OnBoarding Group

• DEVELOPING DIVERSE BOARDS •

Cyber Security Policy

Introduction

OnBoarding Group Limited's 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 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 several security measures. We have also prepared instructions that may help mitigate security risks. We have outlined both provisions in this policy.

Scope

This policy provides information about Onboarding Group Limited's role in keeping the company secure. As such, this applies to all of our employees and anyone who has permanent or temporary access to our systems and hardware.

Device Security

Company Devices

All employees of OnBoarding Group Limited must maintain the security of company-issued devices. To maintain this, we have implemented the following:

- All company devices are to be protected with an adequate password.
- All company devices are to be updated with the latest software releases and patches.
- Devices must have full anti-virus software installed with all of the latest updates made.
- Devices must run full system scans regularly.
- All company devices are to be locked when not in use or unattended.
- All company devices to be appropriately secured before employees leave desks and overnight.
- Gain approval for removing devices from company premises.
- Adhere to company policy regarding the installation of third-party applications and personal use.
- Employees are to take responsibility for company devices if removed from the business premises.
- The Management Team is to be notified immediately if the device is lost or stolen so that they can take the appropriate action.

Personal Devices

If personal devices need to be used to access work information, then employees must adhere to the following:

- Personal devices must be password protected.
- Employees are to carry out only permitted tasks on a personal device.
- Devices must have full anti-virus software installed with all of the latest updates made.
- Devices must run full system scans regularly.
- Only make use of secure and private networks when accessing company systems.
- Employees must log out of company accounts at the end of the day or when tasks are completed (such as emails and third-party accounts e.g., social media etc.)
- Ensure devices are secured and not left unattended at any time.

Email Security

A significant number of cyber-attacks are launched via a technique known as phishing. One of the most common ways to send a phishing attack is via email. As such, ensuring email security is maintained is of the utmost importance to avoid becoming a victim of one of these types of attacks. To maintain this, we have implemented the following:

- Verifying the legitimacy of an email.
- Avoid opening attachments or clicking on links included in emails that appear suspicious.
- Avoid opening emails with ominous titles.
- Look out for any significant errors relating to grammar in emails.
- Report any suspicious emails to the Management Team, and if required IT Support, as soon as possible.

Password Management

Passwords form one of the first lines of defence when it comes to security and if compromised this can create issues across the company infrastructure. It is, therefore, important that all employees adhere to the following:

- Use a strong password consisting of upper and lower-case letters, numbers, and special characters.
- Do not use common passwords or one-word passwords.
- Do not reuse your company password for non-work-related purposes.
- Do not share passwords with another employee.

- Do not write passwords down.
- Make use of multi-factor authentication where it is made possible.
- Never allow any other person to access the company's system using your login details.

Secure Data Transfer

There are risks associated when transferring confidential data internally or externally. To minimise these risks, all employees must comply with the following:

- Only transfer confidential data to other employees or third parties when necessary.
- Only transfer confidential information over company networks.
- Verify information relating to the recipient and ensure that they have sufficient security measures in place on their side before sending the data.
- Gain permission from a member of the Management Team for the data transfer.
- Ensure the correct form of encryption is used for the data transfer, and the correct transfer method is used.
- Ensure that data transfers take place in accordance with GDPR and any confidentiality agreements which may be in place.

Cyber Security Requirements

- You must not turn off or attempt to circumvent any security measures (antivirus software, firewalls, web filtering, encryption, automatic updates etc.) that the IT team have installed on your computer, phone or network or the company IT systems.
- You must report any security breach, suspicious activity, or mistake you to make that may cause a cyber security breach as soon as you discover this.
- You should avoid clicking on links to unknown websites, downloading large files, or accessing inappropriate content using company equipment or networks.
- You must not install software onto your company computer or phone.
- You must only access work systems using computers or phones that the company owns.

Consequences of System Misuse

OnBoarding Group Limited considers the following actions to be a misuse of its IT systems or resources:

- Any malicious or illegal activities carried out against the company or using the company's systems.
- Accessing inappropriate, adult, or illegal content within company premises or using company equipment.

- Excessive personal use of company IT systems during core working hours.
- Removing data or equipment from company premises or systems without permission, or in circumstances prohibited by this policy.
- Using company equipment in a way prohibited by this policy.
- Circumventing technical cyber security measures implemented by the company's IT team.
- Failing to report a mistake or cyber security breach within an appropriate time.

If you are an employee, misuse of the IT system will be referred to the Management Team and may be considered misconduct; if you are a contractor and are found to be misusing the company IT systems, your contract may be terminated.

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

Additional Measures

To reduce the likelihood of security breaches, OnBoarding Group Limited also instructs its 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 Management Team.
- Change all account passwords at once if a device is stolen.
- Report a perceived threat or possible security weakness in company systems.
- Avoid accessing suspicious websites.
- Install firewalls, anti-malware software and access authentication systems.
- Inform employees regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly.
- Follow this policies provisions as other employees do.

This policy will be reviewed annually by the Management Team.
Last reviewed 07/04/2025 – next review date 07/04/2026