User Access Control Policy

Contents

Introduction

This policy is to provide a framework for how user accounts and privileges are created, managed and deleted.

It includes how new users are authorised and granted appropriate privileges, as well as how these are reviewed and revoked when necessary and includes appropriate controls to prevent users obtaining unauthorised privileges or access.

Scope

This policy applies to:

- All employees and suppliers who have access to the Department for Work and Pensions (DWP's) information and information systems.
- Information systems and services in programme, project and operational business areas.

There are some access roles which require implementing stronger controls than those for standard users.

Definitions

Users

This is the collective term used to describe all those who have access to the DWP's information and information systems as outlined in the Scope of this policy.

Privileged Users

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 approved elevated privileges that allows equivalent access to that of a privileged user.

Policy Statements

Principle of Least Privilege

Access controls must be allocated on the basis of business need and ‘Least Privilege’. 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.

User Access Account Management

User account management procedures must be implemented for user registration, modification and de-registration on all DWP information systems.

These procedures must also include processes for monitoring redundant and inactive accounts.

All additions, deletions, suspensions and modifications to user accesses should be captured in an audit log showing who took the action and when.

These procedures shall be implemented only by suitably trained and authorised employees.

Access control standards must be established for all information systems, at an appropriate level for each system, which minimises information security risks yet allows the organisation’s business activities to be carried out without undue hindrance.

A review period will be determined for each information system and access control standards will be reviewed regularly at those intervals.

All access to DWP information systems must be controlled by an approved authentication method supporting a minimum of a user ID and password combination that provides verification of the user’s identity.

Users will normally be limited to only one user account for each individual information system for non-administrative purposes. Any variations from this policy must be authorised by the Senior Responsible Owner (SRO) or, where applicable, the Authority.

All users shall have a user ID for their sole use for access to all computing services. All individual user IDs must be unique for each user and never duplicated.

All user accounts that have not been accessed for an agreed period, without prior arrangement, must be automatically disabled.

All administrator and privileged user accounts must be based upon job function and authorised by the SRO or, where applicable, the Authority, prior to access being given.

All changes to privileged accounts must be logged and regularly reviewed.

Procedures shall be established for all information systems to ensure that users’ access rights are adjusted appropriately, and in a timely manner, whenever there is a change in business need, a user changes their role, or a user leaves the organisation.

Users’ access rights will be reviewed at regular intervals no longer than annually.

Access to systems by individual users must be authorised by their manager or where applicable, the Authority.

Password Management

Passwords must not be shared with any other person for any reason.

All default system and vendor passwords must be changed immediately following installation.

All DWP information systems must support strong password management techniques (such as: length, complexity, aging, history, account lockout).

All DWP information systems must technically force new user accounts to change the initial password upon first use to a strong password, after which users must change their passwords on indication or suspicion of compromise.

Monitoring User Access

Systems will be capable of logging events that have a relevance to potential breaches of security.

User access will be subject to management checks.

Responsibilities

Senior Responsible Owner (SRO)

SROs are responsible for ensuring that the requirements of this policy are implemented within any programme, projects, systems or services for which they are responsible.

The SRO is responsible for ensuring that a robust checking regime is in place and complied with to ensure that legitimate user access is not abused.

The SRO may delegate responsibility for the implementation of the policy but retains ultimate accountability for the policy and associated checking regime.

Any non-compliance with this policy must be supported by a documented and evidence based risk decision accepted by the SRO.

Managers

Managers are responsible for ensuring that members of their team have the minimum levels of access to systems they need to perform their job.

They must authorise the access rights for each individual team member and keep a record of the latest access permissions authorised.

Managers should ensure that the access rights of people who have a change of duties or job roles or left the organisation are revoked immediately and that any access tokens (smartcard/USB dongle) are recovered.

All Managers should review the access levels of their people to ensure they are appropriate.

IT Support Teams

IT Support Teams are responsible for granting access to systems as described in local work instructions or use of Role Based Access Controls Matrix in accordance with the relevant procedures.

IT Support Teams must evaluate and, if necessary, challenge authorised access to help identify any obvious anomalies in the access levels granted or requested.

Users

Users must only use business systems for legitimate use as required by their job and in accordance with the procedures for those systems.

Compliance

Compliance against this policy will be assessed regularly.

Any violation of this policy must be investigated and may result in disciplinary action being taken.