Document number: OC.2
Document Name: Access Control and Identity Management Policy
Document Owner: Operations Director
Issue Date: 01/05/2024
Current Revision Date: 01/05/2024

Access Control and Identity Management Policy

Objective and Scope

Prevision Research shall prevent unauthorised access to information systems and the associated applications in order to protect the information they contain.

This document prescribes how access is restricted and controlled including the use of privileged utility programs and access control over general information, and the protection of source code.

The scope of this policy is restricted to applying user access control and identity management principles.

Roles, Responsibilities and Authorities

The Operations Director shall set the principles for access control and monitor compliance to the principles through authorised monitoring and audits.

Individuals have an obligation to follow the policy directions and report any suspected misuse of or interference to their access privileges to an IT delegate or ISMS representative.

Where an exception or deviation from an expectation or plan occurs, the senior assigned role shall make the determination in terms of what is an acceptable change. The change management process may need to be enacted.

Legal and Regulatory

Title	Reference
Data Protection Act 2018	https://www.legislation.gov.uk/ukpga/2018/12/contents
General Data Protection Regulation (GDPR)	https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
The Telecommunications (Lawful Business practice)(Interception of Communications) Regulations 2000	www.hmso.gov.uk/si/si2000/20002699.htm
Computer Misuse Act1990	www.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm
The Privacy and Electronic Communications (EC Directive) Regulations 2003	www.hmso.gov.uk/si/si2003/20032426.htm
Criminal Law Act 1967	https://www.legislation.gov.uk/ukpga/1967/58/introduction

ISO 27001/2 REFERENCES	ISO 27001: 2013 Clause ID	ISO 27002: 2013 Annex A ID	**ISO 27001: 2022 Clause ID**	**ISO 27002: 2022 Control ID**
Access control		9.4.1		5.15
identity management		9.4.2		5.16
Password management / Authentication information Refer Password Protection Policy		9.4.3		5.17
Access rights				5.18

Access Control and Identity Management Policy

Related Information

- Password Protection Policy - includes Authentication information
- Data Breach Notification - IS Incident documents
- Information Classification Policy
- Disciplinary Procedure

Policy

Prevision Research shall ensure only authorised users have access to the information and systems they need when they need it, and that all others are prevented from gaining access to information and information systems.

Access to information and other IS risk related assets should be restricted in accordance with the established topic-specific policy on access control.

Users are held accountable for the security of their access and are required to ensure their authentication is safeguarded.

Information access restriction principles

Access control to software platform applications and secure information is based on the following principles:

- Security requirements of the applications systems and sensitive information
- Information classification of the individual user and their role within the company or externally
- Users ‘need to know and need to use’ principle
- Legislative implications including jurisdictional issues
- Network access rights across the whole of the network - consistency
- Segregation needs - authorisations and access administration to ensure data security and integrity is maintained
- The use of configuration mechanisms to control access to information in systems, applications and services
- Special one off or periodic needs - includes compliance reviews/audits
- Privileged access rights provided for scheduled works and design / development
- Refusal of access to sensitive information by unknown user identities or anonymously
- Removal of access rights when no longer required or in the case of suspected misuse

Above all else, access is assessed on the basis of ‘everything is forbidden unless expressly permitted’.

Access Control and Identity Management Policy

Identity management

Unique identification of individuals and systems accessing information shall be assigned in a manner that assures each person is an entity unto themselves within the system and is held accountable for maintaining their unique identity.

Shared identities are special circumstance situations only, to be approved by the Operations Director.

Removal of identities on termination or when the need is no longer required must be undertaken in a timely manner.

Refer to Password Protection Policy for password complexity, rules and updates. Records of events involving identity theft, loss or corruption shall be recorded as an Incident.

Secure log-on and creating user access procedure - also refer Password Protection Policy

On appointment and signing an employment agreement or contract to work, access controls will be set and tested by the IT delegated person issuing access control.

When roles and responsibilities change, or when termination of employment or vendor contract occurs, access controls will need to be changed or removed. This is under joint control of the line manager and IT delegated person who will jointly determine and approve any variation to scope, access levels or confirm access removal.

For high security access roles, authentication information plus authentication factors (2FA) for accessing critical information systems is required.

When assigning access to both infrastructure services (email, active directory logins) and application services a user ID is created that provides the necessary ‘need to know’ access:

- A User ID shall only be assigned to persons whose role requires access, confirmed by their line manager before requesting access.
- The person assigned the User ID is responsible for all tasks carried out under the User ID.
- User IDs will be set to expire at the end of contract date or after a specified period of time.
- Exceptions will only be considered when there is a clear business case, the request is submitted for approval in writing (email) and approved by the line manager and IT delegated person.
- Before receiving the User ID, as a condition of access, the user must be made aware of the company's privacy and information security policies, the password policy and have completed appropriate induction (employee or supplier/vendor).
- For security purposes, when users log-in the ID and password shall not be displayed.
- Help messages are not provided during log in.
- Monitoring login attempts and locking out after several attempts with a security alert initiated.
- After 5 attempts with a failed username and password, the user is logged out for 30 minutes and an alert is raised in the event log.

Monitoring and review of user access rights

Monitoring systems security shall include:

Access Control and Identity Management Policy

- a history of logins that are both successful and unsuccessful (date/time/device)
- an incident event is logged/raised when a potential login breach is attempted (date/time/device)
- terminate inactive sessions after an agreed period of 5 minutes.

User access privileges need to be monitored to ensure they remain relevant and current to needs.

Reviews by the Operations Director shall be conducted at least 6 monthly to confirm:

- Individual roles have remained the same - employees and vendors remain with the company i.e. employment or vendor contracts have not been terminated or otherwise changed
- any specialist privileges afforded remain relevant
- user behaviour (identified through event or other security monitoring) remains acceptable

Policy review

This policy shall be reviewed by the policy owner annually or immediately after a process change or a policy breach is known to have occurred. Refer below for the most recent review.

History table

Date	Rev No	Changes	Reviewed By	Approved By	Training Y/N