Cyber Security Policy
BP 27

1. Introduction

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.

The Trackwork 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. 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.

2. Scope

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

3. Confidential data

Confidential data is secret and valuable. Common examples are:

- Unpublished financial information
- Data of customers/partners/vendors
- Customer & Project lists (existing and prospective)
- Personal information

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

4. Protection of 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 phone secure by:

- Keeping all devices & passwords protected.
- Maintaining antivirus software.
- Ensuring they do not leave their devices exposed or unattended.
- Installing security updates of browsers and systems when updates are available.
- Log into company accounts and systems through secure and private networks only.

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:

- Password management
- Installation of software

They should follow instructions to protect their devices and refer to the IT Manager if they have any questions.

5. **Emails**

Emails may host scams and malicious software. 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 must refer it to the IT Manager.

6. **Passwords**

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

- Choose passwords with at least twelve 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 six months.

7. **Data Transfer**

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 the IT Manager for help.
- Share confidential data over secure networks.
- Ensure that the recipients of the data are properly authorised people or organisations and have adequate security policies.
- Report scams, privacy breaches and hacking attempts to the IT Manager.

We require our employees to report perceived attacks, suspicious emails or phishing attempts as soon as possible to the IT Manager who must investigate promptly, resolve the issue and send a companywide alert when necessary.

The IT Manager is responsible for advising employees on how to detect scam emails. We encourage our employees to reach out to them with any questions or concerns.

8. 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 IT department.
- Change all account passwords at once when a device is lost or stolen.
- Report a perceived threat or possible security weakness in company systems.
- Refrain from downloading suspicious, unauthorised 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 arrangements.

Trackwork will:

- Install firewalls, anti-malware software and access authentication systems to all Company owned equipment.
- Arrange for IT security training for employees.
- Inform employees regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly.
- Have all physical and digital shields to protect information.

9. Remote employees

Trackwork shall ensure secure remote access arrangements are in place for employees and contractors requiring access to our networks. Remote workers 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. We encourage them to seek advice from the IT Manager.

10. Disciplinary Action

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

Gail Rusling

Company Secretary

January 2024