Password Protection Policy incl information authentication

Objective and Scope

Password protection is the security process that protects information accessible via computer devices that needs to be protected from unauthorised users.

The objective of this document is to provide clear direction and rules for the management of passwords including password development, protection and change control. This supports the allocation and authentication of information including advising personnel on the appropriate handling of authentication information.

Passwords or pass-phrases are often the first line of information protection and defence against unauthorised intrusion. They are only as effective as they are robust.

The scope of this policy includes the use of passwords in all circumstances related to information and data security whether protecting the whole network, a single device or any electronic system containing, receiving or transmitting secure information. This applies to any Prevision Research employee, vendor or any other individual afforded secure access to Prevision Research IT facilities, secure networks or devices.

Roles, Responsibilities and Authorities

The Operations Director shall set the rules for password management and monitor compliance to the rules through authorised monitoring and audits.

Individuals have an obligation to follow the policy directions and report to an IT delegate or ISMS representative any interference with or unauthorised use of their password immediately it is suspected.

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. Change management 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**
Password management system /Authentication of information		9.4.3		5.17

Password Protection Policy incl information authentication

Related Information

- Access Control and Identity Management Policy
- Data Breach Notification
- Information Classification Policy
- Disciplinary Procedure

Allocation of authentication information

The Prevision Research requires the following minimum standards applicable to the authentication of information to be followed:

- Personal passwords or personal identification numbers (PINs) shall be allocated and meet minimum complexity and review standards (Password Protection Policy)
- The verification of user identity shall be undertaken prior to providing new, replacement or temporary authentication information or devices
- The transmission of authentication information shall be transmitted to users in a secure manner including users acknowledgment of receipt of the authentication information (password)
- Vendor authentication information shall be periodically reviewed and updated
- Allocation of authentication information for special events or emergencies shall be controlled and a record kept of such activities including the removal of access in a timely manner

Password Protection Policy

The Prevision Research requires the use of strong (quality) passwords or pass-phrases by any individual or group (Committee) who access, use, or maintain electronic systems that contain, transmit, receive, or otherwise use or display PI or business sensitive information. The rules and standards outlined in this document are mandatory and as password security is critical to organisational security, a breach of this policy may result in disciplinary action or contract termination.

Strong password (pass-phrase) development rules - applies to all password use

Passwords must be strong (quality) passwords. This is defined as a password that is reasonably complex, difficult to guess in a short period of time either through human guessing or the use of specialized software. A pass-phrase is considered a form of password and fits within the same development principles.

As a minimum, a strong password or pass-phrase shall include:

- 8 characters as a minimum that do not form a name, word, slang or dialect e.g. nXp#pd8tUqz
- 12 or more characters if using a mixed phrase e.g. fixdoGbig$orrynot
- Mix of upper/lower case character - English A- Z
- At least one numeric character - 0 - 10
- At least one non-alphabetical character e.g. # % $

What NOT to do with passwords

- Use family names

Password Protection Policy incl information authentication

- Reuse passwords in full or part
- Use short passwords are too easy to deconstruct
- Use birth dates or other personal information such as a phone number
- Use words spelled backwards
- Use patterns such as double digits e.g. aaxxrrjj2233

Password management standards

- Store passwords online via the Prevision Research secure password manager 1Password.
- Never write down passwords on paper, post-it notes or in unprotected electronic files. Do not reuse a password.
- Do not use the same password for more than one platform.
- Do not allow passwords to be displayed as the password is being entered.

Password change management requires frequency of change according to risk as follows:

Domain password age:	Replace every 90 days.
Email password age:	Replace every 90 days.
Low risk password age:	Replace every 90 days.

New accounts and first time users

As a new employee and a first-time password user, new staff are issued passwords that are generated by the Operations Director and are unique for initial entry only.

Once the user has logged into the system, change the password.

Once users are terminated, access is immediately withdrawn and all passwords revoked by the Operations Director.

Access to high risk systems requiring passwords

Systems with high security level (core data) access provided on a need-to-know basis for essential use only. These passwords MUST be encrypted and stored in the Prevision Research secure password manager 1Password.

The password lifecycle of highly restricted systems is limited to monthly after which the password can never be used again.

Password sharing

Sharing of passwords is not allowed and considered a breach of information security except in exceptional circumstances. Exceptional circumstances shall be approved by the Operations Director.

EXAMPLE: Client request:

> A client or an authorised agent of a client formally requests system data not containing sensitive information be sent to them through a secure tool or portal provided by them. The password protected encrypted file may then be forwarded accordingly and only to the approved, authorised requester. When sending the password, it should be sent via a known mobile number or email address once the requester has been informed that it is on its way.

Password Protection Policy incl information authentication

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.

Periodic reviews shall take into account feedback from management reviews, regulatory changes and audits. Changes to the policy must be approved by a senior executive then communicated to all previous persons or organisations with access to the policy. Refer below for the most recent review.

History table

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