Securing Personally Owned Devices (aka BYOD)

October 2015

What is this IS Advisory about?
There is a growing trend for staff to use their own mobile device to access University data such as Gmail and app. Mobile technologies have made it possible for a mobile device user to access both 'their stuff' and 'the University's stuff' on the same device. The University is legally obliged to protect its information assets (e.g. staff and student personal data and corporate data) if it is stored or processed on a personally owned device.

Who is this IS Advisory aimed at?
This IS advisory is aimed at staff and third parties using personally owned computer devices to view or process University data.

How does the University monitor compliance with this IS Advisory?
Annual review of this IS advisory will be performed to evaluate its on-going effectiveness and relevance as technology changes.

Who can you contact if you have any queries about this IS Advisory?
Any questions about this advisory should be directed to the IS Service Desk servicedesk@port.ac.uk

1.0 Risks

1.1 The University has very little control over BYODs
1.2 The range of BYODs is large and growing - new functionality is unpredictable.
1.3 The University has little control over the type of data held/accessed by BYODs
1.4 The security of data transferred to BYODs cannot be assured
1.5 Access to data held on a BYOD cannot be assured

In order to mitigate these risks, the University reserves the right to:

- ***Require that minimum security settings are applied on the BYOD;***
- ***Restrict access to University systems and data from BYOD;***

2.0 Good practice requirements

The University must take reasonable steps to minimise the risk of data loss. To achieve this aim, BYOD users must implement the following security controls:

2.1 Set up a PIN, passcode or password to protect access to the device.
If the device is lost or stolen, then access to any data held will be protected.

2.2 Set an inactivity timeout to lock the device after 3 minutes of idle time.
Data on the device is better protected if the device is safe when not in use.

2.3 Keep all software and device operating system software up to date
This keeps the risk of malware infection down to a minimum.

2.4 A jail-broken or ‘rooted’ device has escalated privileges - it is unwise to use such a device unless you have the ability to maintain adequate device security.
Jail-broken devices - “with great power comes great responsibility”.

2.5 Do not store unencrypted University data on the device.
The University is legally obliged to protect its data assets.

2.6 Seek advice from Information Services on the secure deletion of any data which might be stored on the device before selling, exchanging, gifting or disposing of it.

Further advice on how best to secure individual devices can be obtained from Information Services (servicedesk@port.ac.uk).