



baseGreen

Inspiring • Developing • Empowering



CYBER SECURITY POLICY & PROCEDURE



baseGreen



0114 212 5910



hello@basegreen.co.uk
www.basegreen.co.uk



Unit 1, Haggwood Quarry
Honley, Holmfirth, HD9 6PW





POL18-CYBSE – Cyber Security Policy & Procedure

Classification

Document Approval Process		
Document Actions	Completed By	Date
Reviewed and Implemented	MW	5/1/22
Reviewed and rebranded	MW/TF/JD/KS	Aug 24
Next Review		Aug 26

Revision/ Amendments						
Revision number	Section / Paragraph / Page No			Date	Amended by	Comments



POL18-CYBSE – Cyber Security Policy & Procedure

Classification

Document Author	Vonny Broadbent		Role DSL	
Document Owner	Mathew Woodhead		CEO	
	Version No.:	1.0	Date Active:	5/1/22



1. Index

Section No.	Description	Page No.
1.	Index	3
2.	Scope and Application	3
3.	Responsibilities	4
4.	Cyber Security Policy Statement	5
5.	Confidential Data	5
6.	Protect personal and company Devices	6

2. Scope and Application

This procedure applies to all Company personnel and facilities

Failure to comply with the requirements of this procedure may result in investigation and subsequent formal action in line with the Company's Capability and Disciplinary procedures.

3. Responsibilities



CEO

Has overall responsibility for setting and directing: quality, environmental, safety and health, business continuity and information security policy and for ensuring the appropriate resources are available.

Is responsible for setting Company objectives and allocating adequate resources to meet those objectives.

Directors

Are responsible for ensuring that all SMS requirements are established, implemented, maintained and continually improved in accordance with the standards to which the Company subscribes and the legislation relative to the Company's operations.

Is responsible for ensuring that policies, procedures and associated documentation together with the required systems and associated training are developed and cascaded to individual teams.

Are responsible for reviewing, issuing and amending all SMS documentation and for providing information and training at all levels of the Company.

Are responsible for assessing compliance with this procedure during all internal audits.

3.1 Document Owners

Are responsible for all SMS documentation relevant to their department or area of work.

3.2 Document Authors

Are responsible for ensuring that they follow the style guide and process defined within the procedure when producing new or revising existing, SMS documentation.

3.3 All Team Members

Are responsible for ensuring they understand Company policy and procedures and follow the processes at all times.



4. Cyber Security Policy Statement

The Cyber Security Policy includes guidelines and provisions for security measures to help Mitigate cyber security risk. It applies to all Basegreen employees, associates, contractors, and anyone who has permanent or temporary access to the company systems and hardware.

The company is Cyber Essentials compliant and achieved the approved standard for certification.

5. Confidential Data

- Confidential data is to be kept securely and includes:
- Unpublished financial information
- Data of staff, learners, associates, and contractors
- Customers, employers, awarding bodies lists (existing and prospective)

All employees are responsible for protecting this data in line with the GDPR policy.



6. Protect personal and company devices

When employees use their devices to access company e mails or accounts, they introduce security risks to company data. Employees must keep their company issued laptops, tablets, mobile phones secure by:

- Keeping all devices password protected.
- Choose and upgrade antivirus software.
- Lock laptops/phones when leaving them unattended.
- Do not leave devices exposed or unattended.

Install security updates of browsers and systems monthly or as soon as updates are available. Log into company accounts and systems through secure and private networks only. Employees are advised to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

All new employees are provided with instruction for:

- Password management.
- Awareness of antivirus/anti-malware software.

Employees must read and comply with this policy.



baseGreen
Inspiring • Developing • Empowering