Privileged Users Security Policy

Contents

Introduction

This policy provides a definition for what is a privileged user and outlines the measures that must be in place for the management of privileged users who operate across the Department for Work and Pensions (DWP) estate.

Scope

This policy applies to all privileged users who have access to DWP assets. This applies to DWP employees and suppliers who maintain systems or manage DWP information and assets whether the data is processed or stored on DWP ICT systems or on a supplier's system.

Privileged User Definition

A privileged user is a user who has an elevated level of access to a network, computer system or application and is authorised to perform functions that standard users are not authorised to perform.

This includes a standard user with escalated privileges which gives access on a par with a privileged user.

This policy does not cover a standard user who has access rights over and above those granted to other standard users in order for them to perform specialist functions; these are as outlined in the User Access Control Policy.

Policy Statement

Principle of Least Privilege

Privileged users must only be provided with the absolute minimum access rights, permissions to systems, services, information and resources that they need to fulfil their business role.

Authorisation Process

There must be a formal authorisation process to grant, assign and approve the allocation of a privileged user role.

Security Clearance

All privileged users must have the appropriate level of background checks and clearance for the role they are assigned.

User Identification and Access Control

Each privileged user must be uniquely identifiable.

All privileged users must be managed using identity and access management policies.

Account Management

Privileged access is only used and granted when it is needed and revoked when it is no longer required.

Joiners, leavers and movers' processes and procedures must register and include processes for the management of privileged users.

Privileged users must be subject to strong multi – factor authentication or a minimum password policy must be applied.

Privileged user access rights must be monitored and reviewed and revalidated on a monthly basis to confirm that the levels of access are still required for the role.

A record of all privileged user roles assigned and their level of access must be recorded, maintained and made available on request.

Monitoring and Auditing

Logging and monitoring tools and techniques must be used to monitor and manage privileged users' behaviour and actions.

The activities of a privileged user must leave a log or audit records that are outside the read, write and/or delete capability of their role.

Privileged user accounts and their usage must be monitored and reviewed.

Accounts that are dormant or accounts that cannot be associated with a business process and owner must be disabled.

Education, Training and Awareness

All privileged users must have security and awareness training in relation to the role in addition to the standard security and awareness training.

Business Continuity and Disaster Recovery

Business continuity and disaster recovery plans must have clearly defined processes and procedures for allocation and management of privileged users.

Responsibilities

Senior Responsible Owner (SRO)

Privileged user access must be requested in writing, detailing the access required, and authorised by a Senior Responsible Owner (SRO).

A record of all privileges allocated must be maintained by the SRO.

Suppliers

Privileged user access must be requested in writing, detailing the access required, and authorised by the applicable Authority (equivalent to the SRO role) for that Supplier.

A record of all privileges allocated must be maintained by the Supplier Security Manager.

Suppliers must inform the Authority if any access has had to be revoked as a consequence of a security incident.

Suppliers must be able to provide the Authority with audit logs or records that show when the privileged accounts have been used upon request.

Policy Exceptions

If the requirements in the Privileged User Security Policy cannot be met then the reasons for this must be documented, risk assessed and explained to the SRO or, where appropriate, the Authority for their approval.