INFORMATION SECURITY POLICY

Policy Purpose

Delton Contracts Services Ltd is committed to protecting the confidentiality, integrity, and availability of all information assets. This policy provides a framework to protect our data— whether electronic, physical, or verbal—from internal and external threats, ensuring business continuity and legal compliance.

Objectives

- The objective of this policy is to ensure that:
- Information is protected against unauthorised access.
- The confidentiality of information is maintained.
- The integrity of information (accuracy and completeness) is preserved.
- Information and vital services are available to users when required for business purposes.

Our Commitment

- To maintain high standards of information security, Delton Contracts Services Ltd shall:
- Comply with all applicable legislation, including the Data Protection Act 2018 and UK GDPR.
- Assign clear responsibilities for information security to defined roles within the company.
- Ensure appropriate technical and organisational controls are in place to safeguard data.
- Regularly monitor and review security risks and threats to ensure our systems remain effective.
- Provide regular training to all employees to ensure they understand their security obligations.
- Ensure that all subcontractors and third-party partners who handle company data abide by our security standards.

Training and Awareness

- **Induction:** All new employees receive training on information security and data protection as part of their induction process.
- **Ongoing Briefings:** Staff who handle sensitive personal or financial data receive regular updates and advanced training to mitigate the risk of data breaches.

INFORMATION SECURITY POLICY

Reporting Procedure

Delton Contracts Services Ltd encourages anyone who experiences or witnesses harassment to report it immediately.

- **Informal Resolution:** Where appropriate, individuals are encouraged to inform the harasser that their behaviour is unwelcome and should stop.
- **Formal Reporting:** If the behaviour persists or is of a serious nature, it should be reported to a Line Manager or a Director.
- **Whistleblowing:** For serious concerns where confidentiality is a priority, please refer to the company's Whistleblowing Policy.

Disciplinary Action

We maintain a zero-tolerance approach to harassment. Any employee found to have committed an act of personal harassment will be subject to disciplinary action, which may include summary dismissal for gross misconduct.

Responsibility

The Managing Director holds ultimate responsibility for the implementation of this policy. All employees are expected to comply with this policy and treat their colleagues with respect and dignity.

Document Name: INFORMATION SECURITY POLICY
Date Created: 01/01/2024
Version Number: 2 Jan 2026
Revision Date: 01/01/2027
Approved by: Gurbakhs Singh
Position: Managing Director

Approved by	G.Singh Director	Signed:	Date 6/3/2025