EXCELLENT FORTUNE DEVELOPMENT GROUP

Mobile Device Policy

1. Overview

Mobile devices, such as smartphones and tablet computers, are important tools for the organization 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.

2. Purpose

The purpose of this policy is to outline a set of practices and requirements for the safe use of mobile devices to safeguard the company's intellectual property and reputation.

3. Scope

This policy applies to employees, contractors, consultants and all other workers in the company and its subsidiaries, including all personnel affiliated with third parties. This policy applies to all mobile devices, including but not limited to smartphones and tablet computers, whether owned by the company or owned by the employees.

4. Policy

4.1 Devices must be protected with a password, pin, pattern or fingerprint, with the automatic lock screen feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

4.2 If company data is loaded onto the mobile devices, users must only load data essential to their role.

4.3 Users must report all lost or stolen devices to the company immediately.

4.4 If a user suspects that unauthorized access to company data has taken place via a mobile device, they must report the incident to the company immediately.

4.5 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 (Note: 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 unauthorized software).

4.6 Users must not load pirated software or illegal content onto their devices.

4.7 Applications must only be installed from official platform-owner approved sources. Installation of code from un-trusted source is forbidden.

4.8 Devices must be kept up to date with the manufacturer or network provided patches. As a guide, patches should be checked weekly and applied at least once a month.

4.9 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 the company immediately.

4.10 Devices must not be connected to a corporate workstation which does not have an up-to-date and enabled anti-malware protection, and which does not comply with corporate policy.

4.11 Users must not use corporate workstations to backup or synchronize the contents in the mobile devices, such as media files, unless such content is required for legitimate business purposes.

5. Policy Compliance

5.1 Compliance Measurement

The company will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the policy owner in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.