Mobile device policy

ISM.03

Version 0.2.3

July 1 2025

Contents

1 Introduction

This policy defines the controls that must be in place to protect mobile device assets. Mobile devices includes any device that is able to be easily transported and fixed devices such as desktops that are not situated in a secure facility. This includes laptops, tablets, smartphones, smartwatches and portable media devices.

Mobile device management (MDM) solutions are used to supervise and enforce critical security settings of mobile devices used by staff to access or process company data.

1.1 Scope

This policy applies to all Everest Engineering permanent employees, contractors, advisors and contracted partners using, or granted access to, information assets and information processing facilities owned by Everest Engineering, our customers (whether contracted or not) and third party partners.

2 Mobile phones

Staff may access email, calendars, Slack and Notion from their personal or Everest Engineering owned mobile phone by using their Everest Engineering Google Workspace account to register the device with our Google Workspace MDM service

2.1 Security updates

Staff are responsible for ensuring their mobiles are kept up to date with security patches.

Staff may not use a mobile for Everest Engineering purposes once security patches are no longer available.

2.2 Configuration

Mobile phones & tablets must be configured so that:

- a lock screen with a PIN, password or biometric challenge is enabled;
- mobiles automatically lock when idle with a maximum idle time of 5 minutes;
- a PIN or password is required to unlock mobiles on boot; and
- storage must be encrypted in case the mobile is lost or stolen.

Devices that are jail broken or otherwise tampered with, may be refused access to company systems.

2.3 Mobile device management

Google MDM manages the device authorisation and user authentication that allows access to our systems. Everest Engineering's Google Workspace mobile device management will collect and store information about the device and the information it has accessed. Google MDM may also enforce security settings and access to any data shared with the device.

Everest Engineering reserves the right to request removal of company information from mobile devices at any time. This includes copies or cloud backups stored in accounts held by individuals. Everest Engineering may also use Google Workspace MDM remote wipe capabilities to remove mobile access and any local cache copies when the request to securely erase data cannot be confirmed by other means.

3 Laptops and home office desktops

All devices that hold information assets belonging to Everest Engineering or our customers must be kept up to date with security patches. Individuals are responsible for ensuring that updates are automatically applied to their work or personal laptops and desktops if they are used for accessing company systems or information. Custodians of shared computing resources such as servers must ensure that security patches are also applied in a timely manner.

3.1 Management of technical vulnerabilities

All devices must be configured to ensure OS and application updates are applied automatically or as soon as practical. Where updates contain fixes for critical or known exploited vulnerabilities, updates must be installed as soon as practical (within 48 hours) or within one month unless otherwise instructed by Everest IT & Security teams.

Commonly-targeted applications such as web browsers and extensions, office suites and email clients must be updated within two weeks of release of updates, or as soon as practical (within 48 hours) if identified as critical by vendors or working exploits exist.

Everest monitors for security vulnerability advisories for operating systems, firmware and installed software in use at Everest. When critical or known exploited vulnerabilities are published by vendors, best effort will be made to test required fixes and staff will be instructed to install required updates as soon as practical (within 48 hours).

3.2 Hardware and software inventory collection

Device management must ensure OS and application versions are inventoried and regularly reviewed.

Accuracy, frequency and coverage of inventory collection must be reviewed quarterly in addition to routine operational monitoring processes.

BYOD devices will be included in inventory collection for monitoring purposes, however to ensure accuracy of company asset registers, device ownership must be tracked as BYOD.

3.3 Mobile device management enrolment

All devices will be enrolled in our device management solution. Devices that cannot be enrolled will be tracked, with appropriate exemptions raised for review and approval prior to use.

Where a device or operating system is not supported by Everest's device management capability, equivalent inventory collection and risk mitigation processes must be developed to protect data stored on the device prior to approval for use.

Laptops enrolled in a Customer's MDM must be tracked for the duration of the engagement and re-enrolled in Everest's MDM prior to use on other projects. Customer MDM enrolments must be reviewed at least quarterly to ensure re-enrolment in Everest MDM at the end of the engagement.

3.4 Management of software

Everest core applications and paid software will be managed by Everest including the installation, configuration and updates for vulnerability and license management purposes.

Software installed on company laptops (including BYOD) must comply with Everest Software Use and Anti-Malware policies

Additionally, Everest monitors for and prevents installation or use of software described in "ISM-17 Software Use Policy" section "Prohibited Use"

3.5 Endpoint protection

All devices used to access company data shall be protected by endpoint protection software and policies to enforce security posture and protect against malware.

To ensure the protection of data and company systems, Everest may remote lock, network isolate or equivalent actions in the event that endpoint protection detects indicators of compromise on a device.

To manage risk to company devices from malicious sites and malware, Everest may monitor and block sites identified as high risk or known to contain malware.

Endpoint protection software will include both real time file integrity and signature based detection in addition to periodic file system scans.

Security posture of endpoints will be managed to ensure;

- Encryption of data at rest (OS native file system encryption)
- Automatic screen lock after 15 minutes of inactivity
- Password required to resume after sleep, hibernate or power on
- Host firewall is enabled
- Operating system security updates are set to automatically install
- Prevent installation of software that violates software or acceptable use security policies

3.6 Bring your own device

Staff may choose to use a "bring your own device" (BYOD) laptop or desktop instead of an Everest Engineering supplied device. Staff choosing to use a BYOD device must consent to installing and configuring Everest's standard device security configuration, endpoint protection and to abide by acceptable use policy.

Systems that are not able to install our endpoint protection agent or implement other security controls *may be* permitted by exception. Exceptions must be tracked and regularly reviewed.

BYOD devices used for Everest or client work at Everest may be subject to inspection or remote wipe to ensure removal or all company and client data prior to leaving the organisation.

4 Data security classification and tracking

Our data security classification policy applies to all devices that store or process Everest Engineering information assets or those of our customers. This requires all devices to have a data security classification label assigned and to be tracked in our asset register.

Devices may only be used to store and process information assets that has an equal or lesser security label than that assigned to the information assets.