Ahead

MANAGEMENT GROUP

Mobile Device Policy

Building fair and effective standards into our business

Table of Contents

AheadMG Ltd 4th Floor, Silverstream House, 45 Fitzroy Street, Fitzrovia, London, W1T 6EB

Management@aheadmg.co.uk

Document Control

Document History

	Author	Version	Description
08/10/2015		V0.1	Template Draft
09/10/2015	Matthew Westmacott	v0.2	Initial AheadMG Draft
05/06/2017	Andy Fox	V0.3	Reviewed at board meeting, minor amendments.
11/01/2017	Andy Fox	V1.0	Baselined version
12/09/2018	Tracy Allen	V1.1 (Draft)	Draft - Added Text covering GDPR Updated AheadMG business address.
		V1.1 (Approved)	Latest Updates accepted at Exec Meeting
19/07/2019	Tracy Allen	V1.2 (Draft)	Minor updates for 2019
		V1.2 (Approved)	Latest Updates accepted at Exec Meeting
18/02/2022	Donna Chapman	V1.3	Minor updates for 2022
24/08/2023	Donna Chapman	V1.4	Minor updates for 2023

Signatories

Name	Role	Sign off Date
Andy Ewell	AheadMG Delivery Director	11/01/2016
Neil Hickman	AheadMG Finance Director	11/01/2016

Document Storage

All versions of the policy will be stored on our website https://www.aheadmg.com/new-starters/

Mobile Device Policy

Introduction

Mobile devices, such as smartphones and tablet computers, are important tools for AheadMG and supports their use to achieve business goals.

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

AheadMG 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.

Scope

1. All mobile devices, whether owned by or owned by employees/associates, inclusive of smartphones and tablet computers, that have access to corporate networks, data and systems are governed by this mobile device security policy. The scope of this policy does not include corporate IT-managed laptops.

2. Exemptions: Where there is a formally agreed or approved business need to be exempted from this policy (too costly, too complex, adversely impacting other business requirements) a risk assessment should be conducted and an exception confirmed.

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

Policy

Technical Requirements

1. All Devices must use a current, up-to-date and supported Operating Systems, including all updates and patches/fixes. For example Android, iOS versions must be current with all updates enabled and accepted/installed within a 3-month period.

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 AheadMG's Security Policies. This password must not be the same as any other credentials used within AheadMG.

4. Only devices managed by AheadMG IT will be allowed to connect directly to the company network.

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

User Requirements

1. Users may only load AheadMG or client data that is essential to their role onto their mobile device(s).

2. Users must report all lost or stolen devices to management@aheadmg.com immediately.

3. If a user suspects that unauthorised access to AheadMG data has taken place via a mobile device, they must report the incident in alignment with AheadMG's incident handling process – see: AheadMG Information Security Incident Management Policy and Procedure.

4. Devices must not be "jailbroken" or "rooted" * 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 untrusted sources is forbidden. If you are unsure if an application is from an approved source contact IT (management@aheadmg.com).

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 once a month.

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 AheadMG's policy.

9. Devices must be encrypted in line with AheadMG's Security Policies and guidelines.

10. Users may must be cautious about the merging of personal and work email accounts on their devices. They must take particular care to ensure that AheadMG data is only sent through AheadMG email system. If a user suspects that AheadMG data has been sent from a personal email account, either in body text or as an attachment, they must notify managment@aheadmg.com immediately.

11. The above requirements will be checked regularly and should a device be noncompliant it may result in the loss of access to email, a device lock, or in particularly severe cases, a device wipe.

12. The user is responsible for the backup of their own personal data and AheadMG will accept no responsibility for the loss of files due to a non-compliant device being wiped for security reasons.

13. Users must not use AheadMG's workstations to backup or synchronize device content such as media files, unless such content is required for legitimate business purposes.

**To jailbreak/root 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.*

Actions which may result in a full or partial wipe of the device, or other interaction by IT

1. A device is jailbroken/rooted

2. A device contains an app known to contain a security vulnerability (if not removed within a given time-frame after informing the user)

3. A device is lost or stolen

4. A user has exceeded the maximum number of failed password attempts