Access Control Policy

Last updated: November 2023

1. Overview

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

2. Purpose

The purpose of this policy is to define how new users are authorised and granted appropriate privileges. This includes how users are reviewed and revoked when necessary, and includes appropriate controls to prevent users obtaining unauthorised privileges or access.

3. Scope

This policy applies to:

- All employees, third parties and suppliers who have access to our data and information systems.
- Information systems and services in all business areas.

There are some access roles that require stronger controls than those of standard users.

4. Policy

Definitions

Users

This is the collective term used to describe those who have access to the information and information systems, 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, data, computer system or application. The privileged user 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.

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 information systems.

These procedures must also include processes for monitoring active, 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, when and to what.

These procedures shall be performed only by suitably trained, certified and/or authorised employees.

Access control standards must be established for all information systems, at an appropriate level for each system. This 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 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 InfoSec Team.

All users will 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 a previously 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 InfoSec Team.

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.

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

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

The InfoSec Team 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 Data Protection Officer 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 Data Protection Officer.

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. Managers must also ensure that any access tokens (smartcard/USB dongle) are recovered.

All managers should review the access levels of their people to ensure they’re appropriate.

IT support teams

IT support teams are responsible for granting access to systems as described in local work instructions. This also includes the 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.

5. Policy Compliance

Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the Infosec Team in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

None.

7. Definitions and Terms

The following definition and terms can be found in the Cloudoko Glossary.

- Data Protection Officer
- Access Control
- Role Based Access Control
- Smartcard

8. Revision History

Date of Change	Responsible	Summary of Change
November 2023	Kevin Boldy	Initial Version

www.cloudoko.com