Security Standard – Access & Authentication SS-001 (part 1)

Chief Security Office

Date: 26/10/2023

Department for Work & Pensions

This Access and Authentication 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 Authority 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:

https://www.gov.uk/government/publications/dwp-procurement-security-policies-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	18/09/2017
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 • 11.1.3 role-based or attribute-based • 11.2.2 Single Sign On • 11.2.4 removed Microsoft as vendors no-longer specified; added ref to Tech Radars • 11.3.6 'two-man' changed to 'two-person' to avoid gendered language use; added four eyes principle • 11.3.8 roles, permissions, entitlements • 11.3.9 Change management processes • 11.3.12 Successful and unsuccessful; 'DWP Records Management Policy' changed to 'DWP Information Management Policy as this is the actual location of the information. • 11.4.1 Security Vetting Policy; 'Operational'; added ref to Priv User standard • 11.4.12 inserted reference to the principle of Least Privilege and outward reference to the Privileged Users Security Policy • 11.6.7 Non-human accounts • 11.7.1 Must utilise MFA • 11.7.3 Password changes • 11.7.5 Secondary accounts • 11.9.1 'contract' replaced by 'formal agreement' to allow for XOrg collaboration • 11.9.3 'DWP Business Owner' replaced by 'Identified Risk Owner' • 11.10.2 removed reference to "Government Digital Service (GDS) Good Practice Guides (GPG)" as these are out of date. Replaced by NCSC guidance and CDDO guidance. • 11.10.5 at least monthly	26/10/2023

Version	Author	Description	Date
		• 11.7.10 removed as it is out of date and contrary to NCSC best practice on changing passwords. Subsequent sub-sections 11.7.11 – 11.7.20 renumbered accordingly • 11.7.20 Password Managers • 11.8.4 Non-human accounts • 11.9.1 Contract • 11.9.3 Third party identities • 11.9.8 & 11.9.9 In line with contract • 11.9.9 Consider risk • 11.9.11 Security testing • 11.11 API Authentication requirements	

3. Approval History

Version	Name	Role	Date
1.0		Chief Security Officer	18/09/2017
2.0		Chief Security Officer	26/10/2023

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

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

- controls tests performed by first-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. C].
- independent external audit

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

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 Requirements

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 Access and Authentication Security Standard defines the minimum technical security measures that **must** be implemented 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 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 access and authentication are implemented consistently across the Authority and by third party providers where applicable.
- mitigate risks from common threats and vulnerabilities associated with access and authentication, to an acceptable level for operation.
- support the achievement of security outcomes described in Appendix A.
- Support the creation of digital identities [see External References – NIST 800-63 Digital Identity Guidelines].

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 new access and authentication solutions for the Authority
- To assist in providing advice and guidance on secure access and authentication;
- 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 access and authentication deployments within the Authority and supplier base (contracted third party providers), for the purposes of delivering applications and services that handle Authority data.

The standard applies to the following;

- Access and authentication solutions managed by the Authority or Third Party Supplier or other support function for internal Authority use.
- Any access and authentication solutions used to support Authority services and/or data by a third party provider.
- Non-human accounts, such as service accounts or automated accounts, unless where human dependent controls are referenced e.g. biometrics.
- Authority and supplier identities that are managed by the Authority i.e. not those identities managed by third parties.

This standard **does not** apply to customer identity.

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 General Security Control Requirements

Reference	Minimum Technical Security Measures	NIST ID
11.1.1	Controls **must** be implemented to restrict access to business applications, information systems, network services, and computing devices, and the information stored on and processed by them.	PR.AC-1 PR.AC-4
11.1.2	The Authority and its Suppliers **must** implement appropriate identification and authentication controls to manage the risk of unauthorised access, and to ensure the correct management of user accounts and enable auditing.	PR.AC-1 PR.AC-4 PR.AC-7

Reference	Minimum Technical Security Measures	NIST ID
11.1.3	All individual Authority information systems, applications, services and networks **must** be equipped with and maintain a System Access Control Policy which **must** be approved by the appropriate Information Asset Owners, who must enforce access control (e.g via role-based or attribute-based) requirements on the systems they are responsible for.	PR.AC-1
11.1.4	The System Access Control Policy **must** provide the information that those involved in designing, developing, operating and using the system, application or service will need, in order to ensure that: a) the system, application or service is developed with the appropriate security mechanisms in place; b) That procedures can be developed to support the operation of the system, application or service in accordance with the appropriate security policies and standards.	PR.AC-1 PR.AC-6
11.1.5	System Access Control Policies **must** be supported by documented procedures, which take account of: a) The Authority's Security Standards, information security classifications, agreements with application owners, requirements set by the owner of systems and legal, regulatory and contractual obligations; b) The need to enforce individual accountability, apply additional control for users with special access privileges, (See also SS-001 pt2 Privileged User Access Security Standard [Ref. A]), and provide segregation of duties.	PR.AC-1 PR.AC-6 PR.AT-2

11.2 Identity and Access Management Control Requirements

Reference	Minimum Technical Security Measures	NIST ID
11.2.1	Identity and access management arrangements **must** be incorporated into an Authority-wide solution, and applied to new business systems, applications or services when they are introduced into the Authority.	PR.AC-1 PR.AC-6
11.2.2	Identity and access management arrangements **must**: • include a method for validating user identities prior to enabling user accounts • keep the number of sign-ons required by users to a minimum, using single sign on capabilities for example.	PR.AC-1 PR.AC-6
11.2.3	Identity and access management arrangements **must** provide a consistent set of methods for: • identifying users using unique UserIDs • authenticating users using passwords, tokens (smartcards) or biometrics etc.) • identifying equipment (e.g., by using MAC-based authentication) • the user sign-on process • authorising user access privileges • administering user access privileges.	PR.AC-1 PR.AC-6 PR.AC-7 PR.AT-2
11.2.4	Identity and access management arrangements **must** be developed to improve the integrity of user information by: • making this information readily available for users to validate • allowing users to correct their own user information (e.g., by providing users with a self-service application) • maintaining a limited number of identity stores (i.e., the location where UserID and authentication information is stored, such as a Lightweight Directory Access Protocol (LDAP) directory service, or other access & authentication product, including cloud-native or system-native capabilities. • using an automated provisioning system (whereby user accounts are created for all target systems, following the creation of an initial entry for a user in a central IAM application) using a centralised change management system.	PR.AC-1 PR.AC-6 PR.AC-7

11.3 Registration Control Requirements

Reference	Minimum Technical Security Measures	NIST ID
11.3.1	Procedures to register and authorise access to an Authority information system, application or service **must** be defined and documented in the System Access Control Policy.	PR.AC-1
11.3.2	The access management functionality **must** provide authorised administrators with the ability to create, amend, delete and suspend User accounts.	PR.AC-1 PR.AC-4
11.3.3	Access management functionality **must** also provide the ability to define the access privileges for the User. See also SS-001 pt2 Privileged User Access Security Standard [Ref. A].	PR.AC-1 PR.AT-2
11.3.4	Access to an Authority information system, application or service **must** not be granted until the authorisation procedures have been completed.	PR.AC-1
11.3.5	Administrators will, under management direction, set up and maintain control of authorised User accounts and be able to view User account privileges and identifiers on request. Documented instructions **must** be provided for Administrators, which detail the procedures that they **must** follow.	PR.AC-1
11.3.6	Administrators **must** risk assess whether a two-person rule (or ‘four eyes principle’) should be applied for initial enrolment to an authentication system and other precautions applied in accordance with local procedures.	PR.AC-1 PR.AC-4
11.3.7	A formal record **must** be created, maintained, and be available for examination, of all Users registered to use an Authority information system, application or service.	PR.AC-1
11.3.8	Where the records are maintained within an Information system, application or service, facilities **must** be available to provide reports to management giving details of registered Users and their Access roles, permissions or entitlements.	PR.AC-1
11.3.9	Formal change management processes **must** be in place, to ensure that records are maintained and are available for examination of all User access privileges awarded, changed or revoked on an Authority information system, application or service. See also SS-001 pt2 Privileged User Access Security Standard [Ref. A].	PR.AC-1 PR.AC-4

Reference	Minimum Technical Security Measures	NIST ID
11.3.10	Records **must** be maintained of the service accounts and their privileges where: a) special accounts have to be created to allow applications to run; b) access to one system, application or service through the use of service accounts entitles access to additional system, application or service. See also SS-001 pt2 Privileged User Access Security Standard [Ref. A].	PR.AC-1 PR.AC-6 PR.AT-2
11.3.11	The records of these service accounts may be maintained automatically by the administration functions of the system, application or service or manually. Where the records are maintained within an Information system, application or service, facilities **must** be available to provide reports to management giving details of Users, including service Users, registered, their access privileges, (See also SS-001 pt2 Privileged User Access Security Standard [Ref. A]) and changes made.	PR.AC-1 PR.AT-2
11.3.12	All access requests (both successful and unsuccessful) **must** be retained by the service, for a period 18 months after access is withdrawn, in accordance with the Authority Information Management Policy [Ref. E].	PR.AC-1

11.4 Authorisation Control Requirements

Reference	Minimum Technical Security Measures	NIST ID
11.4.1	Access to Authority information systems, applications or services **must** not be authorised until all employment and Basic Personal Security Standard checks have been completed in line with the DWP Security Vetting Policy [Ref. G]. Where administrative access to Operational Infrastructure, Systems or Data is granted then SC clearance is required as a minimum, in line with SS-001 pt.2 Privileged User Access Security Standard [Ref. A].	PR.AC-1
11.4.2	Line managers **must** approve requests for access to the Authority network, information systems, applications or services, before access is granted.	PR.AC-1
11.4.3	The user’s line manager **must** ensure that the user is suitably trained to perform the duties associated with the access being requested.	PR.AT-1

Reference	Minimum Technical Security Measures	NIST ID
11.4.4	Users initial access rights **must** be limited to email, Internet browser and office productivity applications. Access requests to other business applications **must** be subject to separate access requests.	PR.AC-4
11.4.5	Users **must** complete the Authority's Security and Awareness training within two weeks of being granted access to the Authority Network.	PR.AT-1
11.4.6	The Authority's information system, application or services **must** provide facilities to manage Users' profiles and access privileges based on their role. See also SS-001 pt2 Privileged User Access Security Standard [Ref. A].	PR.AT-2
11.4.7	The User Profiles **must** provide the level and detail of information necessary to implement the System Access Control Policy for the system, application or service to ensure that the User will only be granted access to those functions for which approval has been authorised.	PR.AC-6 PR.AC-4
11.4.8	The following details **must** be recorded within User Profiles: a) primary/unique UserID; b) full name; c) other UserID (s) if needed to access local and/or remote resources; d) address(es); e) User status (new, suspended, terminated, re-certification required, on-leave, etc.); f) key dates (e.g. User account start, termination, last-changed, re-activation); g) group, job or other role/responsibility codes that grant indirect resource access authorisations; h) all authorised Access Rights; i) any encryption key data, protected encryption servers, credential holders, etc. (if used); j) method(s) of authentication (password, biometric or other credential types and authentication details).	PR.AC-6 PR.AC-7
11.4.9	The Authority's information systems, applications or services **must** provide facilities to control access to the system, application or service based on a User's privileges, as defined by their profile.	PR.AC-1 PR.AC-4
11.4.10	The system, application or service **must** not perform any actions on behalf of a User unless the User has been positively authenticated.	PR.AC-7
11.4.11	The system, application or service **must** provide the User with a password as one factor of authentication.	PR.AC-7

Reference	Minimum Technical Security Measures	NIST ID
11.4.12	The User access **must** be restricted to the minimum necessary to satisfy business needs according to their defined profile / role, according to the Principle of Least Privilege. See also Privileged Users Security Policy [Ref. D].	PR.AC-4 PR.AT-2

11.5 Sign-On Process Control Requirements

Reference	Minimum Technical Security Measures	NIST ID
11.5.1	There **must** be a sign-on process that users need to follow before they are provided with access to information systems, which **must** enable individual users to be identified (e.g., using unique UserIDs).	PR.AC-1
11.5.2	Sign-on mechanisms **must** be configured so that they: • validate sign-on information only when it has all been entered; • limit the duration of any one sign-on session; • are re-enabled automatically after interruption (i.e., the sign-on process is required again following a disconnection from the application).	PR.AC-1 PR.AC-6
11.5.3	Sign-on mechanisms **must** be configured to provide information so that they: • display no identifying details until after sign-on is completed successfully; • warn that only authorised users are permitted access; • record all successful and unsuccessful sign-on attempts; • advise users (on successful sign-on) of the date/time of their last successful sign-on and all unsuccessful sign-on attempts since their most recent successful sign-on.	PR.AC-1 PR.AC-6
11.5.4	Sign-on mechanisms **must** be configured to protect authentication details against unauthorised disclosure by using for example approved; • cryptographic mechanisms to conceal clear text passwords and resist brute force attacks • salting methods to ensure each password hash is unique to resist attacks using rainbow tables.	PR.AC-1 PR.AC-7
11.5.5	Sign-on mechanisms **must** be configured to delete authentication details when they are no longer required by the authenticating system, such as immediately following successful authentication.	PR.AC-1 PR.AC-7

Reference	Minimum Technical Security Measures	NIST ID
11.5.6	The approval of a sufficiently senior business manager **must** be obtained before any important features of the sign-on process are bypassed, disabled or changed.	PR.AC-1 PR.IP-3

11.6 Access Review Control Requirements

Reference	Minimum Technical Security Measures	NIST ID
11.6.1	Where an individual is leaving the Authority their account **must** be deactivated on the day after their employment or contract ends.	PR.AC-1
11.6.2	All deactivated accounts **must** be deleted within 12 months of the account being deactivated.	PR.AC-1
11.6.3	Quarterly reviews **must** be carried out of all Authority leavers, both permanent and contractors, to confirm accounts have been deactivated.	PR.AC-1
11.6.4	Quarterly reviews **must** be carried out of all Authority User accounts, looking for accounts that have been deactivated for more than 12 months. Any such accounts found **must** be deleted**.**	PR.AC-1
11.6.5	Where a user is absent from work for a period greater than six months (due to secondment, courses, maternity leave, long term sickness absence etc) the account **must** be deactivated.	PR.AC-1
11.6.6	Quarterly reviews **must** be carried out of all Authority User accounts looking for accounts that have been dormant for more than 100 days. Where such accounts are detected the relevant line manager **must** be contacted to confirm whether the account is still required, and action **must** be taken to either deactivate or delete the accounts.	PR.AC-1
11.6.7	Access rights for non-human accounts (such as service accounts or automated accounts) **must** be reviewed and re-certified at least every 12 months.	PR.AC-1

11.7 Authentication Control Requirements

Reference	Minimum Technical Security Measures	NIST ID
11.7.1	Access to Authority applications, systems, networks, services and computing devices **must** be restricted to authorised individuals by the use of access control mechanisms. Access control mechanisms typically involve the submission of two pieces of information to prove an identity: a unique identifier (e.g., UserID or a user's email address) and a corresponding authenticator (e.g., a password, digital certificate or fingerprint scan). Access control mechanisms are often classified in terms of the factors that are used to authenticate users, and are based upon something the user: – knows (e.g., a password) – has (e.g., physical token, smartcard or digital certificate) – is or does (e.g., biometrics such as fingerprint, iris pattern, hand geometry, voice characteristic or writing style). Multi factor authentication, (MFA), **must** be utilised as a proportionate counter measure to risk when determining authentication control requirements for internal user access to Authority applications, systems, network services, or computing devices.	PR.AC-1 PR.AC-7
11.7.2	All individual Authority information systems, applications, services and networks **must** be equipped with and maintain a System Access Control Policy which **must** include a Password Management Section, which defines the parameters for the selection and use of passwords or PINs, developed in accordance with NCSC Password Policy: Updating Your Approach November 2018 [See External References].	PR.AC-1 PR.AC-6
11.7.3	Where machine-generated passwords are available, they **must** be used as they eliminate those passwords that would be simple for an attacker to guess, they require little effort from the user to create, and, depending on the generation scheme, can produce passwords that are fairly easy to remember. These passwords **must** be changed on indication or suspicion of compromise (see External References – NCSC password policy).	PR.AC-1 PR.AC-6

Reference	Minimum Technical Security Measures	NIST ID
11.7.4	If user-generated passwords are used, the Password Management section of the System Access Control Policy **must** consider proportionate and appropriate values for password construction ensuring: ▪ structure and format – enforcing the requirement for complex character sets in passwords is NOT recommended. Instead, technical controls **must** be implemented defending against automated guessing attacks by either using account lockout, throttling, or protective monitoring - blacklisting the most common password choices; ▪ frequency of change - regular password changing harms rather than improves security, so placing this burden on users **must** be avoided. However, users **must** change their passwords on indication or suspicion of compromise (see External References – NCSC password policy); ▪ passwords **must** not be dictionary words or the same as the User ID. ▪ Users **must** be able to change their own password after re-entering their current password; ▪ authorised roles / functions **must** be able to initialise or change passwords for Users; ▪ New passwords **must** be entered twice to avoid keying errors;	PR.AC-1 PR.AC-6
11.7.5	New User accounts **must** have passwords set before the account is enabled. It may be necessary in some circumstances to create secondary user accounts; these **must** be associated and attributable to an individual, meet all the same requirements as primary accounts, and are governed and managed in the same way.	PR.AC-1 PR.AC-6
11.7.6	Default or temporary passwords **must** expire at first logon before access to system, application or service resources by a new user is allowed.	PR.AC-1 PR.AC-6
11.7.7	Passwords **must** not be stored, transmitted or otherwise expressed in a clear text e.g. human or machine readable format, by any process handling the password.	PR.AC-1 PR.AC-6
11.7.8	Passwords **must** be stored as a hash of the password value using an approved hashing algorithm with a salt added to the password before hashing (Refer to Authority Approved Cryptographic Algorithms [Ref. B])	PR.AC-1 PR.AC-6

Reference	Minimum Technical Security Measures	NIST ID
11.7.9	Files containing passwords **must** not be stored in the clear, and **must** be protected in line with SS-007 Use of Cryptography [Ref. H].	PR.AC-1
11.7.10	Systems and applications **must** enforce all password parameters.	PR.AC-1
11.7.11	The allocation of passwords **must** be controlled and the process documented in the system Access Control Policy.	PR.AC-1
11.7.12	Passwords **must** only be issued to users when their identity has been confirmed.	PR.AC-1 PR.AC-6
11.7.13	The confidentiality of passwords **must** be maintained when the passwords are being distributed.	PR.AC-1 PR.DS-2
11.7.14	The protection afforded to passwords during distribution **must** be at least commensurate with the classification of the information protected by the passwords.	PR.AC-1 PR.DS-2
11.7.15	If a password is being distributed electronically, it **must** be sent via a route accepted as ‘trusted’ or secure by the Authority or in an approved encrypted format.	PR.AC-1 PR.DS-2
11.7.16	If a password is being distributed by post, it **must** be sent to a pre-defined location for the User.	PR.AC-1 PR.DS-2
11.7.17	User ID information **must not** be included in any communication to a User alongside reference to a password.	PR.AC-1
11.7.18	If a password is being distributed by telephone, it **must** be to a known telephone number for the User, and the identity of the User **must** be authenticated before the password is divulged.	PR.AC-1 PR.DS-2
11.7.19	Where the default configuration of hardware or software includes accounts with default passwords, these passwords **must** be changed before an Authority information system, application or service is brought in to use.	PR.AC-1
11.7.20	Use of an Authority approved password manager is highly recommended, in line with NCSC Password Policy: Updating Your Approach November 2018 [See External References].	PR.AC-1

11.8 Token Management

Reference	Minimum Technical Security Measures	NIST ID
11.8.1	Token Management Procedures **must** ensure that Physical Security Tokens are properly managed at each stage of their lifecycle and **must** cover irregularities such as loss, theft or damage.	PR.AC-1

11.8.2	Token Management Procedures **must** cover:
	a) Ordering;
	b) Storage;
	c) Distribution;
	d) Allocation;
	e) Recovery;
	f) Destruction;
	g) Actions required as a result of loss, theft or damage.
		PR.AC-1

11.8.3	Users **must** only be issued with one security token for a specific system, application or service, with the exception where authorised Privileged User access is dependent upon a second token. In this latter case, the second token **must** only be released or returned under formal change control. See also SS-001 pt2 Privileged User Access Security Standard [Ref. A].	PR.AT-2 PR.AC-6
11.8.4	A security token **must** only be associated with one User identity. This is necessary to ensure that a User's actions are fully accountable. Non-human accounts (such as service or robot accounts) may be assigned to a user identity, and managed accordingly.	PR.AC-1 PR.AC-6
11.8.5	Users **must** be instructed to immediately report any lost or stolen tokens.	PR.AT-1
11.8.6	The process for registering new token Users and issuing them with tokens that **must**: a) ensure that passwords relating to tokens are not sent in the form of clear text (e.g., in email or text messages) and not sent together with the token b) directly involve the person to whom the token uniquely applies (e.g., face-to-face registration in a secure location) c) verify the identity of the User, such as inspecting official identity documentation or through independent confirmation.	PR.AC-1 PR.AC-6

Reference	Minimum Technical Security Measures	NIST ID
11.8.7	Users of token authentication **must** be advised to: a) keep passwords for access to tokens confidential (i.e., to avoid making them visible to others by writing them down or disclosing them to others) b) protect tokens against loss, theft and misuse (e.g., avoid sharing with unauthorised individuals) c) report if the tokens have been or are suspected of being compromised (e.g., tampered with).	PR.AC-1 PR.AC-6

11.9 Additional Third Party Access Control Requirements

Reference	Minimum Technical Security Measures	NIST ID
11.9.1	Third Party access to Authority applications, systems or services **must** not be granted until a formal agreement or contract is in place.	PR.AC-1
11.9.2	Third Party access to Authority applications, systems or services **must** not be granted until a risk assessment and third party assessment has been completed.	ID.RM-1 ID.SC-2
11.9.3	All Third Party access requests **must** be approved by the appropriate identified Risk Owner. Third party user identities **must** be created on Authority systems, it is not permitted for third parties to utilise their own organisational identities on Authority systems.	ID.RM-1 PR.AC-4
11.9.4	All access requests **must** be retained for a minimum period of 12 months.	PR.AC-4
11.9.5	Third Party access accounts **must** not be permanently active and **must** be disabled when access is not required. There **must** be a documented procedure covering requests to enable the account.	PR.AC-1
11.9.6	Multi factor authentication (MFA) **must** be used for all Third Party Accounts.	PR.AC-1 PR.AC-7
11.9.7	All Third Party access **must** be monitored real-time.	PR.AC-1 DE.AE-3
11.9.8	All Third Party access to applications, systems or services **must** be recorded and records retained in line with the contract or formal agreement, and **must** be auditable.	PR.AC-1
11.9.9	Application, system or service owners **must** review Third Party accounts in line with the contract or formal	PR.AC-1

Reference	Minimum Technical Security Measures	NIST ID
	agreement to confirm access is still required, and consider risk.	
11.9.10	Third Party access **must** be terminated immediately at the end of the contract.	PR.AC-4
11.9.11	Organisations with third party access to Authority applications and systems **must** be subject to annual security testing.	PR.AC-4

11.10 Generic Accounts Security Control Requirements

Reference	Minimum Technical Security Measures	NIST ID
11.10.1	Generic or shared accounts **must not** be used to carry out any activities which may be achieved using other individually assigned privileged accounts.	PR.AC-1 PR.AC-6
11.10.2	Generic or shared accounts **must** only be used to carry out activities which cannot be achieved by other means.	PR.AC-1
11.10.3	Line managers are responsible for ensuring the appropriate and necessary use of generic or shared accounts by their staff.	PR.AC-1
11.10.4	All generic or shared account accesses **must** be subject to a technical risk assessment, and authorised in writing by the Senior Responsible Officer or be directly associated with a planned activity e.g. Service Desk Change Request or Incident.	PR.AC-1
11.10.5	The line manager **must** regularly check (at least monthly) to ensure that no unauthorised account access has taken place.	PR.AC-1
11.10.6	While all account usage is subject to monitoring, the use of generic or shared accounts **must** not only be monitored, but **must** always be subject to audit. Additional requirements may apply for privileged user accounts, see SS-001 pt.2 Privileged User Access [Ref. A].	PR.AC-1 DE.AE-3

11.11 API Authentication Requirements

Reference	Minimum Technical Security Measures	NIST ID
11.11.1	Every API endpoint **must** be authenticated.	PR.AC-7
11.11.2	The API gateway **must** implement a mechanism to restrict the number of, and alert on repeated authentication failures.	PR.AC-7
11.11.3	Access policies to all APIs and their resources must be defined and provisioned to an access server, which must be capable of supporting fine-grained policies.	PR.AC-4
11.11.4	Each service **must** have a totally unique API key for calling another service. This key **must** comprise of a unique Service ID and a User ID at minimum.	PR.AC-6
11.11.5	Services **must** only be able to access messaging channels required for their function.	PR.AC-4
11.11.6	Access to any given messaging channel **must** be limited to functionality required (such as read only, write, etc).	PR.AC-4
11.11.7	Messaging credentials **must** be protected appropriately at rest and in transit.	PR.DS-1 PR-DS-2

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.RM-1	Risk management processes are established, managed, and agreed to by organizational stakeholders	11.9.2; 11.9.3
ID.SC-2	Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	11.9.2;
PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	11.1.1; 11.1.2; 11.1.3; 11.1.4; 11.1.5; 11.2.1; 11.2.2; 11.2.3; 11.2.4; 11.3.1; 11.3.2; 11.3.3; 11.3.4; 11.3.5; 11.3.6; 11.3.7; 11.3.8; 11.3.9; 11.3.10; 11.3.11; 11.3.12 11.4.1; 11.4.2; 11.4.9 11.5.1; 11.5.2; 11.5.3; 11.5.4; 11.5.5; 11.5.6 11.6.1; 11.6.2; 11.6.3; 11.6.4; 11.6.5; 11.6.6; 11.6.7 11.7.1; 11.7.2; 11.7.3; 11.7.4; 11.7.5; 11.7.6; 11.7.7; 11.7.8; 11.7.9; 11.7.10; 11.7.11; 11.7.12;

NIST Ref	Security Outcome (sub-category)	Related Security measure

		11.7.13; 11.7.14; 11.7.15; 11.7.16; 11.7.17; 11.7.18; 11.7.19; 11.7.20
		11.8.1; 11.8.2; 11.8.4; 11.8.6; 11.8.7;
		11.9.1; 11.9.5; 11.9.6; 11.9.7; 11.9.8; 11.9.9; 11.10.1; 11.10.2; 11.10.3; 11.10.4; 11.10.5;
		11.11.1; 11.11.2; 11.11.3; 11.11.4; 11.11.5; 11.11.6

PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	11.1.1; 11.1.2; 11.3.2; 11.3.6; 11.3.9 11.4.4; 11.4.7; 11.4.9; 11.4.12; 11.9.4; 11.9.10; 11.9.11 11.11.3; 11.11.5; 11.11.6

PR.AC-6	Identities are proofed and bound to credentials and asserted in interactions	11.1.4; 11.1.5; 11.2.1; 11.2.2; 11.2.3; 11.2.4; 11.3.10; 11.4.7; 11.4.8;
		11.5.2; 11.5.3;
		11.7.2; 11.7.3; 11.7.4; 11.7.5; 11.7.6; 11.7.7; 11.7.8; 11.7.12;
		11.8.3; 11.8.4; 11.8.6; 11.8.7; 11.11.4

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)	11.2.2; 11.2.3; 11.2.4;
		11.4.8; 11.4.10; 11.4.11;
		11.5.4; 11.5.5; 11.7.1;
		11.9.6; 11.11.1; 11.11.2

PR.AT-1	All users are informed and trained	11.4.3; 11.4.5; 11.8.5;

NIST Ref	Security Outcome (sub-category)	Related Security measure
PR.AT-2	Privileged users understand their roles and responsibilities	11.1.5; 11.2.3; 11.3.3; 11.3.10; 11.3.11; 11.4.6; 11.4.12; 11.8.3
PR.DS-1	Data-at-rest is protected	11.11.7
PR.DS-2	Data-in-transit is protected	11.11.7
PR.IP-3	Configuration change control processes are in place	11.5.6;
DE.AE-3	Event data are collected and correlated from multiple sources and sensors	11.9.7; 11.11.6;

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-001 pt2 Privileged User Access Security Standard	Yes
B	DWP Approved Cryptographic Algorithms	No
C	Security Assurance Strategy	No
D	Privileged Users Security Policy	Yes
E	DWP Information Management Policy	Yes
G	DWP Security Vetting Policy	No
H	SS-007 Use of Cryptography security standard	Yes

Requests to access non-publicly available documents **should be made to an assigned DWP Security Architect or DWP Contracts/Supplier Manager.*

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
GPG 44 – Using authenticators to protect an online service
GPG 45 – How to prove and verify someone's identity
NCSC - Introduction to identity and access management
NCSC Password Policy
NIST 800-63 Digital Identity Guidelines

Appendix D Abbreviations

Table 4 – Abbreviations

Abbreviation	Definition
DDA	Digital Design Authority
DWP	Department for Work and Pensions

Appendix E Definition of Terms

Table 5 – Glossary

Term	Definition
Privileged User	A Privileged User is a user who has an elevated level of access to a network, computer hardware or system components or functionality and is authorised to perform functions that standard and elevated users are not authorised to perform.
Business Application	Business application is a DWP owned software programme used by DWP staff or DWP customer to perform DWP business functions such as JSA Online. It does not include MS Office applications.
Generic or shared accounts	Accounts allocated to more than one individual e.g. a team account.
Information System	Information System is a DWP owned software infrastructure used by DWP staff or DWP customer to perform DWP business functions such as Universal Credit.
Information Service	Business application owned by a third party but used by DWP staff or DWP customer to perform DWP business functions such as a hosted learning management system.
Service Account	An account provisioned for use mainly or solely by applications or services rather than a human user.
User Account	An account provisioned for use by human users.

Term	Definition
User Profile	A user profile ensures that all users are authorised to access the information that they need to carry out their jobs in the organisation while at the same time restricting those users from accessing secured information.

Appendix F Accessibility artefacts

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

DWP Digital Accessibility Policy | DWP Intranet

https://accessibility-manual.dwp.gov.uk/

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

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