Information Security Policy

CORELAIN

3rd Floor, Cardinal House,
20 St Mary's Parsonage,
Parsonage Gardens,
Manchester, M3 2LY

Dawson House
5 Jewry Street
Aldgate
London EC3N 2EX

E office@corelain.com
W www.corelain.com
T 0161 820 1121
Company No. 14451716

Regulated by RICS

1. Introduction

CORELAIN LTD (hereinafter "the company") recognises that protecting the confidentiality, integrity, and availability of information is essential to maintaining the trust of its stakeholders and the continuity of its operations.

2. Purpose and Scope

This policy sets out the company's framework for managing information security and applies to all employees, contractors, and third parties with access to the company's systems or data. It covers physical and digital information across all departments and locations.

3. Roles and Responsibilities

The Directors have overall accountability for information security. Departmental managers are responsible for implementing security measures within their teams. All employees are responsible for adhering to this policy and reporting concerns.

4. Information Classification and Handling

Information is classified based on sensitivity into Public, Internal, Confidential, and Restricted categories. Each classification level dictates how information should be handled, stored, shared, and disposed of.

5. Access Control and Authorisation

Access to systems and data is granted on a need-to-know and role-based basis. Employees are provided access credentials appropriate to their role and must not share passwords. Regular reviews of access permissions are conducted.

6. Information Security Risk Assessments

Periodic risk assessments are performed to identify, evaluate, and mitigate potential threats to the company's information assets. Assessments consider physical, technological, and human factors and are reviewed annually or following significant changes.

7. Awareness and Training to Prevent Information Security Breaches

The company provides annual information security awareness training to all employees and contractors. The training includes topics such as phishing prevention, password protection, and secure data handling practices.

8. Whistleblower Procedure for Information Security Concerns

The company encourages stakeholders to report any suspected or actual breaches or risks related to information security. Reports can be made anonymously via the internal whistleblower channel and in accordance with our Whistleblowing Policy, with all submissions treated confidentially and investigated promptly.

9. Incident Response Plan (IRP) for Breaches of Confidential Information

An Incident Response Plan is in place to manage breaches of confidential information. The plan outlines roles, response steps, communication procedures, containment, and recovery processes. All incidents are logged and reviewed to prevent recurrence.

10. Records Management and Retention Schedule

The company maintains a formal records retention schedule which sets the required retention periods for each type of information and the secure destruction methods post-retention. Compliance with this schedule is monitored.

11. Third Party Data Protection Measures

The company ensures that third parties handling its data are subject to adequate information security controls. Due diligence is carried out prior to engagement, and data protection clauses are included in all supplier contracts:

- Vendor Screening and Selection: CORELAIN LTD conducts basic due diligence before engaging third-party vendors, focusing on data protection practices, data processing capabilities, and adherence to relevant data protection regulations (e.g., GDPR).
- Data Processing Agreements (DPAs): All third-party vendors with access to client or company data are required to sign a DPA that specifies data protection requirements, confidentiality clauses, and breach notification procedures.
- Access Control: Third-party access is granted on a need-to-know basis only, with data-sharing restricted to specific project requirements. Access permissions are reviewed periodically to ensure relevance and mitigate risk.
- Data Encryption: Data shared with third parties is encrypted using standard encryption protocols to protect data integrity during transmission and storage.
- Incident Reporting: Third parties are contractually obligated to notify CORELAIN LTD of any suspected or actual data breaches within 24 hours of detection, ensuring timely response and mitigation.

- Termination and Data Disposal: Upon contract termination or project completion, third parties must confirm data deletion in accordance with CORELAIN LTD's data disposal policy, with written confirmation of destruction where applicable.

12. Stakeholder Consent for Processing, Sharing and Retention of Confidential Information

The company obtains stakeholder consent before processing, sharing, or retaining personal or confidential information. Consent mechanisms are documented and reviewed for transparency and compliance with legal requirements.

13. Monitoring, Auditing and Review

Information systems are monitored for unusual activity. Internal audits are conducted annually to ensure policy compliance and the effectiveness of controls. Recommendations from audits are actioned and documented.

14. Breach Consequences and Disciplinary Measures

Employees found to be in breach of this policy may face disciplinary action, up to and including dismissal. Where breaches involve third parties, contracts may be terminated and legal action pursued if applicable.

15. Qualitative Objectives and Quantitative Targets

CORELAIN LTD is committed to continuous improvement in information security.

- Qualitative Objective: CORELAIN LTD aims to cultivate a culture of information security awareness and compliance throughout the organisation, ensuring all employees understand the importance of safeguarding data and act accordingly.
- Quantitative Target: By the end of 2025, CORELAIN LTD will ensure that 100% of employees in data-handling roles complete annual information security training. Additionally, the Company will conduct biannual internal audits of information security practices and reduce the number of information security incidents by 30% year-on-year.

16. Policy Review

This Policy will be reviewed annually to ensure that it continues to meet the Company's objectives and regulatory requirements. Any changes to the Policy will be approved by the Board of Directors.

17. Policy Queries

Any queries relating to this policy should be directed to the Compliance Officer.

This policy has been approved and endorsed by the Board of Directors and the Management. We believe that by adhering to these guidelines, we will make meaningful contributions to societal and environmental well-being.

Formalised and approved by the board of directors on **06 November 2025**

Signed:	Signed:	Signed:
		
Ian Chadwick (CEO)	Adrian Patel Director (Commercial)	James Pemberton Director (Technical)

Version control

Date issued	Version number	Date reviewed	Approved
23.10.25	V1.0	06.11.25	Adrian Patel