Security Standard - Privileged User Access SS-001 (part 2)

Chief Security Office

Date: 26/10/2023

Department for Work & Pensions

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 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
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 v8 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 11.2.9 removal of “allowing system, application or service and Application controls to be overridden” as deemed to be out of date; added authorising payments 11.2.15 possible exception for Business need; command line usage; risk assessment 11.3.1 Appropriate approvals 11.4.1 cloud-based,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	26/10/2023

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. D].
- 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 Privileged User 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 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.

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 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

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. For the purposes of this document 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 users are not authorised to perform (see Appendix E).

The standard applies to the following;

- Privileged user access solutions managed by the Authority or a 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.

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

10.1 Secrets Management

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

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

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.	PR.AC-1 PR.AC-2 PR.AC-3
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
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.	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, 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 Authority 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.	PR.AC-1 PR.AC-6 PR.AT-2

11.2 Privileged User Access Control Requirements

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), **must** be subject to a formal and documented management authorisation procedure recorded in the System Access Control Policy.	PR.AC-1
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.	PR.AC-1 PR.AC-4
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].	PR.AC-4
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 NDAs and to maintaining Authority information security standards.	PR.AC-4

11.2.5	All Privileged Users **must** have the appropriate level of background checks and clearance for the role they are assigned, in line with the Authority Security Vetting Policy [Ref. C]: • Privileged users with significant system or service privileges (those with extensive access rights) **must** a hold National Security Clearance; • 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; • A risk assessment **must** be used to determine whether DV is the appropriate level of clearance where the assets that are to be accessed do not carry a classification of TOP SECRET but nonetheless the risk of harm that could be caused would be as high as if they did have a TOP SECRET classification, for example privilege users with access all areas control of systems. • Access **must** consider risk, be time bound, and be regularly reviewed in line with the level of privilege granted.	PR.AC-7
11.2.6	In exceptional circumstances, where it is critical that an individual starts work in a National Security Vetted role before their clearance has completed, they **must** have at the least acquired BPSS clearance and completed their vetting application form then require direct 1-2-1 supervision at all times. The decision to allow access without clearance **must** be risk assessed, documented and signed off by the appropriate Senior Responsible Officer and the Head of Security Vetting. If the risk is accepted then the individual **must** be bought 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.	PR.AC-7
11.2.7	All contractors requiring Privileged User access **must** be accountable to and have their access managed by an Authority permanent member of staff.	ID.SC-4

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 the same level of scrutiny when assigning users to them **must** be applied.	PR.AC-4
11.2.9	Only authorised Privileged Users **must** perform actions such as (this list is not exhaustive): • the enabling and disabling of peripheral devices; • mounting of removable storage Media; • backing up and recovering User Objects; • starting and shutting down the system, application or service • authorising payments	PR.AC-1 PR.AT-2
11.2.10	Privileged Users **must** sign additional agreements to accept responsibility for their use of privileges and be issued with specific procedures relating to use of their system, application or service privilege.	PR.AC-6 PR.AT-2
11.2.11	All credentials assigned to a privileged user **must** be recorded.	PR.AC-6
11.2.12	Privileged Users **must not** use privileged accounts to carry out day to day duties or any action which does not require the use of a privileged account, e.g. viewing a batch job status from a system administrator account.	PR.AT-2
11.2.13	Privileged Users **must** be subject to multi factor authentication.	PR.AC-1
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.AC-1

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. 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.	PR.AC-4
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'); • 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 oversight and very frequent audit of all security affecting operating system privileges such that all operations are the subject of review.	PR.AC-4 PR.AT-2

11.3 Changes to Privileges Security Control Requirements

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, by completion of the appropriate form and by following a documented process.	PR.AC-4
11.3.2	All Privileged User Accounts **must** be reviewed every 90 days by the user's line manager to ensure that: • Users continue to hold the necessary security clearances; • 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.AC-1
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.	PR.AC-1
11.3.4	Where a privilege user account has been dormant for four weeks it **must** be suspended.	PR.AC-1
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.AC-1
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.AC-1
11.3.7	Line manager **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.AC-1

11.4 Generic Accounts Security Control Requirements

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.	PR.AT-2
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.	DE.CM-7
11.4.3	Line managers **must** ensure the appropriate and necessary use of generic or shared privileged accounts by their staff.	DE.CM-7
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.	PR.AT-2 ID.GV-4
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.AC-1
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.	DE.CM-7

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.GV-4	Governance and risk management processes address cybersecurity risks	11.4.4
ID.SC-4	Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	11.2.7

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;11.2.9;
		11.2.13;11.2.14;
		11.3.2;11.3.3;11.3.4;
		11.3.5;11.3.6;11.3.7;
		11.4.5

PR.AC-2	Physical access to assets is managed and protected	11.1.1
PR.AC-3	Remote access is managed	11.1.1

PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	11.1.2;
		11.2.2;11.2.3;11.2.4;
		11.2.8;11.2.15;11.2.16;
		11.3.1

PR.AC-6	Identities are proofed and bound to credentials and asserted in interactions	11.1.4;11.1.5; 11.2.10;11.2.11
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)	11.2.5;11.2.6
PR.AT-2	Privileged users understand their roles and responsibilities	11.1.5; 11.2.9; 11.2.10; 11.2.12; 11.2.16; 11.4.1; 11.4.4

DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed	11.4.2;
		11.4.3;
		11.4.6

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

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

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
Business Application	Business application is an Authority owned software programme used by Authority staff or Authority customer to perform Authority business functions such as JSA Online. It does not include MS Office applications.
Information System	Information System is an Authority owned software infrastructure used by Authority staff or Authority customer to perform Authority business functions such as Universal Credit
Information Service	Business application owned by a third party but used by Authority staff or Authority customer to perform Authority business functions such as a hosted learning management system
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.
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