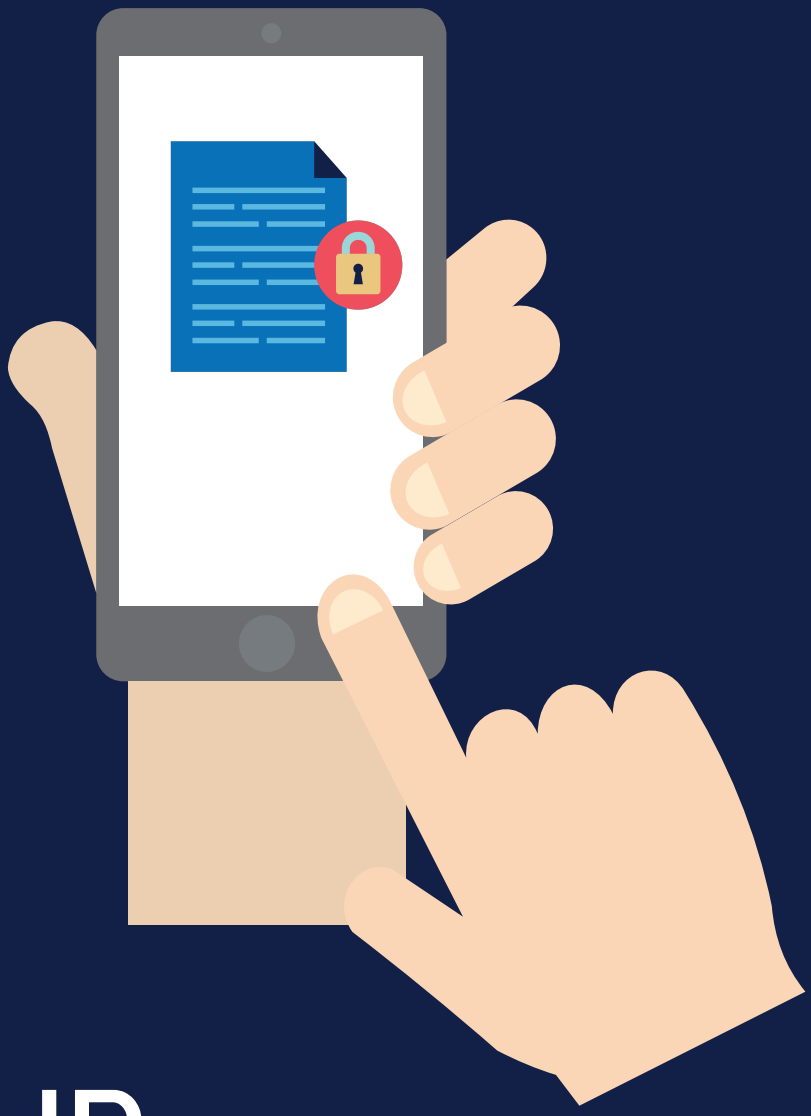


BRING YOUR OWN DEVICE (BYOD)

A guide to securing workplace data on any device

www.breakwaterit.co.uk

breakwater IT

WHAT IS BRING YOUR OWN DEVICE?

Bring Your Own Device (BYOD) is the concept of **employees using personal devices to conduct their work**, rather than devices purchased by the organisation.

It's vital to note that **BYOD may apply to some organisations without their knowledge**. This could include Microsoft, Apple or Android mail applications or the Microsoft Teams application, onto devices such as mobiles and tablets, or PCs and laptops.

EXAMPLE

An employee downloading the Outlook application to a personal mobile device without the knowledge or consent of the employer. This could potentially mean company data is being accessed on an unsecure device.

There are pros to using BYOD in the workplace. Including allowing employees to use devices they feel comfortable with, to support flexible working or to reduce overheads.

Overall, it is important to remember that **the organisation will own any company data or resources** accessed or stored on the device, but **the device itself belongs to the user.**

THE RISKS OF BRING YOU OWN DEVICE

There are several security risks to allowing BYOD in the workplace. These include:

- Loss or theft of the device due to regular use outside of work hours
- Devices not complying with company policies or procedures, for example, password entry on the device, encryption, anti-virus protection
- Increased support will be needed for a wider range of devices and operating systems
- Corporate data may be at higher risk of theft or malicious intent

BRING YOU OWN DEVICE POLICIES

BYOD policies are measures put in place to monitor or restrict the movement of workplace data. There are several ways to make having BYOD in place secure for both the organisation and users. Let's explore the key methods:

SECURE PASSWORDS AND MULTI-FACTOR AUTHENTICATION

Ensure that you have policies in place for staff to have secure passwords and multi-factor authentication (MFA) on all devices accessing organisational data.

You can take this further and enable password protection or MFA on applications and software.

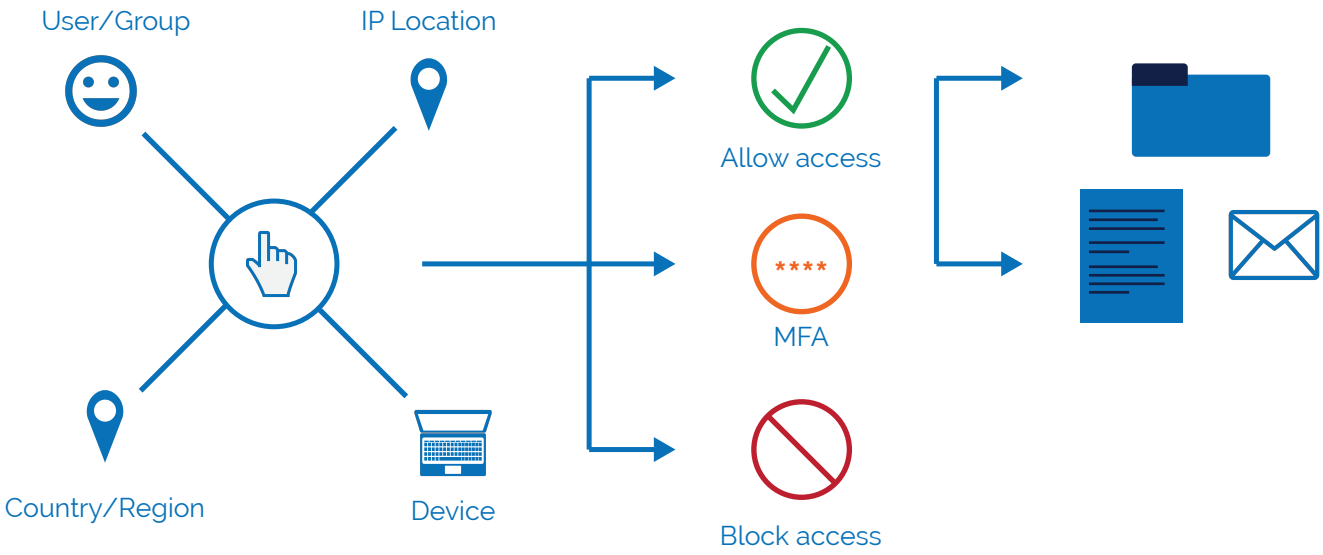
CONDITIONAL ACCESS

Conditional access allows you to set a criteria which must be matched in order for employees to gain access to data.

Office 365 services can have conditions and actions applied:

Conditions – policies can be targets at specific users or groups. You can block certain devices, or geographical access. Alternatively, you can allow certain IP addresses to access data, such as your work or a home IP.

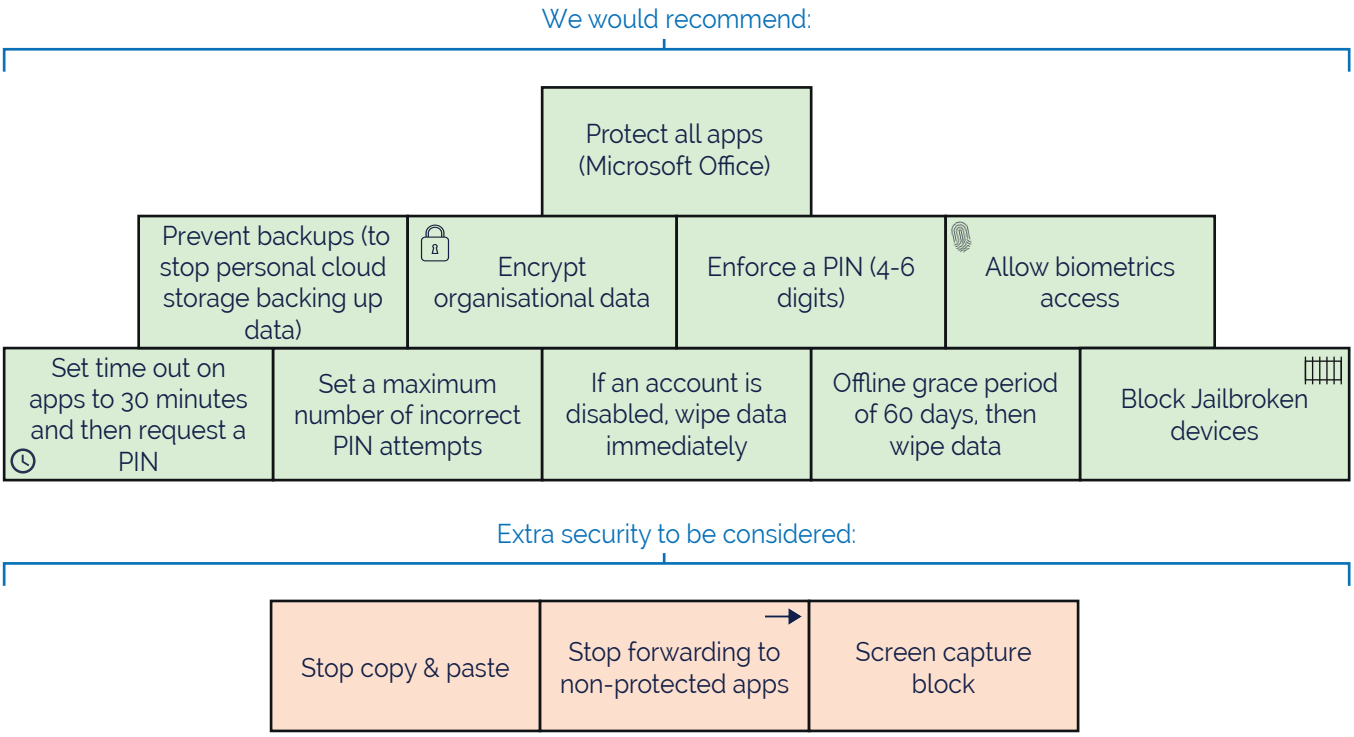
Actions – to enable the conditions, actions must be put in place. These include allowing access, blocking access or requiring MFA to access an application.



APP PROTECTION POLICIES

App protection policies help to keep your data safe by blocking or monitoring the movement of workplace data in apps.

Policies can be applied to corporate and personal devices with apps installed that contain workplace data. This is because the data is protected within the app, rather than through device management solutions. This means that you can apply the policies without physically handling the device.



IN SUMMARY...

Whether your organisation does or does not have BYOD in place, you should still enable preventative measures to protect yourself. You may not be aware of staff downloading or accessing data from a personal device. Therefore, we recommend you enable app protection and data loss prevention policies to securely restrict the movement of your data.

For any additional help with BYOD, or anything else you need, get in touch:

Service Desk:
01603 709301 | servicedesk@breakwaterit.co.uk

Enquiries:
01603 709300 | enquiries@breakwaterit.co.uk