Information Classification Policy incl acceptable use

Objective and Scope

Information classification is a process by which Prevision Research assesses data and assigns a level of protection it shall be given.

The objective of this policy is to ensure that Information classification is documented and followed to ensure an appropriate level of information and asset protection, in accordance with its importance and sensitivity to the organisation and information owners.

The scope of this policy includes risks in relation to legal considerations, information value to the organisation, sensitivity and criticality in terms of unauthorised disclosure or modification.

Roles, Responsibilities and Authorities

The Operations Director takes ownership of creating and assigning information classification standards.

Individuals shall be responsible for managing and following the information classification and security of the information they handle and report any suspected breaches to management immediately they are known.

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
Health and Care Act 2022	https://www.legislation.gov.uk/ukpga/2022/31/contents/enacted
The Telecommunications (Lawful Business practice)(Interception of Communications) Regulations 2000	www.hmso.gov.uk/si/si2000/20002699.htm

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
Classification of Information		8.2.1		5.12
Labelling of Information		8.2.2		5.13
Handling of assets		8.2.3		5.10

Related Information

- Mobile Devices Policy
- Physical (Equipment) Asset Management Policy (including maintenance and acceptable use of physical assets)

Information Classification Policy incl acceptable use

Policy

Prevision Research has a responsibility to protect the information that it creates and collects, uses and records. The level of protection provided depends on the nature of the information collected, its legal obligations and the importance and sensitivity of the information.

Prevision Research assets that hold or otherwise are subject to exposure to sensitive information are also subject to classification controls. Refer to 'Physical (Equipment) Asset Management Policy'.

Access to information is provided to staff and third parties to allow them to undertake their day-to-day activities. It is recognised that there is an underlying need to facilitate ongoing sharing of information where appropriate, however this must be within the standards set out in this document. Any information created becomes a record and is managed according to its risk classification.

Classification of information

The information classification scheme is developed through a risk assessment of sensitive information based on confidentiality, integrity and availability (CIA) criteria plus the need to consider risk of harm to individuals, operational issues or significant business integrity loss.

Classification criteria should:

- provide a concise instruction on how to handle and protect data
- specifically apply the classification to groups of information rules to reduce the need for a case-by-case risk assessment

Information classification standard

Information, whether electronic or hard copy, shall be nominated as per the classification, noted in document footer (optional) and held or stored as specified.

PUBLIC CLASSIFICATION

Public classification is general access information and can be made available externally. There is no risk of harm to the company, clients or individual by providing the information.

BUSINESS USE ONLY

Business use only classification applies to information used only within the business, however will not cause adverse effects should it be unintentionally disclosed, modified or destroyed. This is generally internal information of the company and not client information.

CONFIDENTIAL CLASSIFICATION

Confidential classification applies to sensitive information such as intellectual property, personal identifiable information, contractual and client-related information and any other that is protected by law.

The unauthorised disclosure, modification or destruction of such information would adversely affect the organisation, a client or individuals.

Access to confidential classified information is limited to authorised persons only with signed confidentiality declarations or confidentiality clauses in their employment contract. Consider the need for encryption of confidential classified information.

Information Classification Policy incl acceptable use

HIGHLY CONFIDENTIAL CLASSIFICATION

HIGHLY confidential classification is considered to be access to source data, however it may be the case in some contractual and client project work where data loss has significant legal repercussions. Such data could be records where loss or vulnerability could cause serious legal ramifications putting the business, industry, client and individuals at risk.

This level of information must be limited to authorised persons with confidentiality declarations or clauses in their contracts or signed NDAs) and retained in-house unless authorised by the Operations Director).

Highly confidential classified information requires either encryption or two factor authentication access to electronic files.

Labelling of information

Labelling must be practical and effective for ease of use.

Electronic data can be labelled via folder naming, or embedded in electronic documents such as footers/headers nominating information classification status. This shall remain when in printed format.

Metadata is used as a summary tool in order to make tracking easier for data providing information about multiple aspects related to data.

Physical assets are only subject to a tag or other form of hard labelling if they are exposed to secure or sensitive data use. USB sticks should only be used for general use of nonsensitive data.

Acceptable use of information and other assets

Personnel including third party users shall follow standard protocols in using information:

- Only use information and information assets for the purpose for which it was provided
- Respect the access restrictions supporting the protection requirements for each level of classification
- Do not replicate or duplicate data for any purpose other than that approved for the particular work case
- Do not communicate the contents of information being handled to other persons or organisations unless there is a business case to do so
- Respect and protect temporary copies of information to a level consistent with the protection of the original information

Communicating and storage of information assets

Public classification and business only classification do not require any specific security controls for the handling of assets as they are not content sensitive.

Confidential Classification requirements:

- Do not use confidential hard copy documents for recycling or reuse purposes.
- Hard copy or electronic documents cannot be replicated in any way without permission of the document owner. If replication does occur, the same level of security applies to the replicated version as does the original.

Information Classification Policy incl acceptable use

- Documents may be emailed only with permission and through secure signature on receipt. This trail must be traceable and auditable.

Highly Confidential Classification requirements:

- NEVER use highly confidential documents for recycling or reuse purposes.
- Highly classified documents must not be replicated without permission of the document owner or company executive. If replication does occur, the same level of security applies to the replicated version.
- Document drives holding highly confidential information shall be subject to authentication access by username and password that restricts access to files. This must be approved by a company executive.
- Documents may be emailed only with executive permission and through encryption and secure signature on receipt. This trail must be traceable and auditable.

Suspected unauthorised disclosure or modification

Report any lost, damaged property, unauthorised access/use or suspected malware activity immediately to management. Provide details regarding likely impact on data security and effects on company or client information.

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