Security Standard - Privileged User Access

SS-001 (part 2)

Chief Security Office

Date: 25/02/2026

This Privileged User Access 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	denotes a recommendation: an advisory element.
may	denotes approval.
might	denotes a possibility.
can	denotes both capability and possibility.
is/are	denotes a description.

1. Contents

2. Revision history

Version	Author	Description	Date
1.0		First published version	18/09/2017
1.1		10.2.5 Requirements for DV clearance defined.	21/02/2018
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 Section 10. to include a Privileged user definition and forward reference to Appendix E. 10.1 Secrets Management 11.1.1 Cloud based, SaaS, hybrid 11.1.5 Record Management Policy replaced by Information Management Policy; documented agreements 11.2.5 Added ref to Security Vetting Policy; risk based and time bound; DV and risk assessment requirements 11.2.6 Head of Security Vetting; conditional; appointment 11.2.8 Separation of duties/toxic combinations; user groups / personas	26/10/2023

		11.2.9 removal of “allowing system, application or service and Application controls to be overridden” as deemed to be out of date; added authorising payments 11.2.15 possible exception for Business need; command line usage; risk assessment 11.3.1 Appropriate approvals 11.4.1 cloud-based, non-human and service accounts; accountable owner 11.4.2 Conditions for shared privileged accounts 11.4.5 Accountable owner	
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 Introduction – new definition; admin tiering definitions; increased threats; threat modelling Scope – Definition of PU tiers added; Local privileged user accounts 11.1.1 Admin consoles, orchestration, interfaces, zero-trust, least privilege, conditional access	25/02/2026

		11.1.2 MFA for privileged functions; alignment with JML processes 11.1.3 Annual review 11.1.4 Audit requirements 11.1.5 Additional controls 11.1.6 ‘Browse-down’ architectures 11.1.7 Remote administration; ZT devices 11.1.8 Privileged Access Workstations 11.2.1 PU tiers; Controlled workflow; Out of band verification 11.2.2 Account disabling; break glass accounts 11.2.3 MFA, auditing and logging, and credential strength 11.2.4 NDAs; Temporary access 11.2.5 Pre-employment checks; NSV levels; Vetting procedures and requirements 11.2.6 Pre-employment checks, NSV, Security Questionnaire; Co-location; real time monitoring 11.2.7 Change requests 11.2.8 User group requirements 11.2.9 Security sensitive changes 11.2.10 Limit sharing of user details; training requirements	

		11.2.11 Central register 11.2.12 Standard Business Functions; authorising payments; Segregated privileged sessions 11.2.13 Added ref to Access & Authentication standard 11.2.15 DWP approved SIEM; Business justification, time-bound; time limit 11.2.16 Monitoring, manual or automated 11.2.17 Agentic AI usage 11.3.1 Out of band verification; access management requests 11.3.2 Quarterly reviews 11.3.3 & 11.3.4 Automated suspension 11.3.8 Session log retention 11.4.1 Generic account requirements 11.4.7 Generic account logging and alerting Internal Refs – Vetting procedures External Refs – NCSC Secure system administration Glossary – Break glass accounts; Browse-down; Out of band verification Abbreviations - CNI	

3. Approval history

Version	Name	Role	Date
1.0		Chief Security Officer	18/09/2017
2.0		Chief Security Officer	26/10/2023
2.1		Chief Security Officer	25/02/2026

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.

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 Privileged User Security Standard defines the minimum technical security measures that **must** be implemented for use within the Authority.

A privileged user is defined as:

“A user that is authorised, in accordance with their specific job role, to perform security-relevant functions that standard users are not. Such functions require a higher level of trust and may include, but are not limited to, managing security configurations, altering system operations, administering other user accounts, or accessing sensitive business, financial, or policy data.”

This definition applies whether the privileges are held permanently or are granted on a temporary or time limited basis.

Privileged access is critical given the foundation it provides for all other security assurances and should be considered the top security priority at every organisation, noting any compromise has a high likelihood of significant negative impact. The definition of privileged users includes both ‘administrative’ (e.g. network administrator, security analyst, database administrator etc.) or ‘support’ (e.g. IT helpdesk). Threat assessments have shown a notable increase in intent to compromise support privileged users through the use of social engineering, almost certainly due to their assumed or actual enhanced network permissions and insight into business processes

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 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 privileged user access are implemented consistently across the Authority and by third party providers where applicable
- mitigate risks from common threats and vulnerabilities associated with privileged user access, to an acceptable level for operation.
- support the achievement of security outcomes described in Appendix A.
- enable a risk based approach to be utilised in granting privileged user access; RBAC threat modelling may be used to model individual system RBAC risk levels against the requirements in this standard.

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

To manage different levels of privileged users, they can be grouped together in different tiers, in line with NCSC guidance for ‘Secure System Administration’ [see External References], using the following definitions;

Tier 0 - This is the root of trust that all other administration relies upon. If an attacker manages to compromise this, they could gain access to components in other tiers that are built upon it.

Examples:

- Root domain administrators that are able to create additional, highly privileged accounts.
- The root account in a cloud service, that manages the privileges of all other accounts.

- Offline infrastructure that is used to generate cryptographic material which other components rely upon.

As tier 0 includes the most critical components, ensuring secure access in an emergency **must** be considered. This can be referred to as ‘break glass’ access and should only be used as a last resort.

Tier 1 - This is infrastructure that still allows highly privileged functions on critical systems. However, it is more constrained than tier 0 as users in this tier can’t replicate this level of access. The impact of compromise could still cause widespread disruption.

Examples:

- Administrators of a critical database used to store a large amount of sensitive information, which several systems rely upon.
- The ability to control and manage a number of critical services in a cloud environment.
- Infrastructure that is used to set operational thresholds on critical control systems.

Tier 2 - This is infrastructure that allows privileged functions to be performed, but over a small amount of components. These components may still be critical, but the impact of compromise is limited, forcing an attacker to carry out additional work if they require a full compromise to achieve their objective.

Examples:

- Administrator access on an important business support application.
- Root level access on a front-end web server that forms part of a wider cloud architecture.
- Administration of a dashboard responsible for monitoring an industrial control system.

Tier 3 - This is infrastructure that allows a constrained set of functions over a single or small number of components. The impact of compromise in this tier may be undesirable and embarrassing, but not catastrophic to business operations.

Examples:

- First line support staff issuing a password reset.
- The ability to trigger a predefined action in a cloud environment, such as promotion of new feature code into a live environment.
- Modification of values in an industrial control system that are bounded by limits set by a component or administrator in a lower tier.

The standard applies to the following;

- Privileged user access solutions managed by the Authority or Third Party Supplier or other support function for internal Authority use.
- Any privileged user access solutions used to support Authority services and/or data by a third party provider.
- Local privileged user accounts that are not included in a privileged user access solution. The use of local privileged user accounts **must** be avoided, but where this is not possible, an exception **must** be sought.

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

10.1. Secrets Management

(Important) this paragraph contains ‘must’ activities.

Secrets management is a practice that allows staff such as developers or engineers to securely store sensitive data such as passwords, keys, and tokens in a secure environment with strict access controls, rather than hard-code them into scripts or source code. In a large environment, especially one that is virtualised or cloud-based, with a large number of types of secret, management of such secrets can be difficult to manage manually.

Use of Digital Design Authority approved secrets management tools is permitted and may also be used to support non-human or service accounts, but the requirements of this standard, and that of SS-001 pt.1 Access and Authentication Security Standard [Ref. A] **must** still be applied.

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. Technical Security Control Requirements

(Important) this table contains ‘must’ activities.

Reference	Minimum Technical Security Measures	NIST ID
11.1.1	Controls **must** be implemented to restrict access to business applications, information systems, services networks and computing devices, including cloud based systems, Software as a Service and hybrid services, and the information stored on and processed by them. They **must** explicitly cover administrative consoles, orchestration tools, and infrastructure management interfaces (e.g. hypervisors, cloud portals, CI/CD pipelines), and **must** enforce least privilege, zero-trust network segmentation, and conditional access principles.	PR.AA-04 PR.AA-05

11.1.2	The Authority and its Suppliers **must** implement appropriate identification and authentication controls (which **must** enforce MFA, with phishing resistant factors e.g. FIDO2, smartcard, biometrics etc. [which **must** be on a separate device]) for privileged functions to manage the risk of unauthorised access, and to ensure the correct management of user accounts and enable auditing. Account lifecycle management for human users **must** align with Joiners / Movers / Leavers (JML) processes with automated provisioning/deprovisioning. If this is not possible, an exception **must** be sought. The lifecycles for non-human accounts **must** also be managed, but these will not necessarily align with JML processes.	PR.AA-01 PR.AA-03 PR.AA-05 PR.PS-04
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. This **must** be reviewed annually or after any significant change to the system’s security posture.	PR.AA-05

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. The policy **must** include audit configuration requirements (e.g. event types, log retention, and correlation to privileged activity).	PR.AA-05
11.1.5	System Access Control Policies **must** be supported by documented procedures, which take account of: a) The Authority’s Security Standards, the Government Security Classification Policy (GSCP), documented agreements with application owners, requirements set by the owner of systems and legal, regulatory and contractual obligations, including the DWP Information Management Policy (see External References); b) The need to enforce individual accountability, apply additional control for users with special access privileges and provide segregation of duties. c) Additional controls including auditing and logging (which can include session recording), ‘just-in-time’ access, and ‘break-glass’ procedures.	PR.AA-05

11.1.6	Applications and systems **must** implement 'browse-down' architectures to prevent 'high trust' access from 'low trust' systems.	PR.AA-05
11.1.7	Remote administrative sessions **must** be brokered through secure jump hosts or bastion services. Where web consoles are accessed from Authority Zero Trust devices, this requirement does not apply.	PR.AA-05
11.1.8	Privileged Access Workstations (PAWs) **must** be used by default to perform privileged activities, in line with the Privileged User Tiers defined in the Scope of this document.	PR.AA-01 PR.AA-03

11.2. Privileged User Access Control Requirements

(Important) this table contains 'must' activities.

Reference	Minimum Technical Security Measures	NIST ID
11.2.1	Access to operating system, application or service privileges **must** be strictly controlled. Issue of all elevated privileges, (above those of a 'normal' user, and in line with the Privileged User Tiers defined in the Scope of this document), **must** be subject to a formal and documented management authorisation procedure recorded in the System Access Control Policy, and raised and approved through a controlled workflow / change management service. This **must** include implementing out-of-band verification, mandatory presentation of ID on-camera / in person, and challenge / response questions based on pre-agreed phrases shared with privileged users.	PR.AA-02 PR.AA-05

11.2.2	All default or built in Privileged User accounts **must** have their passwords changed at installation. Default Privileged User account names **must** be changed to a less obvious name or, subject to a technical risk assessment, the default account **must** be disabled. Where disabling is not possible, accounts and credentials **must** be secured in an appropriate security store and rotated automatically (unless in the case of ‘break glass’ accounts).	PR.AA-01 PR.AA-05
11.2.3	Privileged access to Authority systems, applications or services **must not** be granted until registration and authorisation procedures have been completed in compliance with SS-001-1 Access and Authentication Security Standard [Ref. A], including requirements for MFA, auditing and logging, and credential strength.	PR.AA-02 PR.AA-04
11.2.4	To gain authorised registration as a Privileged User, an individual **must** be a permanent Authority employee or a permanent employee or contractor of an organisation which has a formal contractual agreement with the Authority, including a commitment to non-disclosure agreements (NDAs) and to maintaining Authority information security standards. Temporary or emergency elevated access **must** only be granted through an auditable time bound exception.	PR.AA-02 PR.AA-04

11.2.5	All Privileged Users **must** have the appropriate level of pre-employment checks and, in most cases, the appropriate level of National Security Vetting (NSV) for the role they are assigned, in line with the DWP Security Vetting Procedures [Ref. C]: • Privileged users with significant system or service privileges (those with extensive access rights) **must** a hold the NSV level of Security Check (SC) or above; • Privileged users with significant CNI system or service privileges **must** have a minimum SC clearance; • Privileged users with access rights to citizen identity / customer personal information **must** have a minimum SC clearance; • Where the assets are not classified TOP SECRET but would cause severe long-term damage to the UK economy, then a risk assessment **must** be used to assess if DV is required. • Access **must** consider risk, be time bound, and be regularly reviewed in line with the level of privilege granted.	PR.AA-02 PR.AA-04
11.2.6	In exceptional circumstances, where it is critical that an individual starts work in a National Security Vetted role before their security clearance has completed, they **must** have at the least completed the standard pre-employment check of the Baseline Personnel Security Standard and completed the Security Questionnaire as part of the NSV process. They will further require direct 1-2-1 co-located supervision at all times.	PR.AA-02 PR.AA-05

	The decision to allow access without clearance **must** be risk assessed, documented and signed off by the Head of Security Vetting. If the risk is accepted then the individual **must** be brought into the Authority on a conditional appointment, with the condition being that they need to pass their vetting to remain in role. If clearance is then refused the individual will be dismissed under the terms of the conditional appointment. Where privileged access is required, this **must** be supported by a valid clearance (i.e. SC or above, depending on the individual scenario). If this clearance is not in place, a formal exception is required; • This exception **must** be raised by the relevant Deputy Director with the Director of Digital Transformation, who will determine if the exception is valid – Deputy Directors cannot authorise this themselves; • If the Director of Digital Transformation supports the exception request, he/she will then approach the Chief Security Officer to consider the request, and only if agreed, can the exception be granted without the appropriate clearance in place.	
11.2.7	All contractors requiring Privileged User access **must** be accountable to and have their access managed by a permanent member of Authority staff, including review and approval of all privilege change requests.	PR.AA-02 PR.AA-05

11.2.8	Applications for Privileged User accounts **must** be checked to ensure that the privileges requested map to and are restricted to the user's roles and responsibilities and that no unnecessary privileges or conflicting roles and responsibilities have been requested. Separation of duties **must** be considered, to prevent 'toxic combinations' of incompatible responsibilities e.g. creating payments and authorising payments. It is permitted to set up 'user groups' or 'personas' with associated use cases and access tiers to make managing groups of privileged users easier, but these **must** be formally documented, risk assessed, and approved, and the same level of scrutiny when assigning users to them **must** be applied and reviewed every 90 days.	PR.AA-02 PR.AA-05
11.2.9	Only authorised Privileged Users **must** perform actions such as (this list is not exhaustive): • the enabling and disabling of peripheral devices; • backing up and recovering User Objects; • starting and shutting down the system, application or service • making security-sensitive configuration changes (e.g. modifying ACLs, firewall rules, IAM policies etc.).	PR.AA-05

11.2.10	Privileged Users **must** sign additional agreements to accept responsibility for their use of privileges and be issued with specific procedures and provided with training relating to use of their system, application or service privilege, including insider threat awareness, phishing/social engineering prevention, and secure operational practices. Privileged users **must not** share any role-specific details on the internet or on social media to minimise the risk from social engineering.	PR.AA-05 PR.AT-02
11.2.11	All credentials assigned to a privileged user **must** be recorded in a central register.	PR.AA-01
11.2.12	Privileged Users **must not** use privileged accounts to carry out day to day duties or standard business functions which do not require the use of a privileged account, e.g. viewing a batch job status from a system administrator account, or authorising payments. Privileged sessions **must** be segregated from standard sessions (e.g. via separate virtual desktops or jump servers).	PR.AA-02
11.2.13	Privileged Users **must** be subject to multi factor authentication, in line with SS-001-1 Access & Authentication security standard [Ref. A].	PR.AA-03
11.2.14	Machine generated passwords **must** be used wherever possible for Privileged User accounts and **must** be changed at least every 90 days.	PR.AA-01 PR.AA-05

11.2.15	Access to raw operating system facilities and command lines **must** be treated and managed as privileges and applied strictly in accordance with the ‘least privilege’ principle. These access privileges **must** only be allocated once options for use of alternative equivalent business application level privileges have been exhausted. Command line usage **must** be attributable to named individuals and logged to an Authority approved centralised Security Information and Event Management (SIEM) system wherever possible. The use of anonymous, redirected, proxy or shared user accounts with raw operating system, application or service privileges **must** be prohibited unless when a specific business need requires it and is authorised by an appropriate Business owner and supported by a risk assessment, a business justification, and be time-bound.	PR.AA-05
11.2.16	The use of security critical operating system privileges (e.g. Administrative privilege management) **must** be the subject of a mutual control regime involving two or more privileged personnel. This can be accomplished in a number of ways, for example by: • A workflow system, application or service that requires authorisation of activities to enable a pathway for exercise of the privilege; • Division of privileges such that one administrator, or group, has privilege to enable/disable the critical operation (a ‘gatekeeper’) and another has privilege to exercise it (an ‘executor’);	PR.AA-05 PR.PS-04

	- Use of an advanced authentication and authorisation system, application or service that requires either multiple tokens to be presented, or segments of a passphrase to be entered, to allow the action to take place; Accounting for such operations **must** provide traceability of all personnel taking part. There **must** be near-real time monitoring (i.e. within 15 minutes, which may be manual or automated) and very frequent audit of all security affecting operating system privileges such that all operations are the subject of review.	
11.2.17	Any use of agentic AI tools **must** be approved by the Authority’s Digital Design Authority, and attributable to a named user and unique agent ID, and be fully logged and monitored.	PR.PS-04 DE.CM-03

11.3.

11.4. Changes to Privileges Security Control Requirements

(Important) this table contains ‘must’ activities.

Reference	Minimum Technical Security Measures	NIST ID
11.3.1	Line managers **must** request any necessary alterations to privileges (with appropriate approvals in place), to have privileged user accounts deleted or to have accounts changed or added, via an approved access management request system or process to ensure full auditability. This may include implementing out-of-band verification, mandatory presentation of ID on-camera / in person, and challenge / response questions based on pre-agreed phrases shared with privileged users.	PR.AA-05
11.3.2	All Privileged User Accounts **must** be reviewed every 90 days (or on notification of a change) by the user’s line manager and / or system owner to ensure that: • Users are still in the same role with the same responsibilities; • Current privileges match the requirements to meet those roles and responsibilities and do not exceed them; • No changes have been introduced into working practices which set up a privilege conflict; • The account continues to be used; • All accounts which were used by individuals who have left employment or have changed job roles have been properly terminated and all other means of access removed.	PR.AA-05

	- Evidence of quarterly reviews **must** be retained for audit e.g. signed attestation or system-generated report. Where discrepancies are found, remediation **must** occur within 5 working days.	
11.3.3	Where a privileged user is absent from work for a period of greater than four weeks (due to secondment, training courses, maternity leave or long term sickness absence etc.) the account **must** be suspended. This suspension **must** be automated where technically feasible, and where not, an equivalent manual process **must** be invoked.	PR.AA-05
11.3.4	Where a privilege user account has been dormant for four weeks it **must** be suspended. This suspension **must** be automated and logged where technically feasible, and where not, an equivalent manual process **must** be invoked.	PR.AA-05
11.3.5	Privileges **must** be revoked immediately via the appropriate documented procedure when a user’s employment has been terminated or their role has changed so that it no longer requires elevated privileges.	PR.AA-05
11.3.6	Passwords for any generic or shared system, application or service accounts accessible by the departing user **must** be changed asap when a user’s employment has been terminated or their role has changed so that it no longer requires elevated privileges.	PR.AA-01

11.3.7	Line managers **must** ensure the Privileged User also hands back all means of remote access to systems, applications or services (should they exist) to the service organisation.	PR.AA-01 PR.AA-06
11.3.8	Session logs for departing privileged users **must** be retained for a minimum of 12 months after their departure for investigative traceability.	PR.PS-04

11.5. Generic Accounts Security Control Requirements

(Important) this table contains ‘must’ activities.

Reference	Minimum Technical Security Measures	NIST ID
11.4.1	Generic or shared privileged accounts (including cloud-based, non-human and service accounts) **must** have an accountable owner and **must not** be used to carry out any activities which may be achieved using other individually assigned privileged accounts. Each generic account **must** have a defined purpose, expiry date, and unique identifier to enable traceability, and all such accounts **must** be included in quarterly access reviews.	PR.AA-05
11.4.2	Generic or shared privileged accounts **must** only be used to carry out activities which cannot be achieved by other means. As per section 11.2.15, the use of anonymous, redirected, proxy or shared user accounts with raw operating system, application or service privileges is prohibited unless where a specific business need requires it and is authorised by an appropriate Business owner and supported by a risk assessment.	PR.AA-05

11.4.3	Line managers **must** ensure the appropriate and necessary use of generic or shared privileged accounts by their staff.	PR.AA-05
11.4.4	All generic or shared privileged account access **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.	ID.RA-07 PR.AA-05
11.4.5	The line manager or accountable owner **must** regularly check to ensure that no unauthorised generic or shared privileged account access has taken place.	PR.AA-05 PR.PS-04
11.4.6	While all account usage is subject to monitoring, the use of shared generic or shared privileged accounts **must not** only be monitored, but **must** always be subject to audit when required.	PR.AA-05 PR.PS-04
11.4.7	Logs for generic account usage **must** be integrated into an Authority approved centralised Security Information and Event Management (SIEM) system and retained for at least 12 months. Privileged activity via generic accounts **must** trigger alerts for out-of-hours or anomalous use patterns.	PR.PS-04

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
ID.RA-07	Changes and exceptions are managed, assessed for risk impact, recorded, and tracked	11.4.4
PR.AA-01	Identities and credentials for authorised users, services, and hardware are managed by the organisation	11.1.2, 11.1.8, 11.2.2, 11.2.11, 11.2.14, 11.3.6, 11.3.7
PR.AA-02	Identities are proofed and bound to credentials based on the context of interactions	11.2.1, 11.2.3, 11.2.3, 11.2.4, 11.2.5, 11.2.6, 11.2.7, 11.2.8, 11.2.12
PR.AA-03	Users, services, and hardware are authenticated	11.1.2, 11.1.8, 11.2.13
PR.AA-04	Identity assertions are protected, conveyed, and verified	11.1.1, 11.2.4, 11.2.3, 11.2.4, 11.2.5
PR.AA-05	Access permissions, entitlements, and authorisations are defined in a policy, managed, enforced, and reviewed, and	11.1.1, 11.1.2, 11.1.3, 11.1.4, 11.1.5, 11.1.6, 11.1.7, 11.2.1, 11.2.2,

	incorporate the principles of least privilege and separation of duties	11.2.6, 11.2.7, 11.2.8, 11.2.9, 11.2.10, 11.2.14, 11.2.15, 11.2.16, 11.3.1, 11.3.2, 11.3.3, 11.3.4, 11.3.5, 11.4.1, 11.4.2, 11.4.3, 11.4.4, 11.4.5, 11.4.6
PR.AA-06	Physical access to assets is managed, monitored, and enforced commensurate with risk	11.3.7
PR.AT-02	Individuals in specialised roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind	11.2.10
PR.PS-04	Log records are generated and made available for continuous monitoring	11.1.2, 11.2.16, 11.2.17, 11.3.8, 11.4.5, 11.4.6, 11.4.7
DE.CM-03	Personnel activity and technology usage are monitored to find potentially adverse events	11.2.17

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-001 pt.1 Access and Authentication Security Standard	Yes
B	DWP Information Management Policy	Yes
C	DWP Security Vetting Procedures	No
D	Security Assurance Strategy	No

*Request to access to 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 4 – External References

External Documents List
CIS Critical Security Controls set
NCSC - Secure system administration - Risk manage administration using tiers

Appendix D Abbreviations

Table 5 – Abbreviations

Abbreviation	Definition
CNI	Critical National Infrastructure
DDA	Digital Design Authority
DWP	Department for Work and Pensions

Appendix E Definition of Terms

Table 6 – Glossary

Term	Definition
‘Break Glass’ accounts	Highly privileged, emergency-only admin accounts used to bypass normal security controls and regain access to systems during critical incidents like cyberattacks or system outages, preventing complete lockout.
Browse-down	When administration of a system is performed from a device which is more trusted than the system being administered.
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.
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
Out of band verification	A communications channel separate from that being changed.
Privileged User	Defined in the Introduction section of this document.
Service Account	An account provisioned for use mainly or solely by applications or services rather than a human user.
Standard User	A standard user has privileges assigned to them to allow them to perform their role, but does not allow them access to functionality that can change system parameters, to affect other users.
User Account	An account provisioned for use by human users.

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