



CLIFFE PACKAGING LTD

Information Security Management Policy

Issue No: 2.0

Created Date: 15/06/2023
Contact Officer: Matt Dawber (QHSE Manager)
Latest Revision: 15/06/2024 (2.0)
Review Date: 15/06/2025

Document Title	Document Type	Issue	Page
Information Security Management Policy	Policy	2.0	2/4

1.0 Introduction

1.1 Purpose

Cliffe Packaging Ltd's corporate social responsibility (CSR) policy, along with other interrelating policies, self-imposes a requirement that it conducts business ethically and legally. Information security is a crucial aspect of CSR, with a duty to protect information which implicates interested parties and guarantee business continuity. Compliance with General Data Protection Regulation (GDPR) is also a critical part of information security, ensuring the business protects individual rights and freedoms.

This policy is intended to instruct those individuals within its scope on how their roles in the protection of information and data, whilst informing all interested parties—internally and externally—how Cliffe Packaging complies with its requirements.

This policy is incorporated into a wider business management system, rather than an Information Security Management System (ISMS) and, as listed within its measures, Cliffe Packaging employs third-party contractors to manage its information security controls and maintenance of information technology (IT) systems.

1.2 Scope

The scope of this policy includes all employees, interns and contractors of Cliffe Packaging Ltd. It is also intended to demonstrate how we protect information and data to our interested parties.

1.3 Principles

Our information security principles are determined by applicable laws and guided by the ISO/IEC 27001 standard and its corresponding guidance standards, although we do not operate an ISMS. Information security values are supported by three main principles:

- **Confidentiality:** Access to data assets must be limited to authorised individuals only.
- **Integrity:** Maintaining IT systems, ensuring they remain reliable and fit for purpose.
- **Availability:** Ensuring authorised users have access to relevant information or policies when necessary.

2.0 Objectives

Cliffe Packaging aims to:

- Comply with GDPR and other laws associated with information security.
- Educate and increase awareness of information security measures within our company.
- Implement controls, guided and managed by our third-party contractor, to reduce risk of damage, misuse, theft, loss or abuse of information and data.
- Protect all personal data and respond to incidents as quickly as possible.
- Ensure information is protected by physical controls (important for paper-based information storage).
- Use state-of-the-art preventative software.
- Ensure we can continue to operate in the event of a security incident.
- Have **100%** of staff complete an annual information security awareness training course.

3.0 Controls and Measures

Cliffe Packaging endeavours to meet its information security objectives with the following controls and measures:

Document Title	Document Type	Issue	Page
Information Security Management Policy	Policy	2.0	3/4

- Employment a third-party IT services provider, which develops and offers in-house security management software.
- The use of appropriate confidentiality levels on sensitive documents.
- Operating a Privacy Policy, which outlines how we process and store information from website visitors and for what purpose.
- Employees provide consent to their data being processed through acceptance and signing of a contract of employment, with which an employee handbook is issued, containing information on what we process and why.
- Providing annual training to all employees to promote awareness of information security and best practice.
- Assigns retention periods against information, which are recorded in appropriate registers.
- Requires users of the Cliffe Packaging network to reset their password every 90 days.
- Offsite access to the Cliffe Packaging network is controlled through a virtual private network (VPN) through a WatchGuard firewall.
- All online-available services require a two-factor authentication system to gain access.
- Requiring the use of VMWare's Carbon Black Cloud Sensor on all machines accessing the network, including those used to access the VPN, in conjunction with Microsoft's in-built security measures within Windows 10/11.
- Operating automatic security updates for Windows 10/11.
- A monitored security alarm covering the entire site.
- Closed-circuit television (CCTV) is used on the premises as a physical deterrent and in evidence, where required.
- Access to Cliffe Packaging's site is fob controlled, with each fob holder required to scan into the building.
- Locks on cabinets and rooms used to store sensitive information, with only authorised personnel holding keys.

4.0 Whistleblowing Procedure

4.1 Contact Details

If any interested party needs to report a violation, please contact one of our directors directly using the following details. If you wish for your report to be anonymous, please call from a withheld number or complete a website enquiry marked for the directors' attention, omitting personal details.

Name	Telephone	Email
Philip Dawber	+44 (0) 1782 987099	phildawber@cliffepackaging.com
David Dawber	+44 (0) 1263 863101	daviddawber@cliffepackaging.com

4.2 Confidentiality Guarantee

Every report we receive is treated with the strictest confidentiality, treated with equal priority and dealt with promptly. If a resulting investigation is required, this is conducted thoroughly and as confidentially as possible.

4.3 No Tolerance for Retaliation

Reporting violations and concerns is a requirement of our code of conduct and way of working, so it is imperative anybody feels comfortable in doing so. We **do not tolerate any form of retaliation** against anyone who makes a report in good faith or whose input is required in an investigation.

Document Title	Document Type	Issue	Page
Information Security Management Policy	Policy	2.0	4/4

5.0 Review and Approval

The QHSE Manager has been appointed to oversee the implementation of this policy.

This policy is reviewed at least once annually by the board of directors with guidance from the QHSE Manager, is communicated internally and is made available publicly to all interested parties upon request.

Signed:



Date: 15/06/2024

Philip Dawber

Managing Director