Cyber Policy brief & purpose

Introduction

Our company cyber security policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure.

The more we rely on technology to collect, store and manage information, the more vulnerable we become too severe security breaches. Human errors, hacker attacks and system malfunctions could cause great financial damage and may jeopardize our company's reputation.

For this reason, we have implemented a number of security measures. We have also prepared instructions that may help mitigate security risks. We have outlined both provisions in this policy.

Scope

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

Policy elements

Confidential data

Confidential data is secret and valuable. Common examples are:

- Unpublished financial information
- Data of customers/partners/vendors
- Patents, formulas or new technologies
- Customer lists (existing and prospective)

All employees are obliged to protect this data. In this policy, we will give our employees instructions on how to avoid security breaches.

Protect personal and company devices

When employees use the company digital devices to access company emails or accounts, they introduce security risk to our data. Employees are not allowed to access organisational data via their mobile phones. This restrictions includes email application and Teams. Mobile phones are only used for voice and text messages. All data access is via desktop and laptop computers assigned to employees.

We advise our employees to keep both their personal and company-issued computer, tablet and cell phone secure. They can do this if they:

- Keep all devices password protected.
- Maintain an up-to-date computer antivirus software.
- Ensure they do not leave their 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.
- **Ensure that operating systems are up to date (within 14 days of release)**

We also advise our employees to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others. Employees can use only their assigned devices.

Energys Group Limited
Franklyn House, Daux Road, Billingshurst, West Sussex RH14 9SJ
Phone: 01403 786212 **Fax:** 01403 787 439 **Email:** info@energysgroup.com **Website:** www.energysgroup.com

When new employees receive company-issued equipment they will receive instructions for:

- company laptop and or a tablet
- Password management for company systems

Keep emails safe

Our hosted mail system has a number of security features to keep our data safe including virus protection and impersonation protection. However Emails often host scams and malicious software (e.g. ransomware.) To avoid virus infection or data theft, we instruct employees to:

- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. “watch this video, it’s amazing.”)
- Be suspicious of clickbait titles (e.g. offering prizes, advice.)
- Check email and names of people they received a message from to ensure they are legitimate.
- Look for inconsistencies or give-aways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)
- If an employee isn’t sure that an email they received is safe, they can refer to our hosted supplier support desk.

Manage passwords properly

Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they won’t be easily hacked, but they should also remain secret. For this reason, we advise our employees to:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays.)
- Remember passwords instead of writing them down. If employees need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.
- Exchange credentials only when absolutely necessary. When exchanging them in-person isn’t possible, employees should prefer the phone instead of email, and only if they personally recognize the person they are talking to.
- Change their passwords every two months.

Remembering a large number of passwords can be daunting. We will purchase the services of a password management tool which generates and stores passwords. Employees are obliged to create a secure password for the tool itself, following the abovementioned advice.

Please note that these rules are enforced on the corporate servers and hosted system but you should also adhere to them for any services outside the hosted service.

Transfer data securely

Transferring data introduces security risk. Employees must:

- Avoid transferring sensitive data (e.g. customer information, employee records) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, we request employees to ask our hosted service provider for help.

Energys Group Limited
Franklyn House, Daux Road, Billingshurst, West Sussex RH14 9SJ
Phone: 01403 786212 **Fax:** 01403 787 439 **Email:** info@energysgroup.com **Website:** www.energysgroup.com

Registered in England 05691393
Registered address: New Kings Court, Tollgate, Chandler’s Ford, Eastleigh, Hampshire SO53 3LG
A company in the Energys Group

- Share confidential data over the company network/ system and not over public Wi-Fi or private connection.
- Ensure that the recipients of the data are properly authorized people or organizations and have adequate security policies.
- Report scams, privacy breaches and hacking attempts

Our hosted service provider needs to know about scams, breaches and malware so they can better protect our infrastructure. For this reason, we advise our employees to report perceived attacks, suspicious emails or phishing attempts as soon as possible to our specialists.

Admin level access approval process

Administrator approval

Administrator access is only granted to a Principal Admin via a separate admin account by the Managing Director. The access to admin account is given to authorised individuals (currently the Finance Manager and Group Services Manager) only and only to required applications and information to perform the admin role.

The management team review the list of Principal Admin every 6 months at the management meetings.

The below are part of the process:

- Authentication of users before granting access to applications, devices, using unique credentials
- Removing admin access when no longer required
- Use of admin accounts to perform admin tasks only
- Removing or disabling special access privileges when no longer required (ex. change of role)

Additional measures

To reduce the likelihood of security breaches, we also instruct our employees to:

- Turn off their screens and lock their devices when leaving their desks.
- Report stolen or damaged equipment as soon as possible to the Finance Manager.
- Change all account passwords at once when a device is stolen.
- Report a perceived threat or possible security weakness in company systems.
- Refrain from downloading suspicious, unauthorized or illegal software on their company equipment.
- Avoid accessing suspicious websites.

We also expect our employees to comply with our social media and internet usage policy in our Staff Handbook

Our hosted service provider will:

- Install firewalls, anti-malware software and access authentication systems.
- Investigate security breaches thoroughly.

Our company will have all physical and digital shields to protect information.

Energys Group Limited
Franklyn House, Daux Road, Billingshurst, West Sussex RH14 9SJ
Phone: 01403 786212 **Fax:** 01403 787 439 **Email:** info@energysgroup.com **Website:** www.energysgroup.com

Registered in England 05691393
Registered address: New Kings Court, Tollgate, Chandler's Ford, Eastleigh, Hampshire SO53 3LG
A company in the Energys Group

Remote employees

Remote employees must follow this policy's instructions too. Since they will be accessing our company's accounts and systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure.

All company activities occur within the hosted service.

Disciplinary Action

We expect all our employees to always follow this policy and those who cause security breaches may face disciplinary action:

- First-time, unintentional, small-scale security breach: We may issue a verbal warning and train the employee on security.
- Intentional, repeated or large scale breaches (which cause severe financial or other damage): We will invoke more severe disciplinary action up to and including termination.
  We will examine each incident on a case-by-case basis.

Additionally, employees who are observed to disregard our security instructions will face progressive discipline, even if their behaviour hasn't resulted in a security breach.

Take security seriously

Everyone, from our customers and partners to our employees and contractors, should feel that their data is safe. The only way to gain their trust is to proactively protect our systems and databases. We can all contribute to this by being vigilant and keeping cyber security top of mind.

Name:	Kevin Cox
Position:	Managing Director
Telephone:	01403 786 212
Email:	kevin.cox@energysgroup.com

Signed: _____ **Date: 3rd December 2024**

Kevin Cox

Managing Director

Energys Group Limited
Franklyn House, Daux Road, Billingshurst, West Sussex RH14 9SJ
Phone: 01403 786212 **Fax:** 01403 787 439 **Email:** info@energysgroup.com **Website:** www.energysgroup.com

Registered in England 05691393
Registered address: New Kings Court, Tollgate, Chandler's Ford, Eastleigh, Hampshire SO53 3LG
A company in the Energys Group