7 Steps to establish a cyber foundation

We believe businesses of all sizes need to build the appropriate cyber resilience - this starts with a foundation. Whilst this will differ depending on your business and technology estate, we'd like to recommend these initial steps to get you started.

1. Activate Two-Factor Authentication (2FA)

Two-Factor Authentication creates a secondary defence against any weaknesses in login credentials and allows you to act fast if a breach occurs. 2FA is customisable on most platforms allowing for improved security through increased access control to systems and data.

2. Create bring your own device (BYOD) policies

Businesses should ensure personal devices used for work are secure and meet your policy. There are some occasions where BYOD is not recommended, such as where highly confidential information needs to be accessed. IT & cyber policies can answer questions about BYOD's requirements, allowing employees to know the do's & don'ts.

3. Implement a password manager

Implementing a password manager can help small businesses manage their credentials and protect accounts. A password manager can help employees create and store strong passwords. You should carefully select a password manager that is suitable for your needs and can be customised to allow and disable access.

4. Secure Wi-Fi connectivity with a VPN

By securing your connection, you can prevent unauthorised access and protect data from being intercepted. A VPN ensures that employees access company data over a secure connection, particularly when working remotely. A VPN adds an extra layer of protection to your online communication.

5. Provide security training

Delivering regular training & awareness, you can empower your employees with the skills to identify and respond to potential threats. This ensures the protection of devices, network, and data as part of good cyber hygiene. Investing in cyber awareness will safeguard your business and promote a vigilant culture.

6. Turn on automatic backups

By enabling automatic back-ups, you have access to the most recent data. If you experience a technical failure or system unavailability, you can retrieve data and minimise business disruption. You can manage the frequency, test retrieval of data and perform periodic manual back-ups.

7. Select the right partners

Understanding how your sensitive data will be managed by third parties is crucial to your business. It's vital to thoroughly assess their cybersecurity policies, controls and their ability to comply with relevant regulatory requirements. Additionally you should have the right to audit their practices.

Klyk are here to assist you to a greener, securer tech future. Vist **HelloKlyk.com** or email **Zahid@HelloKlyk.com** to find out more.