System and Application Access Management Policy

Objective and Scope

Prevision Research shall prevent unauthorised access to information systems (development and operating) 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 principles to organisational processes, technology and personnel. It ensures user-access risks are mitigated while still enabling access to information on a need-to-know basis when required.

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
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**
User endpoint devices				8.1
Access rights to privileged programs				8.2
Information access restriction		9.4.1		8.3

System and Application Access Management Policy

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 to program source code		9.4.5		8.4
Secure log in		9.4.2		8.5
Use of privileged utility programs		9.4.4		8.18

Related Information

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

Policy

The 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.

Lifecycle access management

Lifecyle access management includes data creation, processing, storage, archive, transmission and disposal.

Access principles are established for dynamic access based on device ID, location and application taking into account the user classification of information criteria.

Operational support systems are in place including monitoring and reporting processes and technical infrastructure.

General management systems for issuing access (authentication processes), encryption of PII or other highly sensitive information, monitoring usage and alert notifications.

System and Application Access Management Policy

Information and other assets access controls

The need for access to information and information systems is determined by the information and systems owner having undertaken a risk assessment to clarify risk aspects and impacts. the following access restriction principles are then applied.

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’.

Protecting high value sensitive information

Dynamic access management techniques and processes shall be considered when:

- there is a need to share highly sensitive information with individuals or organisations outside of the company security framework
- there is a need to dynamically change in real time the use and distribution of such information
- granular control over access provisions is necessary and/or advisable
- the need for specific protection against unauthorised changes, copying, printing or other exposures is necessary
- traceability of change and activity management for future investigation is required

User endpoint devices

Information stored on, processed by or accessible via an endpoint drive shall be protected by:

- Device security
- Restriction on software installation

System and Application Access Management Policy

- Controlled software updates and patches in a timely manner
- Limitations of use via public networks
- Encryption if approved by the Operations Director
- Remote disabling and lock out capability

Monitoring and review of user access rights

Monitoring systems security shall include:

- 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 15 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

Network service use and security

The Operations Director shall manage the functionality of and access to internal and external network connections including user rights (as per above). Ensure network services on systems are disabled unless a specific business reason for the service is required and can be justified (project, job role or business case).

Risks associated with the network service must be considered and resolved prior to implementation of any network service.

Network access includes:

- authorisation for access and access levels (which elements of the network can be accessed) ,
- controls necessary to protect the network, and
- means of network access allowed.

Use of privileged utility programs and access rights of privileged programs

The use of utility programs capable of overriding system and application controls are strictly controlled by the Operations Director.

Privileged access programs and the rights of use are generally admin accounts used by IT staff to perform maintenance on workstations, servers, network devices, databases, mainframes and special projects.

These are restricted to roles with specific needs, for a limited time and only as authorised by the executive team.

Passwords associated with operators using utility programs and privileged access rights shall be held in 1Password as a high security access control measure. Network access credential (secure shell) key access is secured with the use of public/private keys.

System and Application Access Management Policy

The need for authentication and authorisation for utility programs access is mandated and under approval control of the Operations Director. Segregation of network communications for utility programs from application software is practiced.

Key passwords are stored online via the Prevision Research secure password manager 1Password.

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