Mobile Device Security Policy

Title: Mobile Device Security Policy					
Version	**Issue Date**	**Revision Description**	**Author**	**Approved By & Date**	**Next Review Date**
1.0	Feb 2013	First Issue	Tony Evans	DISAG	
1.1	Sept 2013	Changed University title	Alan Davies	DISAG	
1.2	Oct 2015	Reviewed and additional policy note added for 'untrusted apps'.	Tony Evans	VCEB-ICT (For consideration 6/11/15)	
1.3	Nov 2015	Approved by VCEB-ICT subject to minor change.	Tony Evans	VCEB-ICT 6/11/15	Nov 2016

Mobile Device Security Policy

INTRODUCTION

This policy outlines the minimum acceptable controls that are required for mobile device connectivity with University systems and services. Some University services, such as email, may enforce controls on the device if they are being used.

It should be noted that this Policy will be reviewed periodically and may change in line with technological and other developments. Members of staff can access the latest version of the Policy on the Staff portal.

CONTEXT

Mobile devices are increasingly being used to connect to University systems and services. This usage includes access to services such as web applications and email, connectivity to wireless networks, and physical connectivity to computer systems.

User account credentials are commonly stored or cached on mobile devices, and University data may be stored without encryption. Access to the functionality of the device is often inadequately protected, or not protected, by a PIN (Personal Identification Number). Data stored on the device may not be backed up.

As such, a misplaced, unattended or stolen mobile device may expose the University to risks of unauthorised access, breaches of confidentiality and data loss. In addition, an unpatched or weakly configured device exposes the University to similar risk. By their very nature a mobile device is more likely to be lost or stolen, and therefore increases the likelihood of this risk.

Users should be aware that the access and use of personal and University information on mobile devices is covered by legislation such as the Data Protection Act 1998 and the Freedom of Information Act 2000.

SCOPE OF POLICY

For the purpose of this policy, a mobile device is defined to be any portable technology running an operating system optimised or designed for mobile computing, such as Android, Blackberry OS (RIM), iOS (Apple), Windows Mobile, and Symbian. This excludes technology running general-purpose operating systems found on laptops, netbooks, MacBooks such as any of the Microsoft Windows desktop or server operating systems, versions of MacOS, or Linux.

This policy applies to all users using a mobile device to access University systems or services that require authentication, or where University data or credential are stored or cached on the mobile device, regardless of whether it is a personally or University-owned device.

POLICY STATEMENTS

A mobile device that is used to access University services must be configured to:

- Require a passcode of 4 or more digits/characters, or other secure authentication method.
- Request the passcode after a maximum period of five minutes inactivity.

The owner of the mobile device should ensure that:

- The passcode or other authentication credential is not divulged to a third party.
- The device and installed apps are kept up---to---date with vendor patches.
- The device is not left unattended in a public environment.
- If the device is lost or stolen, University account password(s) must be changed.
- University-licensed software/applications are used within the licensed terms and conditions.
- The device is securely wiped prior to disposal.

Additionally, where personal, confidential or other sensitive University data is accessed via the device:

- The data must be encrypted on the device and in communication.
- Where backups of the data are provided these must be encrypted.
- Where that data is of such criticality that functions or operations would be disrupted should it be unavailable, lost or become corrupted, these should not solely be stored on mobile devices.
- The device must be configured to enable remote wiping, and, in the event of loss, remote wiping must be used to attempt a removal of University data from the device.
- No attempt should be taken to circumvent the native security of the device, such as “jailbreaking” or “rooting”.
- Ensure that, in a public environment, it is not possible for third-parties to view University personal or confidential information.
- Care must be taken over the installation of ‘apps’ that could compromise the security of your mobile device leading to the disclosure of personal, confidential or other sensitive University data.

All University-owned devices, and those personal devices with highly personal, confidential and/or sensitive data pertaining to the University, must be configured to allow University’s Mobile Device Management technology to manage agreed settings. The University’s Mobile Device Management technology will enforce this policy and other controls that the University considers appropriate. Where encryption software has not been used to protect the data,

regulatory action may be pursued.

The user is responsible for the security of University data held on the device. Any loss of mobile devices (personal or University owned) that have held University data should be reported to the Information Governance Team.

The University may disable any mobile device's access to corporate resources at any time. The University cannot be held responsible for damage to personal content as a result of making use of University services (e.g. email).

ENFORCEMENT

Mobile device access to University systems and services is a privilege and not a right. Where there is non-compliance with this policy (e.g. not configuring a passcode), the privilege may be removed from the user and/or University disciplinary procedures could be invoked.

RESPONSIBILITIES

It is the responsibility of members of staff to read and act in accordance with the principles of this Policy. The University will ensure this Policy is accessible to all members of staff and incorporated in induction information. The University will periodically review and update the Policy and members of staff will be notified of any significant changes.

Staff should be aware that by using a personal device(s) to access University owned information they are bound by the University's Policies and legal obligations.

If assistance is required to set up the device in order to adhere to this policy or to assist with any accessibility issues, contact IT Services support using the 'IT On-line Support' facility in the first instance.