Mobile Device Security Policy

Introduction

Mobile devices, such as smartphones and tablet computers, are important tools for the organisation and their use is supported to achieve business goals.

However, mobile devices also represent a significant risk to information security and data security as, if the appropriate security applications and procedures are not applied, they can be a conduit for unauthorised access to the organization's data and IT infrastructure. This can subsequently lead to data leakage and system infection. A primary concern is to ensure the security of personal data in accordance with the Data Protection Act 1998.

Lineal 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.

Scope

All mobile devices, whether owned by Lineal or owned by employees, that have access to corporate networks, data and systems, not including corporate IT-managed laptops. This includes smartphones and tablet computers.

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 being authorised by the security management team.

Policy

Technical Requirements

1. Devices must use the following Operating Systems: Android 6 or later, IOS 10 or later.
2. Devices must store all user-saved passwords in an encrypted password store.
3. Devices must be configured with a secure password that complies with Lineal's password policy. This password must not be the same as any other credentials used within the organization.
4. With the exception of those devices managed by IT, devices are not allowed to be connected directly to the internal corporate network.

User Requirements

1. Users must only load data essential to their role onto their mobile device(s).
2. Users must report all lost or stolen devices to Lineal's security management team immediately.
3. If a user suspects that unauthorised access to company data has taken place via a mobile device, they user must report the incident in alignment with Lineal's incident handling process
4. Devices must not be "jailbroken"* or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user.
5. Users must not load pirated software or illegal content onto their devices.

6. Applications must only be installed from official platform-owner approved sources. Installation of code from un-trusted sources is forbidden. If you are unsure if an application is from an approved source contact Lineal's IT.
7. Devices must be kept up to date with manufacturer or network provided patches. As a minimum, patches should be checked for weekly and applied at least within a month of release.
8. Devices must not be connected to a PC which does not have up-to-date and enabled anti-malware protection and which does not comply with corporate policy.
9. Devices must be encrypted in line with Lineal's compliance standards.
10. Users must be cautious about the merging of personal and work email accounts on their devices. They must take particular care to ensure that company data is only sent through the corporate email system. If a user suspects that company data has been sent from a personal email account, either in body text or as an attachment, they must notify Lineal's security management team immediately.
11. Users must not use corporate devices to backup or synchronise device content such as media files unless such content is required for legitimate business purposes.

*To jailbreak a mobile device is to remove the limitations imposed by the manufacturer. This gives access to the operating system, thereby unlocking all its features and enabling the installation of unauthorised software.

Date of next review: 31st March 2018