE.AE-3 DE.CM-1

	user credentials in case malicious use needs to be investigated. Please note guest/partner bandwidth is throttled.	
11.8.4	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: 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 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 • 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.	PR.PT-1 DE.AE-1 DE.AE-2 DE.AE-3 DE.CM-1
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.PT-1 DE.AE-1 DE.AE-2 DE.AE-3

11.9 Access Control

Reference	Minimum Technical Security Measures	NIST ID
11.9.1	Access points **must** never be managed individually, but via centralised management facilities (to enable single admin account access), **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 the Authority User Access Control Policy [Ref. J].	PR.AC-4 PR.AC-7
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.	PR.AC-4
11.9.3	Access and Authentication **must** be in line with SS-001 pt.1 Access and Authentication Security Standard [Ref. K].	PR.AC-1 PR.AC-4 PR.AC-7

11.10 Administration

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 administrators, in line with SS-001 pt.2 Privileged User Access Security Standard [Ref. N]. They must be appropriately trained and cleared network administrators.	PR.AC-4 PR.AT-2
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.AC-1 PR.AC-4 PR.AC-5
11.10.3	Network management information between APs/ASs and network management servers or consoles **must** be transmitted over a dedicated management VLAN.	PR.DS-2
11.10.4	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).	PR.DS-2

11.10.5	All insecure and unused management protocols on the APs **must** be disabled, and configure remaining management protocols for least privilege.	PR.AC-4

11.11 Incident Management

Reference	Minimum Technical Security Measures	NIST ID
11.11.1	Any security incidents relating to Authority wireless networks should be managed in accordance with the Authority Security Incident Management Policy [Ref. O].	PR.IP-9 DE.AE-5

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 1 – List of Security Outcomes Mapping

NIST Ref	Security Outcome (sub-category)	Related Security measure
ID.AM-1	Physical devices and systems within the organization are inventoried	11.1.4, 11.4.2
ID.AM-2	Software platforms and applications within the organization are inventoried	11.4.2
ID.AM-6	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	11.6.6
ID.GV-1	Organizational cybersecurity policy is established and communicated	11.6.10
ID.GV-3	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	11.6.10
ID.RA-1	Asset vulnerabilities are identified and documented	11.2.13, 11.6.5
ID.RA-5	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	11.2.13
ID.RA-6	Risk responses are identified and prioritized	11.2.13
PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	11.1.1, 11.4.3, 11.4.4, 11.9.3, 11.10.2

PR.AC-3	Remote access is managed	11.1.2, 11.5.1, 11.6.9
PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	11.6.3, 11.6.4, 11.9.1, 11.9.2, 11.9.3, 11.10.1, 11.10.2, 11.10.5
PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)	11.2.8, 11.2.9, 11.2.10, 11.2.11, 11.3.3, 11.3.6, 11.4.3, 11.4.4, 11.4.7, 11.4.8, 11.4.9, 11.6.1, 11.6.2, 11.6.8, 11.6.9, 11.10.2
PR.AC-6	Identities are proofed and bound to credentials and asserted in interactions	11.6.3, 11.6.6, 11.7.1
PR.AC-7	Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	11.2.3, 11.2.4, 11.2.10, 11.2.11, 11.4.7, 11.4.8, 11.4.9, 11.6.3, 11.7.1, 11.9.1, 11.9.3
PR.AT-1	All users are informed and trained	11.1.3
PR.AT-2	Privileged users understand their roles and responsibilities	11.1.3, 11.10.1
PR.DS1	Data-at-rest is protected	11.6.4
PR.DS2	Data-in-transit is protected	11.2.1, 11.2.2, 11.4.5, 11.4.6, 11.5.4, 11.10.3, 11.10.4
PR.DS3	Assets are formally managed throughout removal, transfers, and disposition	11.1.5
PR.DS5	Protections against data leaks are implemented	11.6.5
PR.IP5	Policy and regulations regarding the physical operating environment for organizational assets are met	11.3.8, 11.3.9

PR.IP9	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	11.11.1
PR.PT1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	11.2.14, 11.8.1, 11.8.2, 11.8.3, 11.8.4, 11.8.5
PR.PT3	The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	11.5.3
PR.PT4	Communications and control networks are protected	11.2.5, 11.2.6, 11.2.7, 11.2.8, 11.2.9, 11.2.12, 11.2.14, 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, 11.5.3, 11.6.1, 11.6.2, 11.6.8
DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed	11.5.1, 11.8.4, 11.8.5
DE.AE-2	Detected events are analysed to understand attack targets and methods	11.5.1, 11.8.4, 11.8.5
DE.AE-3	Event data are collected and correlated from multiple sources and sensors	11.8.2, 11.8.3, 11.8.4, 11.8.5
DE.AE-5	Incident alert thresholds are established	11.11.1
DE.CM-1	The network is monitored to detect potential cybersecurity events	11.6.7, 11.8.2, 11.8.3, 11.8.4
DE.CM-3	The physical environment is monitored to detect potential cybersecurity events	11.6.7

Appendix B Internal References

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

Table 2 – 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	DWP Security Incident Management Policy	TBA

Requests to access 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 3 – External References

External Documents List
CIS Critical Security Controls v8 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 4 – 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 of Work and Pensions
GMK	Group Master Key
IEEE	Institute of Electrical and Electronics Engineers
PMK	Pairwise Master Key
PSK	Pre-shared Key
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 5 – 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 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 DWP. 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.

Appendix F Accessibility artefacts

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

https://www.gov.uk/guidance/guidance-and-tools-for-digital-accessibility

https://www.gov.uk/guidance/accessibility-requirements-for-public-sector-websites-and-apps