Cyber and information security policy

Introduction

The aim of the APE cyber and information security policy is to provide clarity what is expected with regards to data security and use of company systems and applications. It should support our employees with understanding of how to maintain the security of both data and applications, i.e.:

- How to transfer company data
- The use of company issued devices
- The use of personal devices

The APE cyber and information security policy has been compiled based on the risks identified through the company risk assessment.

A number of the below settings are automatically configured during device setup, and should not be disabled or subverted.

Device Security

Company Devices

It is vital that employees maintain the security of company issued devices:

- All company devices to be connected to APE's Remote Management and Monitoring system and company domain
- Devices to have Anti-Virus and Firewall enabled
- All company devices to be protected with an adequate password, see Password Management Section below for guidance on password complexity
- Company devices to be updated with the latest software releases and patches
- Devices to be locked when not in use or unattended, with an inactivity lock timer of 5 minutes
- 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 to take responsibility of company devices if removed from the business premises The Line Manger/Director/security specialist 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:

- Personal devices must be enrolled on the company system and meet compliance rules before access is granted. Compliance Rules include, but are not limited to the below:
- Personal devices must be password protected
- Devices must have a recognised anti-virus software installed with all of the latest updates made
- Automatic lock settings enabled to timeout after 2 minutes
- Devices must be on a recognised operating system and version
- Devices must not be Jail-broken or run custom firmware

The following best practices must also be followed:

- Employees to carry out only permitted tasks on a personal device
- Only make use of secure and private networks to log into company systems
- Ensure devices are secured and not left unattended at any time

- The Line Manger/Director/security specialist to be notified immediately if the personal device that had access to company data is lost or stolen

Email Security

A significant number of cyber-attacks are launched via a technique known as phishing. And one of the most common ways to send a phishing attack is via email. Ensuring email security is therefore important in avoiding becoming victim of one of these types of attack. Please follow this guidance:

- Ensure that Multi-Factor Authentication is enabled for your account and is registered to your mobile device
- Verifying the legitimacy of an email – is it from who it suggests it is from? Check the sender's name, email address etc
- Avoid opening attachments or clicking on links included in emails which appear suspicious
- Avoid opening emails with clickbait titles
- Look out for any significant errors relating to grammar in emails. This can be a sign of suspicious activity
- Report any suspicious emails to our external IT company as soon as you are able to do so
- Authentication via secure code to nominated phone number per email address

Password management

Passwords form one of the first lines of defence when it comes to security. But if passwords are compromised this can create issues across the IT infrastructure.

Please follow APE Password management policy:

- Passwords must be a minimum of 8 characters in length and contain a combination of upper-case letters, lowercase letters, numbers and special characters
- Do not use common passwords or one-word passwords – e.g., password, qwerty,123456
- Do not reuse your company password for non-work-related purposes
- Make use of multi factor authentication where it is made possible
- Do not share passwords with another employee. You must have an individual account for any company applications or systems that you make use of. If this is not possible, then consult a director regarding the best way to manage shared access
- Do not write passwords down

Secure Data Transfer

There are risks associated when transferring confidential data internally or externally. To minimise these risks, please follow the below:

- Only transfer confidential data to other employees or third parties when absolutely 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 sign-off from a member of senior management for the data transfer
- Discuss any data transfers with a director/security specialist before going ahead to ensure that it is done in a way that complies with company policy
- Ensure that data transfers take place in accordance with GDPR and any confidentiality agreements which may be in place

Employee Declaration

All employees are required to read this policy and confirm on Breathe HR (the company HR software) that they have read, fully understood and will adhere to the above Cyber and information security policy.