



Calcula Ltd Security of Information Policy

Introduction

Calcula Ltd is committed to ensuring the security and confidentiality of sensitive and personal information. This policy outlines the steps we take to protect the information we manage, including client data, employee records, and other business-critical information.

1. Information Security Objectives

Our primary objectives in managing information security include:

- Protecting information from unauthorised access or disclosure
- Ensuring the integrity and accuracy of data
- Maintaining the availability of information for authorised personnel
- Complying with legal, regulatory, and contractual information security requirements

2. Roles and Responsibilities

- The Information Security Manager (or designated staff member) is responsible for overseeing the implementation of this policy and managing information security efforts.
- All employees and contractors must follow the company's security procedures and report any security breaches or vulnerabilities immediately.

3. Information Classification and Handling

We classify information into the following categories:

- Confidential: Sensitive data such as client contracts, financial records, and personal data. This information must be securely stored and only accessible to authorised personnel.
- Internal Use: Information required for day-to-day operations that is not sensitive but should still be protected.
- Public: Information that can be shared freely without compromising the company's security.

4. Access Control

Access to sensitive or confidential information is granted based on the principle of least privilege, ensuring that employees and third parties only have access to the information necessary to perform their duties.

5. Data Protection and Encryption

- Personal and sensitive data must be stored and transmitted securely. We use encryption methods for data storage and during transmission (e.g., email encryption, encrypted drives).



- Any physical records containing sensitive information will be securely stored in locked cabinets or similar secure facilities.

6. Secure Communication

We require the use of secure communication channels for sharing sensitive data (e.g., encrypted emails, secure file-sharing platforms). Employees must refrain from sending confidential information through unencrypted email or other unsecured methods.

7. Regular Monitoring and Audits

We regularly monitor our IT systems for unauthorised access attempts, data breaches, or other security vulnerabilities. Two stage authentication is required for all new device log-ins.

8. Incident Response and Reporting

In the event of a security incident, employees must immediately report the breach to the Information Security Manager. A prompt investigation will take place, and appropriate steps will be taken to mitigate the impact, including notifying affected parties if necessary.

9. Employee Training and Awareness

All employees and contractors must undergo information security training. This ensures that they understand their responsibilities and the procedures for safeguarding company data.

10. Vendor and Third-Party Security

We require all third-party service providers and contractors to comply with our information security policies. Contracts with third parties must include provisions for data protection and security measures consistent with this policy.

11. Business Continuity and Disaster Recovery

We have established business continuity and disaster recovery plans to ensure that information can be recovered in the event of an incident or disaster that impacts the company's operations.

12. Review and Updates

This policy will be reviewed regularly and updated as needed to reflect changes in technology, legal requirements, and company operations.



Acknowledgment

All employees and sub-consultants are required to sign an acknowledgment that they have read and understood this policy.

Signature:



Signed by:

Liam M Perry

On behalf of: (Company)

Calcula Ltd

Date:

23/09/2025