Mobile Computing Policy

Brunel University London

An ISO/IEC 27001:2013: *Aligned Document - Implementing Cyber and Information Security Best Practice*

Internal Use Only

Mick Jenkins

Chief Information Security Officer

Document History

Version	Author	Comments	Date
V 0.1	Andrew Clarke	Initial Draft	09/09/2019
V 0.2	Andrew Clarke	PWG amendments and comments	19/09/2019
V 1.0	Andrew Clarke	DSB Approval	30/11/2019

Document Approval

Owner: Michael Jenkins	Chief Information Security Officer
Signature: MGJ	Date 30 Nov 2019
Approver: Pekka Kahkipuro	Chief Information Officer
Signature: PK	Date: 30 Nov 2019
Distribution:	

This document requires the approval from BUL as defined in the ISMS Compliance document.

Contents

1. About this document

1.1 Purpose of Document

This Policy establishes the area within Brunel University London (BUL) supporting security measures to be adopted to manage the risks introduced by using mobile phones and other mobile devices such as laptops, tablets.

Please refer to Brunel University London ISMS Document BUL-GLOS-000 - SyOPs Glossary of Terms for the glossary of terms, acronyms and their definitions for the suite of Brunel University London ISMS documentations.

1.2 Responsibilities

Table 1 – responsibilities

Title / Role	Description
Systems Manager	• Responsible for specifying and/or providing the local firewalls, anti-malware software, automatic updating, connectivity and backup facilities required under this procedure
Network & Infrastructure Manager	• Responsible for specifying and/or providing the firewalls facilities required under this procedure
Head of Customer Services	• Responsible for ensuring user training is adequate for policy compliance
All Users	• All Users of mobile computing devices are responsible for ensuring that such devices are purchased, used and disposed of in accordance with the University's policies and procedures. In particular, users must ensure that they act in accordance with the University's various information security policies and that they have completed the University's mandatory training module on information security.

1.3 ISO 27001 - Conformance

This section indicates the University Conformance to ISO27001:2013.

University ISMS Control Number	SOA – Number A6 - University of Information Security
ISO 27001:2013 Conformance Control	Information Classification Objective A.6.2.1 Mobile Device Policy

1.4 Scope

The aspects of this policy relating to stewardship of the University's mobile computing assets apply to all mobile computing devices purchased with University-administered funding irrespective of source, including general funds, research grants and K1 accounts. The information security aspects of this policy apply to all mobile computing devices, both University-owned and BYOD (Bring Your Own Device), used to access university systems and services remotely. Where an individual opts to use a BYOD for work on 'highly restricted' data, they are advised to back-up any personal data stored on the device to allow for remote data wiping in the event of loss.

1.5 Definition

For the purpose of this policy, "mobile computing devices" refer to all forms of portable computing equipment managed by Brunel University that can store digital data. Examples include, but are not limited to, laptops, netbooks, tablets and mobile phones.

1.6 References

- Information Classification policy
- Network Access Policy
- Cryptographic policy
- Secure Disposal Policy
- Remote Working policy
- Password Policy
- Brunel Acceptable Use Policy (BACUP)
- BUL-POL-6.2.1 - Information Security Remote Working Policy

2.0 Mobile Computing Management

2.1 Stewardship of Mobile Computing Devices

2.1.1 Like all equipment purchased from University-administered funds (see 1.4 above), mobile computing devices remain the property of the University. They must be returned to the University on request or on termination of employment. (Ref BUL Procurement Code)

2.1.2 Laptops, tablets and mobile phones should be purchased in accordance with the University's Procurement Purchasing Policy.

2.1.3 Mobile computing devices should be used for the intended business need and in accordance with the University's information security and acceptable use policies, i.e. mobile devices should be used only by University staff and predominantly for University business. Incidental personal use where it is consistent with any requirements of the University's IS policies may be permitted by consent of the individual Line Manager.

2.1.4 The security of any University data stored on a mobile computing device must be given due consideration. Any unique data generated on such a device should be copied onto the appropriate University data store at the earliest opportunity. University Confidential information must not be copied or backed up to unsecure devices.

2.1.5 Users with administrative privileges on laptops must ensure that any software, or media file loaded onto the machine is used in compliance with the appropriate license(s) and copyright considerations.

2.1.6 Users of Brunel Managed mobile computing devices are responsible for maintaining the currency of the computer operating systems, anti-malware and productivity applications ("patching"). It is not permitted to make any alterations to the hardware or software that significantly impair security. If the user is not comfortable with this responsibility, they should return it to their IS support (College IT or IS) on a regular basis, allowing sufficient time for updates to be installed.

2.1.7 Users must maintain University owned mobile computing device in compliance with warranty conditions and in no way invalidate the warranty by tampering with the hardware.

Should the device be required beyond the period of its original warranty, any repairs or replacement parts are funded by the end user's sources (e.g. research grants).

2.1.8 If a user has any reason to suspect that their University managed mobile device has become infected with malware, they should immediately cease to use it, and return it to IS support (College IT or IS) for examination / disinfection.

Users should seek advice from IS support (College IT or IS) before passing on, discarding, or otherwise disposing of, any University purchased mobile computing device.

2.2 Information Security

2.2.1 All Brunel users of mobile computing devices which access University data must complete the University's mandatory training unit on information security. All users of mobile computing devices which access University data must comply with the Brunel Acceptable use Policy.

2.2.2 Users are responsible for the physical security of their mobile computing devices and any University data stored on it.

2.2.3 Information being accessed or processed using mobile computing devices should be treated in accordance with the Information Classification policy and the Information Classification Procedure in order to classify the information they wish to access correctly and have put in place the required security protection measures.

2.2.4 There are increased security and reputational risks associated with the processing of any data classified as 'University Confidential' or 'Protect' so users of mobile computing devices should give serious consideration before removing such data from within the safety of the University Network.

For 'University Confidential' information, users should consider encryption of the data.

2.2.5 Mobile computing devices used in pursuance of University business must have remote wiping agents installed upon them by IS to ensure University Confidential data can be removed securely should the device be lost or stolen.

BYOD owners are responsible for ensuring that if they intend to hold University Confidential data on their device that the minimum requirements for Brunel University London's hardware and software configurations are upheld. BUL-POL-6.2.1 - Information Security Remote Working Policy

The University uses Information protection technologies[1] to protect the University information.

The IS Service Desk will advise the user only on suggested actions but they will not action any changes to non-Brunel University London equipment.

2.2.6 Any loss of mobile computing device or suspected breach of information security should be reported immediately to IS, Chief Information Security Officer, as well as the user's Head of Department. Suspected theft of a mobile computing device should also be reported to Security.

2.2.7 In the event of loss of mobile computing devices, users should anticipate that the University will take steps to mitigate the risk of any potential information security breach by the remote wiping of equipment. In such an event, any personal data the user has stored on the device *may* be deleted.

2.2.8 The University requires users to act with care in public places so as to avoid the risk of confidential computer activity being overlooked by unauthorised persons. Users should avoid internet café and other public wi-fi connections as these pose information security risks and should be avoided especially when accessing highly sensitive information. If absolutely required, then a VPN should be used for secure connectivity.

2.2.9 Users of Brunel owned unmanaged devices and BYOD are responsible for ensuring that they maintain anti-virus software, operating systems and security updates, as appropriate to the equipment, if they use it to access, store or process institutional digital data.

2.2.10 IS will monitor and log network usage as a means to protect information. The University carries out regular and ad hoc audits of all devices to ensure that they are configured in compliance with this procedure.

2.2.11 The University requires that mobile devices are physically protected against theft and damage while in transit, in storage or in use.

2.2.12 The University enforces University password policy on all mobile platforms and ensures they; have password protection (including when

[1] Such as IRM (Information Rights Management) and DLP (Data Loss Prevention).
Information rights management (IRM) protect University Confidential information from unauthorised access and allows an owner to control, manage and secure information from unwanted access.
Data loss prevention (DLP) is a strategy for making sure that end users do not send sensitive or critical information outside the University network. DLP uses rules to classify and protect confidential and critical information so that unauthorised end users cannot accidentally or maliciously share data whose disclosure could put the University at risk.

idle e.g. screensaver / lock screen), utilise appropriate encryption (ideally whole disk encryption where supported, otherwise file or application encryption), avoid accidental / unsecure sharing (via things like folder and printer sharing, Bluetooth, over non-Brunel email etc).