IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

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

Chief Security Office

Date: March 2018

Department for Work & Pensions

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

Version Control Table

Version	Date	Major Change

Updating policy

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

The version control table will show the published update date and provide a thumbnail of the major change. CAUTION: the thumbnail is not intended to summarise the change and not a substitute for reading the full text.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

Contents

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

1. Introduction

1.1. This Privileged User Access Control Security Standard provides the list of controls that are required for business applications, information systems, networks and computing devices, to restrict and control the allocation and use of privileged access rights.

This list of requirements ensures a baseline level of security that is approved and accepted by the Department for Work and Pensions (DWP) to afford the necessary level of protection to its systems and data.

1.2. For further clarity and relevance, this standard is aligned to the DWP Digital Blueprint, which defines the direction for all departmental technology.

1.3. Furthermore the security controls presented in this standard are taken from examples of international best practice for information security and have been tailored for Departmental suitability.

2. Purpose

2.1. The purpose of this document is to enable teams to work to a defined set of security requirements which enable solutions to be developed, deployed and managed to Departmental security standards, which are based upon international best practice for information security.

2.2. Secondly, this standard provides a means to conduct compliance based technical security audits.

3. Exceptions

In this document the term **MUST** in upper case is used to indicate an absolute requirement. Failure to meet these requirements will require a formal exemption.

3.1. Any exceptions to the application of this standard or where controls cannot be adhered to **MUST** be presented to an assigned Security Architect and considered for submission to Design Authority (DA) where appropriate. This **MUST** be carried out prior to deployment and managed through the design caveats or exception process.

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

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

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

4. Audience

4.1. This standard is intended for (but not limited to) security controls testing consultants, solution, domain and security architects and system designers as well as engineers and/or system administrators who are provisioning servers for departmental use.

5. Scope

5.1. This standard is to cover systems, applications, networks, and devices handling data within the OFFICIAL tier of the Government Security Classification Policy (GSCP). All of the Department's ICT system, application, or service implementations falling within this category will be subject to the requirements specified within this security standard. The requirements will be applied to new and existing installations.

5.2. The security control requirements laid out in this standard are product agnostic and applicable for all ICT system, application, or service implementations that are provisioned for departmental use.

5.3. Additional controls may be applicable based upon the Security Classification of the information being processed by the Department's ICT system, application, or service implementation.

5.4. In the event of uncertainty on the controls laid out in this standard please contact the Security Front Door for guidance and support on items which require clarification.

6. Security Controls Assurance

6.1. Controls presented in this standard or referred to via this standard may be subjected to a formalised IT Health Check or Penetration Test to provide evidence of adequacy and effectiveness.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

7. Technical Security Control Requirements

Reference	General Security Control Requirement
10.1.1	Controls **MUST** be implemented to restrict access to business applications, information systems, services networks and computing devices, and the information stored on and processed by them.
10.1.2	The Department and its Agencies **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.
10.1.3	All individual Departmental 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.
10.1.4	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
10.1.5	System Access Control Policies **MUST** be supported by documented procedures, which take account of: a) The DWP Security Standards, the Government Security Classification Policy (GSCP), agreements with application owners, requirements set by the owner of systems and legal, regulatory and contractual obligations, including DWP Records Management Policy; b) The need to enforce individual accountability, apply additional control for users with special access privileges and provide segregation of duties.

Reference	Privileged Users Access Control Requirements
10.2.1	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.
10.2.2	All default or built in Privileged User accounts **MUST** have their passwords changed at installation.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

Reference	Privileged Users Access Control Requirements
	Where possible 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.
10.2.3	Privileged access to DWP systems, applications or services **MUST not** be granted until registration and authorisation procedures have been completed in compliance with the Authentication and Access Control Standard.
10.2.4	To gain authorised registration as a Privileged User, an individual **MUST** be a permanent DWP employee or a permanent employee or contractor of an organisation which has a formal contractual agreement with the DWP, including a commitment to NDAs and to maintaining DWP information security standards.
10.2.5	All Privileged Users **MUST** have the appropriate level of background checks and clearance for the role they are assigned: • 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 DV clearance requirement for Privileged users who do not have robust Authentication, Authorisation and Audit controls applied to their access CNI services or where these controls can be circumvented that allows the Privileged account uncontrolled access rights to citizen identity / customer personal information and egress/export rights or capability.
10.2.6	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 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 SRO.
10.2.7	In line with the Guide to Managing Contractors Documentation, all contractors requiring Privileged User access **MUST** be accountable to and have their access managed by a DWP permanent member of staff.
10.2.8	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.
10.2.9	Only authorised Privileged Users **MUST** perform actions such as: a) the enabling and disabling of peripheral devices; b) mounting of removable storage Media;

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

Reference	Privileged Users Access Control Requirements
	c) backing up and recovering User Objects; d) starting and shutting down the system, application or service; e) allowing system, application or service and Application controls to be overridden;
10.2.10	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.
10.2.11	All credentials assigned to a privileged user **MUST** be recorded.
10.2.12	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.
10.2.13	Privileged Users **MUST** be subject to two–factor authentication.
10.2.14	Machine generated passwords **MUST** be used wherever possible for Privileged User accounts and **MUST** be changed at least every 90 days.
10.2.15	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. Use of raw operating system commands **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.
10.2.16	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) A workflow system, application or service that requires authorisation of activities to enable a pathway for exercise of the privilege; b) 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'); c) 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.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

Reference	Changes to Privileges Security Control Requirements
10.3.1	Line managers **MUST** request any necessary alterations to privileges, 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.
10.3.2	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.
10.3.3	Where a privileged user is absent from work for a period of greater that four weeks (due to secondment courses, maternity leave or long term sickness absence etc.) the account **MUST** be suspended.
10.3.4	Where a privilege user account has been dormant for four weeks it **MUST** be suspended.
10.3.5	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.
10.3.6	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.
10.3.7	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.

Reference	Generic Accounts Security Control Requirements
10.4.1	Generic or shared privileged accounts **MUST not** be used to carry out any activities which may be achieved using other individually assigned privileged accounts.
10.4.2	Generic or shared privileged accounts **MUST** only be used to carry out activities which cannot be achieved by other means.
10.4.3	Line managers of service organisations **MUST** ensure the appropriate and necessary use of generic or shared privileged accounts by their staff.
10.4.4	All generic or shared privileged account access **MUST** be subject to a technical risk assessment and authorised in writing by the SRO or be directly associated with a planned activity e.g. Service Desk Change Request or Incident.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

Reference	Generic Accounts Security Control Requirements
10.4.5	The line manager **MUST** regularly check to ensure that no unauthorised generic or shared privileged account access has taken place.
10.4.6	While all account usage is subject to monitoring, the use of generic or shared generic or shared privileged accounts **MUST** not only be monitored, but **MUST** always be subject to audit.

8. Compliance

Compliance with this standard MUST occur as follows:

Compliance	Due Date
On-going	From the first day of approval
Retrospective	Within 6 months of the approval of the standard.

9. Accessibility

No user interfaces are included in this standard and accessibility is not applicable as part of this standard. However it is deemed that projects implementing this standard are obliged to incorporate accessibility functions.

10. Security Standards Reference List

Document Name	Location	Version
Exceptions Process	XX/XX/XX	

11. Reference Documents

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-123.pdf

12. Definition of Terms

Term	Definition
Privilege 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.
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

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

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.

13. Glossary

Abbreviation	Definition
DA	Design Authority (DA)
DWP	Department for Work and Pensions (DWP)

14. Controls Catalogue Mapping

The table below shows how the controls in this standard map to the DWP Controls Catalogue and thereon to control points in international security standards including but not limited to ISO/IEC 27002:2013, NIST 800-53, and the OWASP ASVS.

***SS-001 Privileged User Access Control STANDARD* Control Statement**	**Baseline Control Set**	
10.1.1	DWP_AC16	Access to information and application system functions shall be restricted in accordance with the access control policy.
10.1.2	DWP_AC19	Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.
10.1.3	DWP_AC01	An access control policy shall be established, documented, and reviewed based on business and information security requirements.
10.1.4	DWP_AC01	An access control policy shall be established, documented, and reviewed based on business and information security requirements.
10.1.5	DWP_AC01	An access control policy shall be established, documented, and reviewed based on business and information security requirements.
10.2.1	DWP_AC01	An access control policy shall be established, documented, and reviewed based on business and information security requirements.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

***SS-001 Privileged User Access Control STANDARD* Control Statement**	**Baseline Control Set**	
10.2.2	DWP_AC20	Password management systems shall be interactive and shall ensure quality passwords.
10.2.3	DWP_AC04	A formal user registration and de-registration process shall be implemented to enable assignment of access rights.
10.2.4	DWP_AC04	A formal user registration and de-registration process shall be implemented to enable assignment of access rights.
10.2.5	DWP_HR05	Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed, and the perceived risks. (BPSS)
10.2.6	DWP_HR05	Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed, and the perceived risks. (BPSS)
10.2.7	DWP_AC08	The allocation and use of privileged access rights shall be restricted and controlled.
10.2.8	DWP_AC08	The allocation and use of privileged access rights shall be restricted and controlled.
10.2.9	DWP_AC21	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.
10.2.10	DWP_AC08	The allocation and use of privileged access rights shall be restricted and controlled.
10.2.11	DWP_AC06	A formal user access provisioning process shall be implemented to

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

***SS-001 Privileged User Access Control STANDARD* Control Statement**	**Baseline Control Set**	
		assign or revoke access rights for all user types to all systems and services.
10.2.12	DWP_AC08	The allocation and use of privileged access rights shall be restricted and controlled.
10.2.13	DWP_AC20	Password management systems shall be interactive and shall ensure quality passwords.
10.2.14	DWP_AC20	Password management systems shall be interactive and shall ensure quality passwords.
10.2.15	DWP_AC24	Access to program source code shall be restricted.
10.2.16	DWP_AC21	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.
10.3.1	DWP_AC15	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.
10.3.2	DWP_AC14	Asset owners shall review users' access rights at regular intervals.
10.3.3	DWP_AC15	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.
10.3.4	DWP_AC15	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.
10.3.5	DWP_AC15	The access rights of all employees and external party users to information and information

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

***SS-001 Privileged User Access Control STANDARD* Control Statement**	**Baseline Control Set**	
		processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.
10.3.6	DWP_AC15	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.
10.3.7	DWP_AC15	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.
10.4.1	DWP_AC08	The allocation and use of privileged access rights shall be restricted and controlled.
10.4.2	DWP_AC08	The allocation and use of privileged access rights shall be restricted and controlled.
10.4.3	DWP_AC08	The allocation and use of privileged access rights shall be restricted and controlled.
10.4.4	DWP_AC08	The allocation and use of privileged access rights shall be restricted and controlled.
10.4.5	DWP_AC08	The allocation and use of privileged access rights shall be restricted and controlled.
10.4.6	DWP_AC08	The allocation and use of privileged access rights shall be restricted and controlled.