OGC® DOCUMENT: ISPG-SM03

External identifier of this OGC® document:

OGC®
Making location count.

# PRACTICE GUIDE FOR MOBILE SECURITY

STANDARD
Implementation

APPROVED

**Version:** 1.1
**Submission Date:** XXX
**Approval Date:** XXX
**Publication Date:** 2018-07
**Editor:**

**Warning:** This document is an OGC Member approved international standard. This document is available on a royalty free, non-discriminatory basis. Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

## License Agreement

Suggested additions, changes and comments on this standard are welcome and encouraged. Such suggestions may be submitted using the online change request form on OGC web site: http://portal.opengeospatial.org/public_ogc/change_request.php

## Copyright notice

## Note

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. The Open Geospatial Consortium shall not be held responsible for identifying any or all such patent rights.

Recipients of this document are requested to submit, with their comments, notification of any relevant patent claims or other intellectual property rights of which they may be aware that might be infringed by any implementation of the standard set forth in this document, and to provide supporting documentation.

# CONTENTS

1

# COPYRIGHT NOTICE

# 1 COPYRIGHT NOTICE

AMENDMENT HISTORY

| CHANGE NUMBER | REVISION DESCRIPTION | PAGES AFFECTED | REVISION NUMBER | DATE |
|---|---|---|---|---|
| 1 | Renamed the document from "Practice Guide for Mobile Device Security 1.0" to "Practice Guide for Mobile Security 1.1", added new chapters on information security management and mobile app development, and aligned references with other practice guides. | Whole document | 1.1 | July 2018 |

2

# INTRODUCTION

# 2 INTRODUCTION

Mobile devices are getting more common and allow users to access information from anywhere at any time. This changes the mode of Internet usage and also brings together new risks in daily operations. While mobile devices and mobile applications (apps) installed in the devices bring convenience and improve efficiency, insecure protection of mobile devices or insecurely written mobile apps pose risks to mobile users and may cause data loss or reputation damage to the app owner. In view of the extra risks introduced by mobile devices due to its high portability, wireless connection capabilities and diverse techniques in mobile app development, this practice guide is developed to provide guidance notes for Bureaux/Departments (B/Ds) to make reference in securing the use of mobile devices in their business and the development of mobile apps for business use.

## 2.1. PURPOSE

The purpose of this document is to provide common security considerations and best practices to B/Ds on the management and use of mobile devices as well as secure development of mobile apps. The best practices on the use and management of mobile devices are described in Clause 5 and they are intended for staff who are involved in the use and adoption of mobile devices and related management solutions. The security best practices on mobile app development are described in Clause 6 and they are intended for developers who are involved in related development life cycle.

This document should be used in conjunction with established government requirements and documents including the Baseline IT Security Policy [S17], the IT Security Guidelines [G3] and other relevant procedures and guidelines, where applicable. In addition to government security requirements, B/Ds should also assess the security risks before adoption of mobile device solutions based on their business needs. B/Ds should consider the security measures and best practices recommended in this document and implement adequate security protection for their mobile solutions.

The materials included in this document are general in nature and are prepared irrespective of the types or platforms of the mobile devices. According to the definition in government security documents, the term “mobile devices” means portable computing and communication devices with information storage and processing capability. Examples include portable computers, mobile phones, tablets, digital cameras, and digital audio or video recording devices. Readers should consider and select the security measures and best practices that are applicable to their own environment.

## 2.2. NORMATIVE REFERENCES

The following referenced documents are indispensable for the application of this document.

- Baseline IT Security Policy [S17], the Government of Hong Kong Special Administrative Region
- IT Security Guidelines [G3], the Government of Hong Kong Special Administrative Region
- Information technology — Security techniques — Information security management systems — Requirements (second edition), ISO/IEC 27001:2013
- Information technology — Security techniques — Code of practice for information security controls (second edition), ISO/IEC 27002:2013
- Information technology — Security techniques — Governance of information security, ISO/IEC 27014:2013
- Information technology — Security techniques — Storage security, ISO/IEC 27040:2015

## 2.3. TERMS AND CONVENTION

For the purposes of this document, the terms and convention given in S17, G3, and the following apply.

**ABBREVIATION AND TERMS**

| | |
|---|---|
| NA | NA |

## 2.4. CONTACT

This document is produced and maintained by the Office of the Government Chief Information Officer (OGCIO). For comments or suggestions, please send to:

Email: it_security@ogcio.gov.hk

Lotus Notes mail: IT Security Team/OGCIO/HKSARG@OGCIO

3

# INFORMATION SECURITY MANAGEMENT

# 3 INFORMATION SECURITY MANAGEMENT

Information security is about the planning, implementation and continuous enhancement of security controls and measures to protect the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission and its associated information systems. Information security management is a set of principles relating to the functions of planning, organising, directing, controlling, and the application of these principles in harnessing physical, financial, human and informational resources efficiently and effectively to assure the safety of information assets and information systems. Information security management involves a series of activities that require continuous monitoring and control. These activities include but not limited to the following functional areas:

- Security Management Framework and the Organisation;
- Governance, Risk Management, and Compliance;
- Security Operations;
- Security Event and Incident Management;
- Awareness Training and Capability Building; and
- Situational Awareness and Information Sharing.

## 3.1. SECURITY MANAGEMENT FRAMEWORK AND ORGANISATION

B/Ds shall establish and enforce departmental information security policies, standards, guidelines and procedures in accordance with the business needs and the government security requirements.

B/Ds shall also define the organisation structure on information security and provide clear definitions and proper assignment of security accountability and responsibility to involved parties.

## 3.2. GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE

B/Ds shall adopt a risk-based approach to identify, prioritise and address the security risks of information systems in a consistent and effective manner.

B/Ds shall perform security risk assessments for information systems and production applications periodically and when necessary so as to identify risks and consequences associated with vulnerabilities, and to provide a basis to establish a cost-effective security program and implement appropriate security protection and safeguards.

B/Ds shall also perform security audit on information systems regularly to ensure that current security measures comply with departmental information security policies, standards, and other contractual or legal requirements.

## 3.3. SECURITY OPERATIONS

To protect information assets and information systems, B/Ds should implement comprehensive security measures based on their business needs, covering different technological areas in their business, and adopt the principle of "Prevent, Detect, Respond and Recover" in their daily operations.

- Preventive measures avoid or deter the occurrence of an undesirable event;
- Detective measures identify the occurrence of an undesirable event;
- Response measures refer to coordinated actions to contain damage when an undesirable event or incident occurs; and
- Recovery measures are for restoring the confidentiality, integrity and availability of information systems to their expected state.

## 3.4. SECURITY EVENT AND INCIDENT MANAGEMENT

In reality, security incidents might still occur due to unforeseeable, disruptive events. In cases where security events compromise business continuity or give rise to risk of data security, B/Ds shall activate their standing incident management plan to identifying, managing, recording, and analysing security threats, attacks, or incidents in real-time. B/Ds should also prepare to communicate appropriately with relevant parties by sharing information on response for security risks to subdue distrust or unnecessary speculation. When developing an incident management plan, B/Ds should plan and prepare the right resources as well as develop the procedures to address necessary follow-up investigations.

## 3.5. AWARENESS TRAINING AND CAPABILITY BUILDING

As information security is everyone's business, B/Ds should continuously promote information security awareness throughout the organisations and arrange training and education to ensure that all related parties understand the risks, observe the security regulations and requirements, and conform to security best practices.

## 3.6. SITUATIONAL AWARENESS AND INFORMATION SHARING

As cyber threat landscape is constantly changing, B/Ds should also constantly attend to current vulnerabilities information, threat alerts, and important notices disseminated by the security industry and the GovCERT.HK. The security alerts on impending and actual threats should be disseminated to and shared with those responsible colleagues within B/Ds so that timely mitigation measures could be taken.

B/Ds could make use of the cyber risk information sharing platform to receive and share information regarding security issues, vulnerabilities, and cyber threat intelligence.

4

# INTRODUCTION TO MOBILE SECURITY

# 4 INTRODUCTION TO MOBILE SECURITY

As technologies advance, the computational power of mobile devices continues to increase, and at the same time they become even smaller and lighter. While there are many obvious advantages with these devices, they also bring security concerns that need to be addressed. Also, while mobile apps bring much convenience to users, poorly written mobile apps increase risk of data loss. This section highlights the security measures and best practices to address the common security concerns and illustrates how they should be incorporated in the major stages of mobile device management life cycle and mobile app development life cycle. B/Ds may select and map the security measures and best practices to their own management and development life cycle model based on their business needs.

## 4.1. SECURITY CONCERNS OF MOBILE TECHNOLOGIES

Security threats to mobile devices come from many directions. Mobile devices often need additional protection because their nature generally places them at higher exposure to threats than other client devices, such as a workstation in the office area. Major threats to mobile devices can come from the device itself, network (e.g. mobile, internet) or application (e.g. mobile app, mobile web app). The security concerns of mobile technologies are highlighted below:

**Device**

- Lack of physical security controls

  Mobile devices are typically used in a variety of locations outside the B/Ds' control, such as employees' homes, coffee shops, hotels, and conferences. The devices' mobile nature makes them much more likely to be lost or stolen than other devices, so their data is at increased risk of compromise.

- Insufficient control to accessories in mobile devices

  Mobile devices are usually equipped with cameras and microphones. Inappropriate video capturing, audio recording and photo taking may cause a security concern. Moreover, sensitive information in video/audio records or photos might be retrieved by unauthorised persons if the mobile device is not properly protected.

- Use of untrusted mobile devices

  Many mobile devices, particularly those that are privately owned, are not necessarily trustworthy. The use of mobile devices that have been jailbroken or rooted can pose additional security risks because the built-in restrictions on security have been bypassed in such devices.

### Network

- Use of untrusted networks

  Mobile devices primarily use non-organisational networks, such as external Wi-Fi or cellular networks, for Internet access. These networks are susceptible to eavesdropping, which place sensitive information transmitted at risk of compromise.

- Use of unsecure communication technologies

  In contrast to workstations in the office area which mainly rely on Local Area Network (LAN) or office Wi-Fi for communication, mobile users can deploy a wide variety of communication technologies such as Bluetooth, Near Field Communication (NFC) for data connection. Every communication technology has its own security risk. If sensitive information is intercepted over an unsecure communication media, it would lead to a security breach.

### Application

- Use of untrusted apps

  Mobile devices are designed to make them easy to find, acquire, install, and use third-party applications from mobile app stores. This poses obvious security risks, especially when mobile device platforms and mobile app stores do not place security restrictions or other limitations on the published applications developed by third-party.

- Use of location services

  Location services are commonly used by social media, navigation, web browsers, and other mobile-centric applications to identify the locations of mobile devices and its owner. Mobile devices with location services enabled are at increased risk of targeted attacks because it is easier for potential attackers to determine where the user and the mobile device are, and to correlate that information with other sources to launch attacks such as spear phishing.

- Use of untrusted source

  Mobile apps may induce untrusted input from malicious source that are not common to other types of devices. An example is the 2D barcode, which are now commonly used because camera is a built-in component in today's smartphones and tablets. This could induce targeted attacks, such as placing malicious 2D barcodes at a public location.

The above paragraphs discuss on the general security concerns on mobile technology and its application. When developing mobile apps, further security risks need to be addressed. The developer can refer to Open Web Application Security Project (OWASP) Mobile Top 10 to understand those critical risks that mobile app development faces. B/Ds should take reference of these common security risks and avoid such problems in their codes. B/Ds should also review and define the security requirements of their applications to mitigate risks so as to avoid vulnerabilities originated from security design. The risks as mentioned by OWASP are highlighted below:

- Improper Platform Usage

  The potential threat comes from the misuse of a platform feature and failure to use platform security controls, e.g., Android intents, platform permissions, misuse of biometric recognition features or other security controls of the mobile operating system. Misusing platform features may put the system under risk (e.g., cross-site scripting).

- Insecure Data Storage

  Insecure data storage vulnerabilities occur when development teams assume that users or malware will not have access to a mobile device's filesystem and subsequent sensitive information on the device. This can result in data loss or extraction of the app's sensitive information via mobile malware, modified apps or forensic tools.

- Insecure Communication

  Insecure communications from one point to another put the app data at risk of exposure, which may cause possible leakage of sensitive information over the network communication. The issue could be caused by poor handshaking, incorrect SSL versions, weak negotiation and plain text communication of sensitive assets.

- Insecure Authentication

  Attackers may compromise passwords, keys, or authentication tokens to impersonate the identity of other users. The issue could be caused by the absence or improper implementation of authentication mechanisms and bad session management.

- Insufficient Cryptography

  Attackers may steal or access poorly protected data resulting from missing or improper use of cryptographic functions to encrypt sensitive information assets.

- Insecure Authorisation

  Attackers may bypass the authorisation mechanism and execute over-privileged functionality. The issue could be caused by the failure of a server to correctly enforce identity and permissions as defined by the mobile app, if the mobile app only trusts the client-side authorisation but fails to perform server-side authorisation.

- Client Code Quality

  Poor client codes may lead to vulnerabilities such as buffer overflows and memory leaks by passing malicious input to the mobile app. This may result in foreign code execution or denial of service on remote server.

- Code Tampering

  Attackers may modify a mobile app via creating malicious forms of the app hosted in third-party locations. The attacker may also use phishing attacks to induce user for installation.

- Reverse Engineering

  Attackers may analyse the core binary of the mobile app and perform reverse engineering to obtain its source code, libraries, algorithms and other assets with the aim of exploiting vulnerabilities, harvesting sensitive data or stealing intellectual property.

- Extraneous Functionality

  Developers may add hidden backdoors or functions during application debugging. If the developer forgets to remove such backdoors before production, attacker can make use of them to perform malicious attacks.

5

# MOBILE DEVICE SECURITY

# 5 MOBILE DEVICE SECURITY

This section is intended for users and administrators who are involved in the use and adoption of mobile devices and related management solutions. For developers who need to understand the details on protection measures for mobile app development, please refer to “Clause 6 — Mobile App Development Security” for details.

## 5.1. MOBILE DEVICE USAGE LIFECYCLE

Similar to other information systems, mobile devices include three major stages throughout their usage lifecycle — Provision, Usage and Decommission. The paragraphs below discuss the best practices on how to protect the mobile devices in various stages of the lifecycle.

### 5.1.1. Provision of Mobile Devices

When considering adoption of mobile device technologies in business, B/Ds should identify the needs for mobile device and how mobile device solutions can support their business. A mobile device security policy should be established to specify the business and security requirements for the use of mobile device technologies with the following considerations:

- The types of approved mobile devices and the approval mechanism.
- The data classification permitted on each type of mobile device. Sensitive information shall not be stored in privately-owned mobile devices.
- The control mechanism to ensure the compliance with government security requirements based on the data classification.
- The procedures to ensure timely sanitisation of government data stored in the mobile devices when staff is posted out or ceases to provide services.

Based on the business and security requirements, B/Ds should develop adequate processes and procedures for provision of mobile device. In particular, security hardening procedures of mobile devices should be developed to enforce security configurations in accordance with government security requirements and the mobile device security policy. All mobile devices should be hardened according to the security hardening procedures before transferring to users. For sample configurations regarding security hardening, please refer to Annex A.

B/Ds should review and modify their processes and procedures with necessary adjustments to include the following best practices in the provisioning stage:

- Identify the list of supported models that fulfils the operation and security requirements.

- Perform risk assessments prior to deployment of new mobile device models, and implement a continuous risk monitoring mechanism for evaluating changes in or new risks associated with the mobile devices.
- Install security control tools, such as Mobile Device Management (MDM)[1], Data Loss Prevention (DLP), personal firewall software and anti-malware solution whenever feasible. The tools should be mentioned in B/Ds' hardening procedures.
- Deploy ONLY authorised applications into government mobile devices. Users may install third-party applications if they are authorised by an officer as designated by the B/D. B/Ds shall define and maintain a list of authorised software including freeware, open source software and programming libraries based on operational needs.
- Perform security hardening and deliver hardened mobile devices to users.
- Disseminate the acceptable use policy and security reminders to users to remind them to apply security best practices.
- Obtain users' acknowledgement on receiving the acceptable use policy, security reminders and the mobile devices in good condition. The acknowledgement can be a signed agreement or email.
- Enable a power-on password.
- Deploy minimal password length and complexity requirements according to B/Ds' departmental security requirements.
- Configure the mobile device in such a way that it locks automatically after a period of inactivity.
- Enable data erasing feature when there is consecutive incorrect attempts to enter the password if available. The actual number of consecutive incorrect attempts should be defined according to B/Ds operational needs. Remote wipe functionality should also be enabled to protect data from device lost or stolen. Moreover, selection of wiping solution should be carefully made such that sensitive data should not be recovered after the wipe.
- Enable device level, full disk or file based encryption feature for all storages of mobile devices, where possible.
- Consider using multiple factors authentication such as digital certification together with password for VPN connections.
- Maintain asset-tracking information such as serial number, inspect applications on devices, and keep track of them for audit.

[1] MDM is an application (or a set of applications) that provides management capabilities in policy, inventory, security and service for mobile devices such as mobile phones and tablets. For details of MDM, please refer to Clause 5.2 Mobile Device Management Solution

## 5.1.2. Use of Mobile Devices

Even if the security controls have been implemented in the provisioning stage, people and process are two important factors for keeping mobile devices in a safe environment. Therefore, this section focuses on the best practices related to the on-going operation process for the management and use of mobile devices.

### 5.1.2.1. Administrators

Administrators should follow the best practices as follows:

- Check available upgrades and/or patches for the mobile device OS and mobile applications with proper change management.
- Apply the verified update and/or patches to mobile devices.
- Check the status of mobile devices regularly to ensure security measures are in place. Use of jail-broken, rooted and compromised devices should be detected and restricted.
- Maintain an inventory record for government mobile devices with user information and a list of installed mobile applications.
- Maintain a list of approved desktop or mobile applications for mobile devices which are defined by officer as designated by the B/D.
- Enforce hardware encryption of a mobile device whenever possible.

### 5.1.2.2. Mobile Users

Users should follow the acceptable use policy and security reminders including but not limited to:

**DON'Ts:**

- Do not modify mobile device setting unless approval is obtained.
- Do not try to perform jailbreaking / rooting or exploit the OS of a mobile device by using unauthorised tool. Such manipulation may introduce unexpected security risk and void the warranty.
- Do not allow wireless connections from unknown or un-trusted sources on your device.
- Do not open or access links in social media, instant message, Short Message Service (SMS), Multimedia Messaging Service (MMS), or email from misleading, suspicious or un-trusted sources.

- Do not download programs and contents from unknown or un-trusted sources.
- Do not install illegal or unauthorised software on the mobile device.
- Do not connect to external data network directly (e.g. via cellular network) when the mobile device is connected to government internal network.
- Do not use public printers.
- Do not allow any mobile applications to automatically upload or synchronise information from a mobile device to other unauthorised devices. Example includes the public cloud storage vendor, photo sharing social media and mobile vendor backup solutions by cloud technology.
- Do not store password of any other systems (e.g. email, ATM card and network login) on mobile device. The password auto-save function should be disabled.
- Do not use government provided mobile device extensively for private or personal activities.

**DOs:**

- Follow security procedures defined by B/D.
- Install only approved applications as provided by B/Ds.
- Ensure the security features of the OS and installed applications are enabled as specified in the hardening procedures.
- Apply latest malware signatures and definitions, if available.
- Stay alert on security vulnerabilities on mobile devices, and follow the instructions to apply the relevant patches according to the affected systems and versions list.
- Perform full data backup with encryption regularly to authorised computers or storage. If the device contains sensitive information, the protection of backup copies shall follow prevailing government security requirements.
- Turn off wireless connections such as Wi-Fi, Near Field Communication (NFC), Bluetooth and/or infrared connectivity when not in use.
- Disable the Wi-Fi auto-connect option to avoid connecting to un-trusted/rogue network automatically.
- Turn off location services setting in your mobile device if it is not necessary to run location-based application.
- Be cautious when connecting to publicly available Wi-Fi hotspots, and do not access government data unless with adequate security protection.

- Establish a VPN connection to your B/D's government internal network. This can ensure that all data transmission would be subject to the corresponding security controls.
- Safeguard a mobile device in your possession and do not leave the device unattended without proper security measures.
- Be aware of surrounding environment when handling sensitive information to mitigate the risks of overhearing and peeping.

#### 5.1.2.3. Awareness Training

User training is an important activity to promote user security awareness in using mobile devices. Government staff should understand security requirements from mobile user's point of view such that human error can be minimised. Training to mobile users should be arranged such that a certain level of understanding of security requirement in mobile devices, the security measure and security threats can be delivered to users.

General speaking, the awareness training to mobile users should include:

- Security requirements for mobile devices in using and decommissioning stage.
- Reporting mechanism of lost or stolen mobile device.
- Information classification and corresponding security requirements for sensitive information in mobile devices.
- Recent mobile devices security news and trends as time goes by.

### 5.1.3. Decommissioning of Mobile Devices

At the last stage of mobile device management, the devices may be decommissioned due to physical damage, end of support, re-issue to other staff or other B/Ds, etc. B/Ds should define device decommission procedures consisting of secure data deletion, mobile devices factory reset and disposal such that mobile device can be re-used or securely disposed without data leakage. Mobile users and administrators should follow the procedures in order to protect government data in safe custody and reduce the chance for data leakage to unauthorised parties.

For loss or theft of mobile devices, please refer to Clause 5.3.3 which provides best practices for handling this scenario in details that mobile users and administrators should follow.

#### 5.1.3.1. Administrators

Administrators should follow the best practices as follows:

- Verify the condition of the returned device.

- Check whether sensitive information has been processed and/or kept in the device. If in doubt, it should be assumed that it has.
- Clear or destroy government data securely before disposal, reuse or repair. If the device contains sensitive information, administrators shall follow government security requirements. For physical damage, mobile users should inform administrators the classification of information stored within the damaged mobile device.
- Perform vendor factory reset, if available.

#### 5.1.3.2. Mobile Users

Users should follow the best practices as follows:

- Perform necessary data backup for B/Ds' operations.
- Clear or destroy information securely before returning the mobile devices to administrators who may not be legitimate to access that information. For information erasure, please refer to the corresponding section in IT Security Guidelines and the Practice Guide for Destruction and Disposal of Storage Media.
- Return the mobile device as soon as possible.

## 5.2. MOBILE DEVICE MANAGEMENT SOLUTION

Centralised Mobile Device Management (MDM) technologies are becoming popular as a solution for controlling the use of mobile devices issued by the organisation or owned by individual staff. MDM solution provides additional management capability such that B/Ds should consider using such solution to maintain proper management to their mobile devices.

### 5.2.1. Capabilities of Mobile Device Management Solution

MDM solution provides management capabilities in policy, inventory, security and service for mobile devices such as mobile phones and tablets. Generally speaking, the technical capabilities include:

- Containerisation — provides an isolated environment for processing data via physical, virtual or per-app container (Please refer to Annex B).
- Wipe remotely when mobile device is lost or stolen, if available.
- Data wipe after repeated logon attempt failure.

- Deploy and configure mobile devices with pre-configured setting.
- Enforce security controls such as using VPN for encrypting information transmission over wireless network.
- Provide audit trailing details on data accessing.
- Monitor abnormal activities.
- Control mobile application installation and removal.

The above capabilities are examples only and not indicated as mandatory requirements for B/Ds when selecting their MDM solution. B/Ds should consider the needs to enforce security controls with alternative solutions where applicable with regard to their own business and operation environment.

### 5.2.2. Best Practices on Mobile Device Management Solution

The following are some best practices commonly enforced through MDM solution for security management of mobile devices.

- Enforcement of Security Policy

  With the help of MDM technologies, technical measures could be uniformly enforced on all departmental mobile devices in accordance with the departmental IT security policy and other relevant policies, procedures and guidelines. The configured MDM security policies should be documented and reviewed regularly.

- Secure Data Communication and Storage

  Data communications between the managed mobile devices and B/Ds' backend services should be protected by strong encryption, such as Virtual Private Network (VPN) technologies. Data stored on both built-in storage and removable media storage should also be protected by strong encryption. Data within the containers should be also encrypted. No copy/paste and cut/paste are permitted outside the MDM realm. Remote wipe functionality should be enabled in case the device has been lost or stolen. After a certain number of incorrect authentication attempts, the device should wipe itself automatically.

- User and Device Authentication

  To access internal resources, the user and the device itself should be authenticated via various means, for example, network-based device authentication, password authentication, and token-based authentication. After idled for a predefined period, the device should be locked automatically. Remote lock functionality should be enabled such that administrators could lock the device remotely in case the device is believed to be lost, stolen, or left in an unsecured location.

- Enterprise Mobile Application Management

  B/D's mobile applications should be distributed from a single, trusted mobile app store. The digital signatures should be verified to ensure that only applications from trusted sources could be installed on the device. Whitelisting should be used to further restrict which applications may be installed on B/Ds' mobile devices. An up-to-date inventory of all applications installed on each device should be maintained. Last but not least, the synchronisation services of mobile application should be disabled if not needed.

### 5.2.3. Other Considerations of Mobile Device Management Solutions

Some other considerations of MDM solutions for mobile devices are depicted as follows:

- MDM solution may not be available for portable computer OS as MDM software is primarily designed for mobile phones and tablets OS instead of computer OS.
- Data erasing feature after consecutive incorrect attempts for portable computer OS is yet to be a common feature while data erasing is commonly available for major mobile OS.
- Some OSs of mobile devices are customised by manufacturers, administrators or mobile users may not be able to apply security patches for known vulnerabilities in a timely manner.

## 5.3. SCENARIO SPECIFIC SECURITY GUIDANCE

This section provides security guidance focusing on different scenarios of government staff in using mobile devices, including: handling sensitive information, sharing of mobile devices within B/Ds, and loss or theft and security incident relating to mobile device. Other than the best practices mentioned in Clause 5.1, these scenarios may commonly occur in daily operation with noticeable impact to mobile device security. Example includes improper sensitive information handling, data leakage to other teams through device sharing or loss/theft of mobile devices, and attacks to mobile devices due to software vulnerabilities.

### 5.3.1. Handling Sensitive Information with Mobile Devices

In compliance with the security requirements of the Government, B/Ds shall observe government security requirements and documents. In addition, B/Ds should adopt the following security practices to protect mobile devices and information against common security threats:

- Do not process or store TOP SECRET or SECRET information on mobile devices.

- Encrypt all sensitive information when stored in and transmitted from a mobile device.
- Minimise storing of sensitive information on a mobile device.
- Do not store sensitive information on mobile device, except the information is protected with appropriate security measures.
- Do not synchronise sensitive information from a mobile device to public cloud storage, privately-owned IT equipment or other unauthorised devices.
- Completely clear or destroy all sensitive information in a mobile device when it is no longer required, and protect the storage of the device until disposal or re-use.
- Do not store sensitive information in privately-owned mobile devices.
- If the mobile device contains sensitive information, put the mobile device in a secure place and keep it in a locked room or cabinet, when not attended.
- Use privacy screen filter to narrow the viewing angle and position carefully the display screen so that sensitive information cannot be peeked by unauthorised persons.
- Configure multi-level password control for use of a mobile device and access to sensitive information, if possible.
- Do not capture screen displaying any sensitive information.
- Do not allow sensitive information to be transferred to the facilities of public IT services and vendors' backup services.
- Remind mobile users to inform administrators or the responsible party as soon as possible about any loss, theft or damage of government mobile device. Mobile user is responsible for the security and should protect the mobile devices from theft, loss and damage at all times.

### 5.3.2. Shared Access to Mobile Devices

Shared access to government mobile devices should be prohibited unless among persons who are authorised to access all the information stored on the device. Shared access should be authorised based on operational need. Example includes departmental mobile device accessing information within a team, testing device for mobile application development, and outside work and roster based jobs such as data centre operation. B/Ds should ensure that all activities in relation to sensitive information are tracked by audit trails and logical access control software in case shared access is needed.

If there is operational need for sharing mobile devices across government staff, the staff should observe the following best practices:

- Store information based on need-to-know basis.

- Do not perform any backup unless authorised.
- Log out all applications after use or when handing over to other staff.
- Do not configure or store individual email account and password.

### 5.3.3. Loss, Theft and Security Incident

Mobile devices are usually small in size and easy to be stolen or lost. B/Ds should review and modify their security incident handling procedures with necessary adjustments for incident handling of lost or stolen devices. Users should report promptly and escalate if an information security incident occurs in accordance with the security incident handling procedures.

In particular, B/Ds should consider including the following best practices for handling lost or stolen mobile devices:

- Revoke the user accounts that may have been compromised.
- Remotely wipe the data stored on the lost or stolen devices, whenever technically possible.
- Establish, test and regularly review the handling procedures for handling lost or stolen mobile devices.
- Report the incident to the Government Information Security Incident Response Office (GIRO) if sensitive data is involved.

## 5.4. SECURITY GUIDANCE ON PRIVATELY-OWNED MOBILE DEVICES

One basic security concern related to using privately-owned mobile devices in organisational environment is the role of ownership[2]. With the sole control of their mobile devices, staff may install any mobile applications based on their own preferences, which may introduce malware to the mobile devices. In addition, staff may modify the booting up software and/or firmware of their mobile devices to override vendors' defined security controls so as to gain more control and flexibility on the devices. In view of the above security risks together with the risk of data leakage due to the loss of the devices to the wrong hands, using privately-owned mobile devices for business purpose should not be allowed unless with adequate security protection.

[2] Bring your own device Security and risk consideration for your mobile device program http://www.ey.com/Publication/vwLUAssets/EY_-_Bring_your_own_device:_mobile_security_and_risk/$FILE/Bring_your_own_device.pdf

When considering adopting mobile device solution involving privately-owned mobile devices, B/Ds should observe government security requirements about use of privately-owned IT equipment. In addition, S17 section 20.1.3 requires that unclassified information should also be protected from unintentional disclosure.

Mobile Device Management (MDM) and Mobile Data Loss Prevention (Mobile DLP) are two possible technical solutions for protecting government information from unauthorised access when using privately-owned mobile device for business purpose. MDM is more focused on device's management capability while mobile DLP emphasises on data controls. B/Ds may refer to the Practice Guide for Data Loss Prevention for additional considerations in protecting government information under different scenarios. The security services supported by a typical MDM solution are specified in Clause 5.2.1.

## 5.5. RESTRICTIONS ON MOBILE DEVICES AND ACCESS LEVELS

B/Ds should specify their business and security requirements for the use of mobile device technologies in the mobile device security policy. For example, B/Ds may limit the types of mobile devices (by operating system version, by brand/model of mobile phone, etc.) and require tiered levels of access, such as allowing government provided mobile devices to access many resources, while privately-owned mobile devices running the B/D's mobile device management client software to access a limited set of resources.

B/Ds should make their own risk-based decisions about what levels of access should be permitted from which types of mobile devices. Some factors that B/Ds should consider when setting mobile device security policy are highlighted in the following:

- Compliance with government security requirements

  Privately-owned mobile devices for business purpose should not be allowed unless adequate security protection is enforced in accordance with government security requirements.

- Sensitivity of work

  Some work involves access to sensitive information or resources, while other work does not. B/Ds may have more restrictive requirements for work based on their business needs.

- Technical limitations

  Certain types of mobile devices or operating systems may be needed, such as those with hardware-based security features or those running a particular mobile device management client software.

- Work location

  Risks will generally be lower for devices used only in the environment under B/Ds’ direct control than for devices used in a variety of locations.

6

# MOBILE APP DEVELOPMENT SECURITY

# 6 MOBILE APP DEVELOPMENT SECURITY

This section is intended for developers who are involved in mobile app development life cycle. For users and administrators who are involved in the use and adoption of mobile devices and related management solutions, please refer to Clause 5 — Mobile Device Security.

## 6.1. CONSIDERATIONS IN MOBILE APP DEVELOPMENT

Mobile apps are also susceptible to different threats as the applications are now used to access sensitive information and perform business critical activities. As a best practice, to develop and maintain secure mobile apps, various security considerations and measures, both technical and administrative, need to be implemented during different stages of mobile app development.

The methodology on software development is evolving with new development style such as agile software development, DevOps / DevSecOps (compounding "development", "security" and "operations") for continuous integration and continuous delivery to build mobile apps faster and/or more secured using an iterative development process. It focuses on continuous communication, integration, measurement and delivery to foster the processes between app development, testing and quality assurance. No matter what methodology is used, design for a secure mobile app should be embedded into every stage of development life cycle, in particular early stage, so as to minimise security risk and avoid re-work due to design deficiency.

The following are common stages and key security considerations to help identify potential security risks in mobile app development:

| DEVELOPMENT LIFE CYCLE | SECURITY CONSIDERATIONS |
|---|---|
| Requirement | Security requirements should be defined along with functional requirements and further incorporate security during other phases of software development. |
| Design | Design the application architecture in accordance with the security specifications aligned in the requirement stage. |
| Development | Develop the mobile app following secure coding best practices and perform source code security assessment |
| Testing | Validate the performance, accuracy and security of system functionalities. |
| Pre-production | Perform security risk assessment and security audit |
| Maintenance and Support | Maintain security assurance with continuous testing and appropriate security controls. |
| Decommission | Decommission the app when it no longer serves the purposes. |

# 6.2. MOBILE APP DEVELOPMENT LIFECYCLE

## 6.2.1. Requirement Stage

Security should be considered during the requirement phase so that security is included throughout the development life cycle. Security requirements should be defined along with functional requirements and further incorporate security during other phases of software development. If the requirements are defined properly, identified risks could be addressed in early stages, which can greatly reduce extra work in later stages and remediation effort. The following areas should be considered for security requirements:

- Architecture, Design and Threat Modelling Requirements

  Process should be in place to ensure the security concern has been explicitly addressed when planning the architecture and design of the mobile app. The functional and security roles of each component should be well defined. Topics such as threat modelling, secure development and key management should be covered. For example, apply relevant and sufficient security controls to safeguard the data and transactions before implementation.

- Data Storage and Privacy Requirements

  Developer should have good understanding on the type and sensitivity of data to be handled and if any critical transaction would be involved. Sensitive data can be unintentionally exposed to other apps on the same device and data may also be leaked during transmission. Moreover, mobile devices are more easily lost or stolen compared to other types of devices. Developers should adhere to concerned laws and regulations on privacy, e.g., Personal Data (Privacy) Ordinance, in order to define a suitable data storage and privacy requirements. Privacy Impact Assessment (PIA) should be conducted if the mobile app has significant privacy implications.

- Cryptography Requirements

  Cryptography should be adopted in protecting the data stored and processed on a mobile device, or in transit between the device and servers. Ensure the mobile app uses cryptography according to industry best practices, including:

  a) Use of proven cryptographic libraries.

  b) Proper choice and configuration of cryptographic primitives.

  c) Do not reuse the same cryptographic key for multiple purposes.

  d) Generate random values using a sufficiently secure random number generator.

- Authentication and Session Management Requirements

  User accounts and sessions should be properly authenticated and managed. This includes using randomly generated access tokens to authenticate client requests, enforcing explicit password policy, and locking of user account when excessive login attempts are found, etc. Application should also be properly handled for change of states, such as requiring re-authentication when the app resumes from background.

- Network Communication Requirements

  Developer should ensure the confidentiality and integrity of information exchanged between the mobile apps and remote service endpoints. Encrypted channel using the TLS protocol with appropriate settings should be used for handling all application data. When using TLS, the apps must enforce certificate validation functions and should not accept self-signed and/or un-trusted certificates. Apps should also be able to detect the use of unauthorised certificates to defend against network attack (e.g., man-in-the-middle attacks).

- Platform Interaction Requirements

  Platform application program interfaces (APIs) and standard components in a secure manner including communications between apps (inter-process communications, e.g. communication of APIs resided in different containers) should be considered.

- Code Quality and Build Setting Requirements

  Security coding practices should be followed in developing the app. For example, the app should be signed with trusted certificate. Mobile device default accessed entitlement should be reduced to minimum (e.g. disable camera/microphone and enable “Do Not Track” by default).

- Resilience Against Reverse Engineering Requirements

  If the mobile app will process or access sensitive information, protection measures should be applied to increase the app’s resiliency against reverse engineering. A list of obfuscation controls such as “app isolation”, “impede dynamic analysis and tampering”, “device binding” and “emulator detection” should be considered.

### 6.2.2. Design Stage

The design stage involves designing the application architecture in accordance with the specifications aligned in the requirement stage. As application architecture is established, development team should review the system design by identifying possible compliance issues as well as security risks with reference to defined security requirements. This includes designing appropriate security controls for a given type of data and incorporating threat modelling to identify and address the risks associated with the application.

A security review should also be conducted in the design stage. It serves as a checkpoint to ensure necessary security requirements are identified and incorporated in the system design.

### 6.2.3. Development Stage

Observing secure coding standards can help improving security and reducing the number of common mistakes that may result in security breaches. Performing security assessments during the development stage also helps to identify necessary security controls, and provides timely feedback to developers regarding the security of their codes. Source code security assessments should also be performed to provide an early indicator of code quality in order to deliver consistent, high-quality mobile apps.

### 6.2.4. Testing Stage

In addition to user acceptance test, system tests, stress tests, regression tests and unit tests are also useful in validating the performance and accuracy of system functionalities. Testing mobile apps could be more challenging than web apps due to the high variant of platforms and testing environment. A comprehensive testing plan should be established to design the testing approach and define the details on “what”, “when” and “how” to test.

### 6.2.5. Pre-Production Stage

A security risk assessment with security audit should be performed before the production launch and after any major changes. Each vulnerability fix may require updates to custom codes that could introduce new vulnerabilities. It is imperative to continuously assess the risk and impact to maintain secure mobile app.

### 6.2.6. Maintenance and Support Stage

New functionalities to the app or updates to existing functions may introduce changes in which security controls should be identified, documented, tested and reviewed to ensure that the system can be effectively protected from attacks or being compromised. Continuous testing is vital to maintain security assurance and protect the app where most attacks occur. The app should be regularly reviewed to ensure sufficient security is in place.

### 6.2.7. Decommission Stage

Consider decommissioning the app if it no longer meets the purposes, or when there are other apps that can better serve the business. Some suggestions on the decommission plan:

- Develop communication strategy to inform all necessary stakeholders (e.g., app users)
- Remove the app from the production environment (e.g., app store)

# 6.3. SECURITY BY DESIGN AND DATA PRIVACY

Security by design and data privacy should be embedded into the whole app system design and development processes to protect the data and individual's right to privacy. Developers should ensure that security issues are incorporated as part of the basic architectural design. Detailed designs for possible security issues should be reviewed, and mitigations for possible threats should be determined and developed. Related laws, regulations and ordinances (e.g., Personal Data (Privacy) Ordinance) should also be followed when defining the privacy requirements. Developers should pay attention to the following best practices during system design in order to protect users' privacy.

## 6.3.1. User Notification

- Inform users on what information / data that the app would collect, what purpose it serves on and how data would be handled.
- Allow users to opt-out from any personal data access/use.
- Offer users with option to delete all app-related data and account related information when he/she requests to remove the app or delete the account.

## 6.3.2. Data Handling

- Reduce the collection of personal data (especially for sensitive personal data) and permission of mobile devices features (e.g., camera and location tracking) to the absolute minimum.
- Protect users' personal data from unauthorised access, disclosure or use by using strong encryption and access control. Avoid storing personally identifiable information (PII) (e.g., credential ID, call logs) or other sensitive data on the user device.
- Do not upload or synchronise sensitive information to external systems or devices without users' permission.
- Discard sensitive data after fulfilling the claimed data usage purpose (e.g., geo-location data).

# 6.4. TESTING FOR MOBILE APP DEVELOPMENT

Testing mobile apps on mobile devices can be more challenging than testing web applications on personal computer due to wide varieties of mobile OS, hardware components and network environment, etc. The following areas should be considered in mobile app testing cycle.

## 6.4.1. Testing Mobile App Functionality

To make sure the mobile app functions properly on supported device, functional testing should be conducted to verify the mobile app features specification. There are also different types of mobile app testing that need to be considered:

- Compatibility testing: Ensure the mobile app functions properly on supported device with different mobile platform such as iOS and Android, and with different screen sizes and versions of operating systems.
- Performance testing: Measure the app performance such as response speed, acceptable user load and app stability, etc.
- System testing: Ensure the mobile app handles possible exception and recovers properly from accidental termination.

## 6.4.2. Testing Code Quality

Developers use a wide variety of programming languages and frameworks in mobile app development. Common vulnerabilities such as injection flaws, memory corruption, and cross-site scripting, may manifest in apps when failed to follow secure programming practices. For example, injection attacks against a mobile app are most likely to occur through inter-process communication (IPC) interfaces, where a malicious app attacks another app running on the device. Testing should be conducted to identify possible entry points for untrusted input or to identify known, dangerous library / application program interface (API) calls.

## 6.4.3. Cryptography in Mobile Apps

Cryptography is crucial in securing the user's data in a mobile environment, where attackers may have physical access to the user's device. Proper encryption or use appropriate key storage APIs should be adopted for storing sensitive information. Avoid using any cryptographic algorithms or protocols that contain known weaknesses. Adopt the best practices and security configurations to ensure the cryptographic algorithms are up to date and in-line with industry standards. Outdated ciphers such as DES, or hashing function such as SHA1 must not be used. Other mis-configuration issues such as insufficient key length, hard-coded cryptographic keys and weak key generation functions should be handled properly.

### 6.4.4. Mobile App Authentication

Appropriate authentication methods should be integrated and performed by both front-end client and back-end service to protect against attacks such as password dictionary attack or brute force attack. In general, username/password authentication is considered for apps that are not sensitive; two-factor authentication is generally considered for protecting sensitive app (e.g., SMS and token). Testing should be conducted to ensure the authentication procedure is consistently enforced on both front-end client and back-end server.

The following steps should be tested on authentication and authorisation:

- Identify the additional authentication factors the app uses.
- Locate all endpoints that provide critical functionality.
- Verify that the additional factors are strictly enforced on all server-side endpoints.

### 6.4.5. Testing Network Communication

Network communication between mobile device and server usually takes place over untrusted networks. It may put the mobile app at risk of network-based attacks such as packet sniffing or man-in-middle-attacks. Encrypted connection (e.g., HTTPS) should be used to ensure confidentiality and integrity of the network data while handling sensitive data. Intercept the tested app's incoming and outgoing network traffic and make sure that the traffic is encrypted, such as capture the network traffic with packet analyser and display the captured traffic in a human-readable format with network protocol analyser. After all, verify that the server is configured according to best practices.

## 6.5. POINTS TO NOTE FOR SECURING MOBILE APP DEVELOPMENT

Mobile apps are subject to similar security considerations and risks as other applications, thus general best practices for application development are also relevant to mobile app development. Due to varying use cases, usage patterns and various mobile platforms, mobile app developers should also take note of the remote web services, platform integration issues and insecurity of mobile devices. Developer should consider the following areas to build a secure mobile app:

- General Considerations
- System/Software
- Data

- Network Management

## 6.5.1. General Considerations

- Adopt security-in-mind approach and apply adequate protection for sensitive data being handled.
- Inform users on what information the app would access or upload, and for what purpose.
- Provide a personal information collection statement if personal information will be collected.
- Apply “least privilege” principle to run the app with the least amount of system privileges and access rights.
- Develop and implement the app according to best practices.
- Design and provision an app to allow updates for security patches.
- Refuse executing the app or alerting users in case jailbreaking or rooting is detected if the app would process critical/ sensitive data.
- Validate all client provided data before processing with expected whitelist of data types, data range, and data length.
- Inform users and obtain consent for any large data consuming app activities.

## 6.5.2. System/Software

### 6.5.2.1. Authentication and Session Management

- Avoid solely using device-provided identifier (like UID or MAC address) to identify the device, but rather leverage identifiers specific to the app as well as the device.
- Adopt appropriate authentication mechanism, consider two-factor authentication based on risk assessment of the mobile app, such as processing sensitive or financial transactions.
- Avoid storing passwords, wipe/clear memory locations holding passwords directly after their hashes are calculated.
- Always make use of the latest security mechanism provided by mobile platform to protect user credentials.

- Perform checking at the start of each activity/screen to see if the user is in a logged in state. If not, switch to the login state.
- Discard and clear all memory associated with the user data, and any master keys used to decrypt the data when an app's session is timed out or user logout.

### 6.5.2.2. Server Controls

- Assess backend services for mobile apps for vulnerabilities and ensure that the backend system is running with a hardened configuration with the latest security patches applied.
- Ensure sufficient logs or information are retained on the backend servers to detect and respond to incidents and perform investigation.
- Review the code of the app to avoid unintentional data transfer between the mobile app and backend servers.

### 6.5.2.3. Code Obfuscation / Reverse Engineering

- Verify the app signature on start-up to ensure that the code has not been altered or corrupted.
- Use obfuscation software to protect source code and hide the app details as far as possible if it is not compiled to machine code format to prevent reverse engineering.
- Implement anti-debugging techniques (e.g., prevent a debugger from attaching to the process) for apps containing sensitive data.

### 6.5.2.4. Use of Third-Party/Open Source Libraries

- Use reliable and/or official versions of software development tools (e.g., software development kits, software libraries) to avoid introducing Trojan Horses or backdoors unknowingly.
- Track third-party frameworks/ APIs used in the mobile app for security patches and perform upgrades.
- Validate all data when received from and send to un-trusted third-party apps (e.g., ad network) before incorporating their use in the mobile app.

## 6.5.3. Data

### 6.5.3.1. Data Storage and Protection

- Only collect and disclose data which is required for business use of the app.
- Classify data storage according to sensitivity and apply controls accordingly. Process, store and use data according to its classification.
- Application data should not be stored in external storage unless appropriate security measures (e.g., strong encryption) are applied.
- Use encryption with appropriate algorithm and key length when storing or caching sensitive data to non-volatile memory and keep minimum necessary data for the use of mobile app for the sake of data protection.
- Perform input validation and perform checking on related areas that the app can receive data to prevent client-side code injection or screen hijack.
- Discard and clear all sensitive data from memory when no longer needed.
- Adopt sandboxing technology to improve security by isolating an application to prevent other applications from interacting with the protected app.

### 6.5.3.2. On-line Payment

- Warn users and obtain consent for any cost implications for app behaviour.
- If paid-for resources are involved, security controls such as a whitelist model or re-authentication for paid-for resources should be implemented to prevent unauthorised or accidental access.
- Use secure mobile payment services if online payment is required. Use application program interfaces (APIs)/templates provided by the official providers and follow closely their guidelines for implementation.
- Inform user the minimum technical specifications that a mobile device must support for the payment service (e.g., TLS supports).
- Adhere to the specific data security standard (e.g., PCI DSS) on developing a mobile app with on-line mobile payment.

### 6.5.4. Network Management

#### 6.5.4.1. Communication Security

- Transmission of any sensitive data such as personal data or credit card information should be protected with end-to-end encryption (e.g., TLS).
- Detect if the connection is not HTTPS with every request when it is known that the connection should be HTTPS.
- When using TLS, the apps must enforce certificate validation functions and should not accept self-signed and/or un-trusted certificates.
- Enable per-app VPN to secure access internal network resources from anywhere and on any mobile devices.

## 6.6. BEST PRACTICES ON SECURE MOBILE DEVELOPMENT FOR ANDROID AND IOS

Developers may also refer to the best practices guide jointly developed by the Hong Kong Wireless Technology Industry Association (WTIA)[3] and the Mobile Security Research Lab[4] on recommendations and practical coding practices for developing secure mobile apps. The guide can be referenced at:

http://www.msr-lab.com/Secure_Mobile_Development_Best_Practices.pdf

[3] http://wtiahk.org/

[4] http://www.msr-lab.com/

A

# ANNEX A (INFORMATIVE) SAMPLE CONFIGURATIONS FOR SECURITY HARDENING

A

# ANNEX A (INFORMATIVE) SAMPLE CONFIGURATIONS FOR SECURITY HARDENING

Security configurations for mobile device hardening as reference are recommended below. The configurations may be enhanced and modified based on B/Ds' business need. Some configurations require additional security solution such as MDM or DLP solution for enforcement purpose. B/Ds may seek advice from product vendors or third party consultants for best practices on security hardening if necessary.

| CONTROLS[a] | PORTABLE COMPUTER | MOBILE PHONES AND TABLETS |
|---|---|---|
| **Password** | | |
| Require password | Yes | Yes |
| Require complex password (e.g. alphanumeric) | Yes | Yes |
| Minimum password length | 8 | 8 |
| Number of failed attempts allowed | 5 | 5 |
| Maximum password age | 90 days | 90 days |
| Password history | 8 | 8 |
| Inactive device timeout | 5 minutes | 5 minutes |
| **Other Device Setting** | | |
| Detect and restrict jail-broken, rooted or software version violations | Yes | Yes |
| Allow installing apps from trusted sources | Yes | Yes |
| Allow installing apps from unknown sources | No | No |
| Allow backup to vendor's cloud service | No | No |
| Allow keychain / key repository backup | No | No |
| Allow photo sharing | No | No |

| | | |
|---|---|---|
| Allow USB file transfer | Yes, if encrypted[b] | Yes, if encrypted[b] |
| Allow users to accept untrusted TLS certificates | No | No |
| Allow modifying account setting | No | No |
| Allow tethering configuration | No | No |
| Allow biometric to unlock device | No | No |
| Show notification messages when the screen is locked | No | No |
| Modify Bluetooth setting | No | No |
| Allow sending diagnostic and usage data to mobile vendor | No | No |
| Require encryption on device | Yes | Yes |
| Enable audit trails | Yes | Yes |
| Use auto time or synchronise with trusted time server | Yes | Yes |
| Force encrypted backups | Yes | Yes |
| Enable Remote Wipe | Not available[c] | Yes |
| Enable local wipe when maximum of failed attempt reached | Not available[c] | Yes |
| Allow mail preview | No | No |
| Allow message preview | No | No |

[a] THE CONTROL ITEMS ARE SAMPLE FOR CONTROLLING MOBILE DEVICES, INCLUDING PORTABLE COMPUTERS, MOBILE PHONES AND TABLETS. HOWEVER, THEY ARE NOT EXHAUSTIVE SUCH THAT B/DS SHOULD MODIFY A BEST-FIT REQUIREMENT LIST BASED ON BUSINESS NEEDS

[b] All data should be encrypted when stored in mobile devices or removable media.

[c] Remote wipe and local wipe may not be available for major computer OS. Therefore, B/Ds should consider the risk of lost or stolen mobile device and apply encryption as one of the compensative controls.

B

# ANNEX B (NORMATIVE) CONTAINERISATION TECHNOLOGY

B

# ANNEX B (NORMATIVE) CONTAINERISATION TECHNOLOGY

The central aspect of a mobile management strategy is creating distinct lines of separation on privately-owned mobile devices between users' personal apps and business apps and their associated data. This has come to be known as containerisation, the securing of business apps and their associated data within digital containers (either physical or virtual) that govern app behaviour and prevent unauthorised interaction with personal apps.

With the various container offerings from different vendors, there are three main types of containerisation, namely, physical container, virtual container and per-app container.

## B.1. PHYSICAL CONTAINER

Working at the chipset or kernel level of a mobile device to separate business apps and their data from a user's personal apps. Physical containers creates hardware level segmentation between a mobile user's business environment and personal environment. Implying a separate OS stack at the kernel level just for business apps to reside and operate. This OS stack is completely distinct from the mobile device's normal OS stack where the users' regular apps reside. As it is a separated domain, administrators can enforce organisation specific security requirements to that particular "Physical Container". A key security aspect of physical containers is that the OS stack typically has to leverage processor-specific capabilities.

One of the biggest benefits offered by physical containers is the top to bottom secure isolation that they offer between the separate OS stack and the device's normal OS stack, ensuring that no interaction can occur between business and personal apps. Since it is a separated platform, the vulnerability will not inherit from mobile device.

However, this stack-level isolation also creates one of the major drawbacks inherent to physical container solutions—disruption of the user experience. Whenever users are logged into the mobile devices' normal OS stack, they have to exit and enter into the separate OS stack anytime they want to use a corporate app. When they want to use a personal app, they have to reverse the process. The constant switching between physical containers not only creates user inconvenience, but also would affect user productivity over an extended period of time. Currently, this kind of solution is OS dependent; third-party and internal software developers have to customise the application to support the physical container.

## B.2. VIRTUAL CONTAINER

Business apps are segmented within an encrypted workspace inside the operating system comparable to a single sandbox with multiple apps running inside it. Policies are implemented to govern what types of interactions may occur among apps inside the virtual container. All interactions between business apps in the container stay within the container. Likewise, all of the data associated with the virtual container's apps remains secure within the confines of the virtual sandbox.

Mobile users is required to input a separated password for authenticating the container and perform business activities. With the adoption of virtual container, the logical separation between the business apps and personal apps is executed by the operating system and kernel. Since the container is run inside the mobile device, the vulnerabilities of the operating system and kernel may affect the security of container. Furthermore, the solution requires third-party and internal software developers to develop or modify their apps to support a vendor-specific container environment. Virtual container strategies also requires specific skills and additional administration effort in the on-going support activities.

## B.3. PER-APP CONTAINER

Per-app container provides a secure self-contained sandbox to each individual app and its associated data, which can provide more granular control to its administrators in securing organisational data, while presenting users a more seamless user experiences. Under this model, administrators can choose to configure general policies that apply to all apps, specific policies for individual apps, or a combination of both. Administrators can also granularly control the directional flow of data for each app, such as inbound and outbound communications. Additionally, since each contained app's data is individually encrypted and secured by policy, the business app will remain protected if a malicious app happens to infect the mobile device.

As enforcement is on per-app basis, users typically do not have to constantly enter and exit contained and non-contained environments to switch between personal apps and business apps. Users can easily see and access all the apps they are authorised to use whether they are personal or corporate apps. The combination of the per-app policy governance and application-level encryption gives B/Ds the additional level of security they need to keep their business apps and data safe.