

33. CYBER SECURITY POLICY

INTRODUCTION

Our Cyber Security Policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure.

MP Power Ltd is a contractor within the supply chain for the UK's Critical National Infrastructure. As such we recognise the importance of maintaining cyber and IT hygiene.

The more we rely on technology to collect, store and manage information, the more vulnerable we become, to severe security breaches. Human errors, hacker attacks and system malfunctions could cause great financial damage and may jeopardise our company's reputation. For this reason, we have implemented a few security measures. We have outlined both provisions in this policy and refer all employees to other company Policies.

SCOPE

This policy applies to all our employees and contractors and anyone who has permanent or temporary access to our systems and hardware.

User Responsibilities

- Use strong, unique passwords and change them regularly.
- Report suspicious emails, links, or activity to the IT department immediately.
- Do not share login credentials or sensitive information with unauthorised persons.
- Keep software and operating systems up to date.

Access Control

Access to systems and data is granted based on job roles and responsibilities. All access must be authorised and logged. Employees should only access information relevant to their duties.

Data Protection

- Encrypt sensitive data both in transit and at rest.
- Regularly back up important files and store backups securely.
- Dispose of data securely when no longer required.

Incident Response

In the event of a security breach, employees must immediately notify the IT department. The organisation will investigate all incidents, take corrective actions, and communicate as required.

Training and Awareness

All staff will receive regular training on cyber security best practices, threat identification, and incident reporting procedures. Ongoing awareness campaigns will reinforce the importance of cyber security.

Policy Review

This policy will be reviewed annually and updated as necessary to address emerging threats and changes in technology or regulations.