Compliance Management Policy

Objective and Scope

The objective of this document is to outline the various aspects of compliance management in order to:

- ensure documented systems are in place to avoid breaches of legal, statutory, regulatory or contractual obligations, and
- ensure that information security is operationally effective in accordance with the documented ISMS system in compliance with ISO 27001.

The scope of this policy also covers aspects of compliance contained in:

- Legal and Contractual Requirements Policy and Register
- Technical IS Reviews Procedure
- Cryptography Policy
- Document, Data Control and Records Management Procedure
- Privacy Policy
- Information Security Policy
- Internal Audit and Auditing Procedure

Roles, Responsibilities and Authorities

The Operations Director or competent delegate takes ownership of systems and regulatory compliance.

This role is supported by the delegated role and responsibilities as stated in the support policies and procedures listed in the scope of this document.

Legal and Regulatory

Refer to the Legal and Regulatory Register for a comprehensive list

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**
Performance evaluation	9.0			
Legal and contractual		18.1		
Identification of applicable legal and contractual requirements		18.1.1		5.31
Intellectual property rights		18.1.2		5.32
IS Reviews		18.2		
Protection of records		18.1.3		5.33

Compliance 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
Privacy and protection of PII		18.1.4		5.34
Regulation of Cryptographic controls		18.1.5		5.31
Independent review of IS		18.2.1		5.35
Compliance with security policies and standards		18.2.2		5.36
Technical reviews		18.2.3		5.36 I 8.8

Related Information

As listed in the scope statement plus ISO 27001.

Policy

The Operations Director plans and manages compliance to the internal ISMS system, regulations and ISO 27001. This is an integrated process involving other support procedures with assigned roles and responsibilities as described in the reference documents below. Refer to these documents for more detailed information.

Legislative and contractual requirements

Refer: Legal and Contractual Requirements Policy and Register

Applicable legal requirements shall be identified across the scope of the organisation's activities. This includes global and regional jurisdictional considerations for legislative obligations in relation to information and cyber security and the protection of personal information of individual persons.

A Legal and Regulatory Register shall be maintained and contain, as a minimum:

- List of legislation and/or regulations and/or Article or Code reference relating to any obligation in relation to cyber security, information, data security or privacy of personal information
- Legal/regulatory document name e.g. General Data Protection Regulation EU (GDPR)
- Jurisdiction covered by the legislation such as country, state or region
- Authority enacting the applicable legislation
- Registration requirements - are you required to register with the authority?
- Obligation to provide a competent person to oversee the legislative obligations
- Scope of the legislation as it relates to data collection, processing and transfer of personal information
- Data security obligations as it applies to the scope of company activities
- Breach notification obligations as it applies to the scope of company activities

Assignment of responsibilities to develop and maintain the register sits with the relevant information technology (for cyber security) or privacy officers (for personal information).

Compliance Management Policy

The register shall be reviewed annually and also when known changes to legislation or business operations occur, including additional services or operational jurisdictions expansion.

Cryptography

Prevision Research reviews the use of cryptography for special projects and contracts to ensure the needs and expectations of regulators including jurisdictional responsibilities and limitations plus the client are being met.

Contracts

Prevision Research shall instruct all parties entering into agreements with Prevision Research of the obligations of all parties in relation to information security. These obligations shall be documented as part of any contract or agreement.

Intellectual property rights

Refer: Legal and Contractual Requirements Policy

Intellectual property rights include software document copyright, design rights, trademarks, patents and source code licences.

Copyright: Intellectual property rights at Prevision Research is addressed, taking into consideration:

- the ownership and management of intellectual property developed by the company in the course of business activities
- the rights of intellectual property of those products and copyright material that are used in the course of business.

Prevision Research senior management shall maintain a list of intellectual property and copyright licences including databases, designed computer programs and other materials: Software List

The copyright licence and mark is displayed on all associated materials distributed by the company.

Use of proprietary software applications

Prevision Research uses proprietary software under license (copyright) user agreements that declare limits of use, distribution and modification imposed by the product owner. Software applications and user agreements are held in a list/register by the Operations Director and monitored to ensure the end-use agreement defined conditions are not breached.

Compliance Management Policy

Protection of records

Refer: Document, Data Control and Records Management Procedure

All records required for business and ISMS purposes shall be protected from loss, destruction, falsification, unauthorised access and unauthorised release.

Electronic records are protected from loss, unauthorised access or release, or unplanned destruction through the following protocols:

- Clear Desk and Clear Screen Policy
- The use of portable media devices is NOT permitted for holding records. Refer Media (Document and Information Handling) Policy.
- The need for cryptographic control of records shall be considered, taking into account risks to highly classified information. Cryptographic keys shall be stored under the control of the Operations Director.
- Stored records are protected from corruption using Windows Defender & Malwarebytes and are stored such that retrievability is timely.
- To enable archived records to be reinstated should the need arise, old versions of software shall be retained by the Operations Director to enable records management to cope with future technology advances.

The methods of storage and handling whether electronic, hard copy or other media shall ensure identification of each record and of the retention period taking into consideration contract, legislative and business needs. Destruction of records after this time is undertaken systematically to ensure the economy of space is considered.

Privacy and protection of personally identifiable information PII

Refer: Privacy Policy

Prevision Research collects personal information about a person when an individual provides such data directly to the company, or when personal information is automatically collected in connection with the use of the company website or Prevision Research services. Personal information Prevision Research collect directly from you may include:

- name, residential address, occupation, email or telephone
- contact details
- opinions and reactions, including your personal experience
- bank account or financial details
- usernames for third party services

Some personal information is automatically collected when you use Prevision Research website, such as

the following:

- IP address and device identifiers
- web browser information

Compliance Management Policy

- page view statistics and browsing history
- usage information
- cookies and other tracking technologies (e.g. web beacons, pixel tags, SDKs, etc.); and
- log data (e.g. access times, hardware and software information).

Refer: Information Security Policy

Prevision Research applies a consistent, risk-based approach to information security that maintains the confidentiality, integrity and availability of information. It does this by protecting information against unauthorised disclosure, access or use, loss or compromise (malicious or accidental), or a breach of privacy. This includes identifying and managing risks to information, applications and technologies throughout their lifecycle by implementing and maintaining an ISMS in compliance with the ISO 27001.

Regulation of cryptographic controls

Refer: Cryptography Policy

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.

Information systems audit considerations

Refer: Internal Audit and Auditing Procedure

Prevision Research provides a program of internal audits to verify compliance to ISO 27001 and the ISMS Framework. Competent auditors shall undertake the audit and provide an audit report to interested parties. Departments and locations within the organisation shall cooperate with the audit program and auditor requests.

In addition to the program of planned audits, additional unplanned audits may be undertaken after an incident or breach, or other high risk information security event. Rules of audit other than pre-scheduling still apply.

Planning the audit schedule is the role of the ISMS Representative, in consultation with organisational management.

The use of third party auditors for internal audit processes is useful when the technical expertise necessary for informed decision making is not available internally, or cannot be found independent of the activity being audited.

Compliance Management Policy

Independent review of information security

Refer: Technical IS Reviews Procedure

Independent reviews of information security is managed through:

1. Internal audits - ISMS Representative
   The internal audit schedule shall incorporate audits of the controls
   These are undertaken by internal auditors independent of the work activities.
2. Incident reports and IS breaches - Data Protection Officer
   Incident reports related to information security shall be subject to an unplanned audit to determine causal analysis and identify improvement opportunities. This occurs whether or not a formal regulatory breach notification is issued.
3. Penetration testing of SaaS providers for the purposes of identifying IS risk and vulnerability

Reporting of the above is made to management as part of management reviews and general operational performance meetings.

Compliance with information security policies and standards

Refer: Technical IS Reviews Procedure

Each jurisdiction within the organisation has an obligation to ensure they assign a competent internal auditor to audit operational processes against the ISMS internal standards.

This is initiated separately from the ISMS planned audit program. When a local internal auditor is not available, or on agreement from the ISMS Representative, this can be integrated into the full organisational program.

Technical reviews

Refer: Technical IS Reviews Procedure

Independent reviews of information security is managed through:

1. Internal audits - ISMS Representative
   The internal audit schedule shall incorporate audits of the controls
   These are undertaken by internal auditors independent of the work activities.
2. Incident reports - IS breaches - Data Protection Officer
   Incident reports related to information security shall be subject to an unplanned audit to determine causal analysis and identify improvement opportunities. This occurs whether or not a formal regulatory breach notification is issued.

Reporting of the above is made to management as part of management reviews and general operational performance meetings.

Technical compliance is reviewed through a series of automated monitoring and testing tools and reported through reports generated by the process.

Compliance Management Policy

1. Penetration testing - IT Delegate
   Penetration testing, whether initiated by the company or by a client, shall be considered as part of the overall information security systems review process
2. Event logging and monitoring of software applications and network devices - IT Delegate
   Logs are monitored to identify exceptions or anomalies and act to determine the nature of the issues.
3. Technical vulnerability management - IT Delegate
   Assessments of technical vulnerabilities are performed on critical assets including routers, access points, firewalls and operating system servers.

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