# Cryptography Policy

## Objective and Scope

Cryptographic control is used for the protection of Prevision Research information and software assets and other classified or sensitive information.

The objective in using cryptography is to protect the confidentiality, integrity and availability of the Prevision Research secure electronic data.

The scope of cryptography is determined after a risk assessment identifies the need and level of cryptographic controls taking into consideration confidentiality, integrity and authenticity of information security needs and regulatory limitations of cryptography.

## Roles, Responsibilities and Authorities

Overall ownership of responsibility for decisions relating to cryptography is assigned to the Operations Director.

Where an exception or deviation from this role is required, the senior assigned role shall make the determination in terms of an alternative. The Change Management Procedure may need to be enacted.

## Legal and Regulatory

| Title | Reference |
|---|---|
| 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 |
| The Freedom of Information Act 2000 | https://www.legislation.gov.uk/ukpga/2018/12/contents |
| Online Safety Act 2023 | https://www.legislation.gov.uk/ukpga/2023/50/contents/enacted |
| 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** |
|---|---|---|---|---|
| Cryptography | | 10.1 | | 8.24 |
| Regulation of cryptographic controls | | 18.1.5 | | 5.31 |

## Related Information

- ISMS Framework and supporting procedures

# Cryptography Policy

## Policy

Prevision Research shall use cryptography to protect confidentiality, authenticity and integrity of information after having risk assessed the needs and taking into account regulatory limitations of cryptography use. Cryptography should never be the only source of data protection considered, it is strongest when supported by other data protection mechanisms. Therefore, cryptography is not a single solution.

### Risk assessment

A risk assessment shall be undertaken to determine the need and legal obligations of using cryptography as a risk mitigation tool. The following risks shall be considered:

- Criticality of the secure or sensitive information to be protected and options for its security other than encryption.
- The ability to unlock the information and reinstate it in a timely manner if required by law.
- Risk of reliance solely on encryption as the only source of protection. If an encrypted system does not have as many other controls placed around it, the vulnerabilities may be more exposed.
- Key management - loss of a key. Prevision Research manages key security through the use of a dedicated electronic key management system under the control of Operations Director.

### Use of cryptographic controls

Cryptographic controls shall be considered for use in the following circumstances:

- Confidentiality
  Using encryption of information to protect sensitive or critical information, either stored or during transmission
- Integrity/authenticity
  Using digital signature certificates or message authentication codes to verify authenticity or integrity of stored or transmitted sensitive or critical information
- Non-repudiation
  Using cryptographic techniques to provide evidence of the occurrence of an event or action so it cannot be denied
- Authentication
  Using cryptographic techniques to authenticate users and other system entities requesting access or transacting with system users, entities and resources

### Key management

When using cryptography to protect digital assets and communications the cryptography is only as effective as the security of the cryptographic keys.

Prevision Research may use:

1. Symmetric keys to encrypt bulk data
2. Private keys with asymmetric algorithms

# Cryptography Policy

3. Hash keys to safeguard the integrity and authenticity of data and transactions with algorithms

Keys must never be stored alongside the data that they protect (e.g. on a server or database).

Prevision Research uses a dedicated electronic key management system managed by Operations Director.

## Regulation of cryptographic controls

Cryptographic laws fall into four main categories:

- Import controls, which is the restriction on using certain types of cryptography within a country.
- Export control, which is the restriction on export of cryptography methods within a country to other countries or commercial entities.
- Patent issues, which deal with the use of cryptography tools that are patented.
- Search and seizure issues, on whether and under what circumstances, a person can be compelled to decrypt data files or reveal an encryption key.

Jurisdictional laws within the ISMS operational scope must be known and observed including those laws that enforce access to encrypted information by a regulatory body. This will influence when encryption can be used. The Operations Director must agree to the intended encryption use.

## 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 |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |