

Cyber Security Policy

General Statement

Merlin Flex Ltd recognises that the risk of data theft, scams, and security breaches can have a detrimental impact on a company's systems, technology infrastructure, and reputation.

To mitigate the risk of a Cyber Security failing the company has introduced safeguards which: -

- ❖ **Protect the company's data and infrastructure**
- ❖ **Outline the protocols and guidelines that govern cyber security measures,**
- ❖ **Define the rules for company and personal use of electronic equipment,**
- ❖ **List the company's disciplinary process for policy violations.**

These safeguards include: -

- ❖ Cyber Essentials Plus and NIST standards and requirements
- ❖ Appointing Cyber Security Representatives
- ❖ Defining Confidential Data
- ❖ Device Security for Company owned equipment and use
- ❖ Device Security for Authorised Personnel Equipment use
- ❖ Email Security
- ❖ Data Storage & Data Transfer

The details of this policy shall be communicated to all employees during their induction into the company and refreshed on an annual basis.

Violation of these safeguards can lead to disciplinary action, depending upon the severity of the violation.

The management team is committed to this policy and it will be reviewed on a bi-monthly basis, or when opportunities arise, to ensure it remains appropriate to the business and its stakeholders.

Signed.

A handwritten signature in blue ink, appearing to read "Mark Merifield", written over a light blue circular stamp.

Mark Merifield (Managing Director)

Date: 20th December 2021

