Document title:

Cybersecurity Policy

Version control

Description	Revision	By	Approved	Date
First issue	A	JW	PM	29.04.24

This document has been approved & authorised by:

Name & Position: Paul Main, Managing Director

Signed:

Telephone: +44 (0)1245 210914 info@paragon-security.com www.paragon-security.com

Brief & purpose

The PARAGON SECURITY LTD. 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 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 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 our employees and contractors 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Unpublished financial information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 their digital devices to access company emails or accounts, they introduce security risk to our data. 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.
Choose and upgrade a complete antivirus software for personal equipment. (The company will provide for company issued equipment).
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.

Telephone: +44 (0)1245 210914 info@paragon-security.com www.paragon-security.com

We also advise our employees to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.
When new employees receive company issued equipment, they will receive instructions for:

Avoiding the use of USB sticks
Password management
Software updates
Phone security

They should follow instructions to protect their devices.

Keep emails safe

Emails often host scams and malicious software (e.g. worms.) 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 should refer to management.

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 recognise the person they are talking to.
Change their passwords every two months.
Apply and use 2 factor authentication when available for software or access.

Telephone: +44 (0)1245 210914 info@paragon-security.com www.paragon-security.com

Two Factor Authentication (2FA)

Two-factor authentication (2FA), sometimes referred to as two-step verification or dual-factor authentication, is a security process in which users provide two different authentication factors or routes to verify themselves.
2FA is implemented to better protect both a user's credentials and the resources the user can access. Two-factor authentication provides a higher level of security than authentication methods that depend on single-factor authentication (SFA), in which the user provides only one factor — typically, a password or passcode.

Two-factor authentication methods rely on a user providing a password as the first factor and a second, different factor — usually either a security token from Microsoft Authenticator or similar, or a biometric factor, such as a fingerprint or facial scan.

Two-factor authentication adds an additional layer of security to the authentication process by making it harder for attackers to gain access to a person's devices or online accounts because, even if the victim's password is hacked, a password alone is not enough to pass the authentication check.

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 IT Support for help.
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 authorised people or organizations and have adequate security policies.
Report scams, privacy breaches and hacking attempts
Our management staff need 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 management. They will investigate promptly, resolve the issue and send a companywide alert when necessary.

Additional measures

To reduce the likelihood of security breaches, we 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 your 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, unauthorised or illegal software on their company equipment.

Telephone: +44 (0)1245 210914 info@paragon-security.com www.paragon-security.com

Avoid accessing suspicious websites.
We also expect our employees to comply with our social media and internet usage policy which are included in the PARAGON SECURITY LTD. Staff Handbook.

We will:

Install firewalls, anti-malware software and access authentication systems.
Arrange for security training to all employees through the GDPR and Cyber Security courses.
Inform employees regularly about new scam emails or viruses and ways to combat them.
Investigate security breaches thoroughly
Follow this policy's provisions as other employees do.
Our company will have all physical and digital shields to protect information.

Remote employees

Employees working out of our offices must follow this policy's instructions. 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.

Never access the internet through an open wi fi portal in coffee shops, hotels or other public places.

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 disregarding 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.

Telephone: +44 (0)1245 210914 info@paragon-security.com www.paragon-security.com