MOBILE DEVICE POLICY

INTRODUCTION

Mobile devices, such as smartphones and tablet computers, are important tools for the organization and the Alabama Department of Postsecondary Education (DPE) supports their use to achieve business goals.

However, mobile devices also represent a significant risk to data security, if the appropriate security applications and procedures are not applied, as they can be a conduit for unauthorized access to the organization's data and IT infrastructure. This can subsequently lead to data leakage and system infection.

DPE has a requirement to protect its information assets in order to safeguard its customers, intellectual property and reputation. This document outlines a set of practices and requirements for the safe use of mobile devices and applications.

1.0 POLICY

1.1 All mobile devices, whether owned by DPE or owned by employees, inclusive of smartphones and tablet computers, that have access to Department networks, data and systems are governed by this mobile device security policy.

1.1.1 The scope of this policy does not include corporate IT-managed laptops.

1.1.2 Exemptions: Where there is a business need to be exempted from this policy (too costly, too complex, adversely impacting other business requirements) a risk assessment must be conducted by the Director of Information Services and presented to the Deputy Chancellor through the Vice Chancellor of Finance and Administrative Services.

1.1.3 Applications used by employees on their own personal devices which store or access corporate data, such as cloud storage applications, are also subject to this policy.

1.2 Devices must use the following Operating Systems: Android 2.2 or later, iOS 4.x or later.

1.3 Devices must store all user-saved passwords in an encrypted password store.

1.4 Devices must be configured to lock the console after a period of inactivity (not to exceed 15 minutes) and require authentication to unlock the device. Where possible, the lock screen password should adhere to the DPE Password Policy.

1.5 Any handheld device that is used in conjunction with DPE activities, including retrieval of email or calendar data must be configured so that it can be locked or erased if it is lost or stolen.

1.5.1 iPhone and iPad users must have **Find my iPhone, iPad, and Mac** configured so that the device can be locked or erased if it is lost or stolen.

1.5.2 Android users must use the **Android Device Manage** (https://www.google.com/android/devicemanager) so that the device can be locked or erased if it is lost or stolen.

1.6 Only devices managed by the Information Services Division will be allowed to connect directly to the internal corporate network.

1.7 These devices will be subject to the valid compliance rules on security features such as encryption, password, key lock, etc. These policies will be enforced by the IT department using Mobile Device Management software.

1.8 All DPE owned mobile devices must have the Find my iPhone or Find my iPad app configured.

2.0 GUIDELINES AND BEST PRACTICES

2.1 Avoid keeping confidential data or otherwise sensitive information on mobile devices, because they are more likely to be lost or stolen and harder to encrypt.

2.2 Keep software updated, since mobile devices are vulnerable to direct attacks from both malware (viruses, etc.) and phishing.

2.3 Delete any text you receive with passwords or other sensitive information.

2.4 Only install apps from trusted resources. Apps can host malware that will expose your passwords, credit card numbers, or anything else you type into your mobile device.

2.5 Turn off Wi-Fi and Bluetooth if you aren't using them. Wireless features give remote access to hackers.

2.6 If you do use Wi-Fi, only do so on secure networks that require a password.

2.7 Back up your data to minimize the chances of losing everything should your device be lost or stolen, or need to be wiped completely due to a virus or other security breach.

2.8 Avoid sharing mobile devices. Personal mobile devices are not designed to support multiple users and can't be set up to protect you from risk caused by other people's activities.