政府资讯科技总监办公室

信息安全

流动安全

实务指南

[ISPG-SM03]

第 2.0 版

2021 年 6 月

版权公告

修改记录

修改次数	修改详情	经修改页数	版本编号	日期
1	本文件由"流动装置安全实务指南 1.0" 更名为"流动安全实务指南 1.1"。并增加关于信息技术安全管理和流动应用程序开发安全的新章节及维持与其他实务指南有一致的参考。	整份文件	1.1	2018 年 7 月
2	增加本文件以下的内容： 流动装置管理指南； 流动应用程序的数据保护； 开发安全流动应用程序的良好作业模式；以及 获授权流动应用程序的评估指南	12; 14; 20-21; 28,30,31; 附件 C	2.0	2021 年 6 月

目录

1. 简介 1
1.1 目的 1
1.2 参考标准 2
1.3 定义及惯用词 2
1.4 联络方法 2
2. 信息安全管理 3
3. 流动安全简介 5
3.1 流动科技面对的威胁 5
4. 流动装置安全管理 10
4.1 流动装置使用周期 10
4.2 流动装置管理方案 16
4.3 指定情景的安全指南 19
4.4 私人拥有的流动装置的安全指南 22
4.5 流动装置的限制及访问级别 23
5. 流动应用程序开发安全 24
5.1 开发流动应用程序的安全考虑 24
5.2 流动应用程序开发周期 25
5.3 安全设计与数据保密 28
5.4 开发流动应用程序的测试 28
5.5 开发安全流动应用程序的注意事项 30
5.6 开发 iOS 和 Android 安全流动应用程序的良好作业模式 33
附件 A: 安全强化配置模板 34
附件 B: 容器化技术 36
附件 C: 评估授权流动应用程序的指南 38

1. 简介

流动装置日渐普及，用户可随时随地存取信息，这改变了使用互联网的模式，同时亦对日常运作带来了新风险。尽管流动装置和其上安装的流动应用程序（应用程序）带来了便利并提高了效率，但保护不足之流动装置或不安全编写之流动应用程序对用户会带来风险，也可能令应用程序拥有者/开发者遭受数据泄漏或声誉受损的威胁。考虑到流动装置的高度便携性、无线连接功能所带来的额外风险，及多样化之流动应用程序的开发技术的特点，我们编写本文件，旨在为决策局 / 部门提供安全使用流动装置和开发流动应用程序的指南。

1.1 目的

本文件旨在为决策局 / 部门提供管理及使用流动装置以及安全开发流动应用程序常见的安全考虑及良好作业模式。**第 4 章**将介绍流动装置使用和管理的良好作业模式，适用于有关使用和采用流动装置及相关管理解决方案的员工。**第 5 章**将介绍流动应用程序开发安全的良好作业模式，适用于参与相关开发周期的人员。

本文件应与政府的安全要求和文件，包括《基准信息技术安全政策》[S17]，《信息技术安全指南》[G3]及其他相关程序与指南一同使用。另外，决策局 / 部门在采纳流动装置方案前，应根据业务需要，评估安全风险。决策局 / 部门应细阅本文件所介绍的安全措施及良好作业模式，为自己的流动装置方案进行合适的保护。

本文件内容属概括性质，可涵盖不同种类及作业平台之流动装置的种类及作业平台。根据政府安全文件中流动装置的定义，「流动装置」指可储存及处理资料的便携式运算及通讯装置，例子包括便携式计算机、流动电话、平板计算机、数码相机，以及数码录音或录像装置。读者应按其环境，考虑及选择适合的安全措施及良好作业模式。

1.2 参考标准

以下的参考文件为本文件在应用上的参考：

- 香港特别行政区政府《基准信息技术安全政策》[S17]
- 香港特别行政区政府《信息技术安全指南》[G3]
- 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

1.3 定义及惯用词

本文件采用《基准信息技术安全政策》和《信息技术安全指南》内所使用，以及以下的定义及惯用词。

缩写及术语	
无	无

1.4 联络方法

本文件由政府资讯科技总监办公室编制及备存。如有任何意见或建议，请寄往：

电邮： it_security@ogcio.gov.hk

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

CMMP 电邮： IT Security Team/OGCIO

2. 信息安全管理

信息安全是关于安全控制和措施的规划、实施和持续提升，以保护信息资产的机密性、完整性和可用性，适用于信息的存储、处理或传输过程及其相关信息系统中。信息安全管理是一套有关规划、组织、指导、控制的原则和应用这些原则的法则，来迅速有效地管理实体、财务、人力资源和信息资源，以及确保信息资产和信息系统的安全。

信息安全管理涉及一系列需要持续监测和控制的活动。这些活动包括但不限于以下的范畴：

- 安全管理框架与组织；
- 管治、风险管理和遵行要求；
- 安全操作；
- 安全事件和事故管理；
- 安全意识培训和能力建立；和
- 态势感知和信息共享。

安全管理框架与组织

决策局 / 部门须根据业务需要和政府安全要求，制定和实施部门信息安全政策、标准、指南和程序。

决策局 / 部门亦须界定信息安全的组织架构，并为有关各方就安全责任提供清晰的定义和适当的分配。

管治、风险管理和遵行要求

决策局 / 部门须采用风险为本的方法，以一致及有效的方式识别信息系统的安全风险、订定应对风险的缓急次序和应对有关风险。

决策局 / 部门须定期和在必要时对信息系统和生产应用系统进行安全风险评估，以识别与安全漏洞相关的风险和后果，并为建立具成本效益的安全计划和实施适当的安全保护和保障措施提供依据。

决策局 / 部门亦须定期对信息系统进行安全审计，以确保当前的安全措施符合部门信息安全政策、标准和其他合约或法律上的要求。

安全操作

为保护信息资产和信息系统，决策局 / 部门应根据业务需要实施全面的安全措施，涵盖业务上不同的技术领域，并在日常操作中采取「预防、侦测、应急和复原」原则。

- 预防措施避免或阻止不良事件的发生；
- 侦测措施识别不良事件的发生；
- 应急措施是指在发生不良事件或事故时，采取协调行动来遏制损害；和
- 复原措施是将信息系统的机密性、完整性和可用性恢复到预期状态。

安全事件和事故管理

在现实环境中，由于存在不可预见并致服务中断的事件，故此安全事故仍可能会发生。若安全事件危及业务的连续性或引起数据安全风险，决策局 / 部门须启动其常规安全事故管理计划，以实时识别、管理、记录和分析安全威胁、攻击或事故。决策局 / 部门亦应准备与有关各方适当地沟通，透过分享对有关安全风险的应急以消除不信任或不必要的猜测。当制定安全事故管理计划时，决策局 / 部门应规划和准备适当的资源，并制定相关程序，以配合必要的跟进调查。

安全意识培训和能力建立

因为信息安全每个人都有责任，所以决策局 / 部门应不断提升机构内的信息安全意识，透过培训及教育，确保有关各方了解安全风险，遵守安全规定和要求，并采取信息安全的良好作业模式。

态势感知和信息共享

因应网络威胁形势不断变化，决策局 / 部门亦应不断关注由安全行业和政府电脑保安事故协调中心发布的现时安全漏洞讯息、威胁警报和重要通知。应将即将或已经发生具威胁的安全警报传达及分享给决策局 / 部门内的负责同事，以便采取及时的应对措施来缓解风险。

决策局 / 部门可以利用网络风险信息共享平台接收和分享安全事务、安全漏洞和网络威胁情报的讯息。

3. 流动安全简介

今时今日，流动装置为用家带来极大的方便，亦对业务运作十分重要，但亦带来安全问题，例如流动应用程序增加数据遗失的风险。本节集中介绍应对常见的安全问题的安全措施及良好作业模式。决策局 / 部门宜根据本身的业务需要及环境考虑安全措施及良好作业模式。

3.1 流动科技面对的威胁

流动装置的主要威胁来自装置本身、网络连接（例如流动通讯网络和互联网）及流动应用程序。与办公室的工作站相比，流动装置通常在室外或路上使用，在这些地方它们更容易遭受威胁和遗失。以下是一些流动技术的相关安全风险：

流动装置

- 使用缺少实体安全控制的装置

  流动装置往往是体积细小，一般用于办公室控制范围以外的各种地方，例如员工家中、咖啡店、酒店及会议场地等，其流动性令装置比其他装置更容易遗失或被盗，令数据外泄的风险增加。

- 使用安全控制不足的流动装置配件

  流动装置通常都备有相机及麦克风。不恰当的录像、拍照及摄影可导致安全问题。另外，若流动装置未有得到适当的保护，未获授权人士便有可能获取装置内的敏感录像、录音或照片。

- 使用不可靠的流动装置

  很多流动装置，尤其是私人拥有的装置，未必可靠。使用已越狱或根权限被破解的流动装置，会导致更多的安全风险，原因是内建的安全限制已被绕过。

- 缺乏对敏感数据的保护

  流动装置用于储存敏感数据，包括个人资料、照片和联络人名单。载有敏感数据的文件亦有可能下载和储存在决策局 / 部门批准和管理的流动装置中。为了防止由于网络攻击或流动应用程序过度收集数据而导致数据泄露，这些敏感数据需要使用流动装置内置功能或获授权的安全工具进行加密保护。

- 不安全的屏幕上锁配置

  锁定屏幕是第一道防线，以防止未经授权访问流动装置及其中所储存的数据。正确的锁定屏幕配置（例如严谨密码）可以保护装置免

遭未经授权访问和数据泄露。此外，某些流动应用程序可能仍会在锁定的屏幕上显示推送通知，例如讯息、由应用程序发出的通知和新收到的电子邮件。如果通知的内容包含敏感数据，这些敏感数据有可能被一些未经授权的人士看到。

- 使用公共的流动电话充电设施

  一些购物中心和公共交通工具都有提供公共流动电话充电设施。如果公共的流动电话充电站（尤其是带有 USB 充电接口）被入侵，则恶意软件将通过该充电站安装到装置上，从而窃取装置内的敏感数据。故此，应尽量避免使用可疑的流动电话充电设施。

网络

- 使用不可信的网络

  流动装置基本上是使用非机构自设的网络访问互联网，如外部 Wi-Fi 及流动电话网络。这些网络容易被窃听，令敏感数据有机会外泄。

- 使用不安全的通讯技术

  与主要依靠局部区域网络或办公室无线网络的办公室内工作台相比，流动装置能够广泛利用各种通讯技术，例如蓝牙和近距离无线通信作数据连接。每种通讯技术都有其安全风险。若敏感数据于通讯媒介中遭拦截，则会导致安全事故。

应用程序

- 使用获授权的应用程序

  为了保障流动装置安全，流动装置上的应用程序应只供业务之用。供个人使用的流动应用程序，例如游戏、在线支付、在线购物等，除非有充分的理由，否则应尽量避免安装在决策局 / 部门所提供的流动装置上。

- 不可信的流动应用程序的风险

  流动装置的设计令用户能从流动应用程序商店中轻易找寻、获取、安装及使用第三方的应用程序。但这却带来明显的安全风险，尤其在不设安全限制或其他制约的流动装置平台及流动应用程序商店所发布的由第三方开发的应用程序。

- 显示流动装置位置的风险

  定位服务是社交媒体、导航及其他流动为主的应用程序普遍会使用，为装置和其用户确定位置的服务。已启用定位服务的流动装置会较有机会成为被攻击的目标，因为这会令潜在攻击者更易知道用户及流动装置的位置，然后将位置数据结合其他来源的信息，从而发动如鱼叉式仿冒诈骗的攻击。

- 不受控制访问流动装置传感器 / 配件的风险

  流动应用程序可能导致智能电话和平板计算机内置相机等桌面计算机不常见的传感器 / 配件，在不受控制的情况下被访问。这样有可能构成针对性攻击的风险，例如一些在公共场所展示的恶意二维条形码或 QR 码。

- 地理标记的风险

  流动装置通常有地理标记功能，能自动将地理信息（即位置和 GPS）标记到装置所拍摄的照片和其他媒体上。因为照片拥有人的姓名和所拍摄照片的地理位置，会在无意间被不知名人士和潜在攻击者收集，增加了个人私隐泄露的风险。

- 泄漏个人资料的风险

  流动装置的联络人名单和通讯簿被广泛用于储存个人资料，例如姓名、电话号码、地址、出生日期、电邮等。一些流动应用程序可能要求访问联络人名单或通讯簿的权限以支持该程序的操作。如果敏感数据（例如个人标识号(PIN)、帐户名称、账号或密码）储存在联络人名单或通讯簿中，便可能构成经流动应用程序泄露这些敏感数据的高风险。

开发流动应用程序

与使用流动应用程序相比，开发流动应用程序时需要处理额外的安全风险。开发人员可参考开放网络应用程序安全计划（OWASP）十大流动应用程序开发风险(Mobile Top 10)，以了解流动应用程序开发面临的主要风险。决策局 / 部门应参考这些常见的安全风险，并避免在编写程序时出现这些问题。决策局 / 部门亦应检讨及界定其应用程序的安全要求，以减低风险，避免设计上的安全漏洞。OWASP 提到的有关流动应用程序风险归纳如下：

- 不当使用平台

  这个潜在威胁源于程序误用平台功能和没有采用平台所提供的安全控制措施（例如 Android 意图、平台权限、不当使用生物识别功能或有关流动操作系统的其他安全控制措施）。不当使用平台功能可能令系统蒙受风险（如跨网址程序编程）。

- 使用不安全的数据储存

  当软件开发者假设用户或恶意软件不能访问流动装置的文件系统及装置的敏感数据时，数据储存漏洞便可能会出现。通过流动恶意软件、经修改的应用程序或取证工具，可能会导致数据遗失或程序中的敏感数据遭提取。

- 使用不安全的通讯

  不安全的通讯会构成应用程序所传输的数据暴露风险，可能导致敏感数据外泄。有关问题的成因可能是不良的交握式通讯、不正确的保密插口层（SSL）版本、使用不合格的交涉协议及以纯文本格式传输敏感数据资产。

- 使用不安全的认证

  攻击者可能会破解密码、密码匙或认证令牌，以假冒其他用户的身分。有关问题的成因可能是欠缺或没有妥善推行账户认证机制，以及不当的对话管理。

- 使用不安全的授权

  一些流动应用程序会在用户认证后自动给与一些权限。这些授权有时会被错误地过度扩展，提供流动应用程序不应该有的权限。如果攻击者得到应用程序的特别权限，便可能导致未获授权而访问敏感数据的情况。

- 使用不足的加密

  如果数据未加密或不当使用加密功能进行加密，攻击者会盗取或访问保护欠佳的数据。

- 客户端程序代码层次的错误

  程序代码层次的错误可能产生漏洞（如缓冲区满溢和内存外泄），让攻击者可对流动应用程序作出恶意输入。这可能会引致执行外部程序代码或远程服务器拒绝服务（DoS）。

- 使用被窜改的程序代码

  攻击者可能会以存放于第三方位置的恶意应用程序窜改该流动应用程序。攻击者亦可能通过仿冒诈骗攻击诱骗用户安装应用程序。

- 不足以防范程序代码还原工程

  攻击者可能会分析核心二进制程序代码，找出其源码、源码库、算法和其他资产，从而利用漏洞、收集敏感数据或盗取知识产权。

- 不当处理外部功能

  在开发阶段，开发者可能会建立一些隐藏的后门程序或功能，以便为应用程序除错。如后门程序在推出的版本仍然存在，攻击者便可利用这些后门程序作出恶意行为。

4. 流动装置安全管理

本章介绍如何在流动装置使用周期内保护装置，以及流动装置管理解决方案的常见安全功能。本章适合于使用和采用流动装置及相关管理解决方案的用户和管理员。

4.1 流动装置使用周期

与其他信息系统相似，流动装置在整个使用周期中包括三个主要阶段 – 提供、使用和停止使用。以下小节将讨论如何在周期的各个阶段保护流动装置的一些良好作业模式。

4.1.1 流动装置的提供

当决策局 / 部门考虑于业务中采用流动装置时，应了解自己对流动装置的需要，以及知道流动装置方案如何支持本身的业务。应订立流动装置安全政策，当中列明使用流动装置的业务及安全要求，并订定适当的流程和程序以提供流动装置。以下是一些考虑事项：

- 审批流动装置的机制及获批准的流动装置的种类。
- 每种流动装置上所容许的数据保密级别。敏感数据不可储存于私人拥有的流动装置内。
- 确保基于数据保密级别的控制机制符合政府的安全要求。
- 根据操作需要，界定和备存授权软件列表，包括免费软件、开源软件和链接库。
- 在职员转职或离职时，确保相关程序能确保适时清除储存在流动装置上的敏感数据。

决策局 / 部门应覆检及按所需调整修改流程，使供应阶段能具有以下良好作业模式：

- 制订符合运作及安全要求的型号清单。
- 在提供新型号的流动装置前进行风险评估，并推行持续风险监察机制，以评估流动装置所涉及的风险转变或新风险。
- 按可行性安装安全控制工具，例如流动装置管理[1]、数据遗失防护、个人防火墙软件及抗恶意软件。应于决策局 / 部门的强化程序中列出所使用的工具。

[1] 流动装置管理是一个（或一系列）应用系统，为流动装置如电话及平板计算机提供政策、库存、安全及服务等方面的管理功能。就流动装置管理详情，请参阅本文件第 4.2 节－流动装置管理方案。

- 在决策局 / 部门所拥有的流动装置中只使用获审批的应用程序。获得决策局 / 部门委任人士授权后，用户才可安装第三方应用程序。
- 为流动装置进行安全强化处理，将已强化的装置交付用户。
- 向用户发放使用政策，并获得用户收到有关使用政策以及状态良好的流动装置的确认。该确认可以是已签署的协议或电邮回复。
- 定期向用户发放安全提示，以提醒他们采用安全良好作业模式。
- 启用开机密码功能。
- 根据决策局 / 部门的部门安全要求，执行最起码密码长度及复杂性的要求。
- 设定流动装置在闲置一段时间后自动锁上。
- 启动当多次连续输入错误密码后，数据自动删除的功能（若有此功能）。决策局 / 部门应按其运作的需要，订立连续错误尝试的实际次数。亦应启动遥距清除功能，当装置遗失或被盗时仍能保护数据。此外，应仔细选择清除方案，以确保删除的敏感数据不能被恢复。
- 在可行的情况下，为流动装置的所有储存器启动加密功能，可于装置层面、全磁盘层面，或档案层面启动加密功能。
- 考虑使用多重认证机制，例如在使用虚拟专用网络之同时使用数码证书及密码。
- 备存资产追踪信息，例如序号、检查装置上的应用程序及监察有关数据作审计之用。
- 流动应用程序权限。为了最大程度地减少安装流动应用程序后受到损害的风险，流动装置的用户应采用「最小权限」原则，以最少系统权限和访问权限执行应用程序，从而使攻击者无法访问其他应用程序（例如浏览器、联络人名单）或流动装置的功能。
- 在安装流动应用程序时，用户应先阅读数据披露、私隐政策声明或同等资料的内容，并充分了解权限的安全风险，然后才按“我同意”或“允许”。通常应用程序要求的某些权限（例如联络人、麦克风和位置讯息）未必是核心功能所需要的，可以通过流动装置上的应用程序权限关闭。

决策局 / 部门应根据政府安全要求及流动装置安全政策，制定流动装置安全强化程序，以执行安全配置。所有流动装置在交予用户前，均应依照安全强化程序加以强化。有关安全强化配置的模板，请参阅附件 A。

4.1.2 流动装置的使用

即使在供应阶段推行安全控制，人和程序仍然是保持流动装置安全的两大重要因素。因此，本节重点介绍流动装置在持续的管理及使用中的良好作业模式。

4.1.2.1 管理员

管理员应跟从以下良好作业模式：

- 留意安全消息，例如安全警报或应用程序的新版本，以检查流动装置操作系统和流动应用程序的可用更新和 / 或安全修补程序；并及时采取适当的变更管理，例如将流动应用程序更新为最新版本。
- 如果流动应用程序已终止支持或不再使用，用户应立即卸除该应用程序，以防止因该应用程序的安全漏洞而受到攻击。
- 于流动装置上安装已经验证的更新及 / 或修复程序。
- 定期检查流动装置以确认安全措施被执行。应检测及限制使用已越狱、根权限遭破解及被入侵的装置。
- 在可行的情况下，启动流动装置中的加密功能。
- 备存决策局 / 部门的流动装置库存记录，记录要包括装置用户数据及已安装的应用程序的列表。有关清单应由决策局 / 部门指定人员保存。

  关于软件特许使用权，决策局 / 部门必须负责定期保存、更新和管理所有软件和流动应用程序特许使用证的记录，并确保为所有已购买、正在使用和已弃置的软件和流动应用程序保存最新的记录，与现存特许证相符。至于软件的机构特许使用权，必须确保已安装的软件数量不超过所购买的软件数量。

- 决策局 / 部门应定期检查软件和流动应用链接库存，以确保所有软件均有特许使用权，以及没有使用未获授权的软件或流动应用程序。

4.1.2.2 流动装置用户

用户应遵从使用政策及安全提示，包括但不限于以下：

不要事项：

- 除已获批准，否则不要修改流动装置的设定。
- 不要尝试使用未经授权的工具为流动装置越狱 / 破解根权限或损害流动装置操作系统，否则可能会带来不能预计的保安风险及令保养服务失效。
- 不要容许不明或不可信的来源经无线连接到装置。
- 不要开启或访问来自具误导性、可疑或不可信来源的社交媒体、实时通讯讯息、短讯服务、多媒体讯息服务或电邮内的连结。

- 不要从不明或不可信的来源下载程序和内容，以及安装流动应用程序。
- 不要在流动装置上安装非法或未获授权的软件。
- 当流动装置连接政府内部网络时，不要直接接驳(如：经流动电话网络)至外部数据网络。
- 不要使用公共打印机。
- 不准使用任何流动应用程序将数据从流动装置上自动上载或同步至其他未获授权的装置，例子包括公共云端储存服务供货商，以及使用云端技术的流动供货商所提供的备份方案和分享相片的社交媒体。
- 不要在流动装置上储存其他系统（例如电邮、提款卡及网络登入等）的密码，亦应停用自动储存密码功能。
- 不要广泛地利用决策局 / 部门所提供的流动装置作私人用途。

须要事项：

- 跟从决策局 / 部门所订立的安全程序。
- 只下载和安装决策局 / 部门批准及提供的应用程序。
- 下载 / 安装之前，阅读流动应用程序的私隐政策以及条款和条件。
- 确保操作系统及已安装应用程序的安全功能已按强化程序中的要求开启。
- 安装最新的病毒及恶意软件的标识符及定义（当有提供时）。
- 对流动装置的安全漏洞保持警觉，及根据受影响的系统及版本，按指示安装相关的修补程序。
- 将已加密的完整数据定期备份至获授权的计算机或储存器。若装置存有敏感数据，则必须跟据现行的政府安全要求保护备份资料。
- 关掉非使用中的无线通信，例如 Wi-Fi、近距离无线通信、蓝牙及 / 或红外线连接。
- 启用网络连接通知功能，以便在加入网络之前获得用户的确认。
- 停用自动连接 Wi-Fi 或自动加入的选项，避免自动连接到不可信 / 假冒的网络。
- 若无须使用具定位功能的应用程序，关掉流动装置的定位服务。
- 在连接至公共 Wi-Fi 热点时，要加倍小心，而且在没有合适保护下，不要访问政府资料。
- 须建立虚拟专用网络联机到所属决策局 / 部门的政府内部网络。这样可确保所有传送的数据都会受到相应的安全控制。
- 妥善保管所持有的流动装置。在没有采取妥善安全措施的情况下，装置须避免处于无人看管的状态。
- 启用超时功能，可在无人看管时锁定装置。当处理敏感数据时须留意周遭环境，以减少被偷听及偷窥的机会。

4.1.2.3 流动应用程序的数据保护

使用流动应用程序时，未授权的访问、数据泄露和异常的数据使用会带来个人私隐的问题。为了尽量减少这方面的问题，流动应用程序功能的访问，操作或授权应基于「最小权限」和「有需要知道」原则，仅授予必要的权限。此外，用户或管理员应定期检查装置上的私隐设置，并在流动应用程序「选择拒绝」不需要的数据收集。

- **资料收集**。通常应明确说明数据收集的目的，以及透过该程序所收集、使用或处理的数据。为了保护私隐，用户应避免通过流动应用程序（例如注册流动应用程序帐户）提供过多的个人资料（例如身份证号码、家居地址、信用卡号码和签名等）。

- **数据使用**。如果未按照私隐政策声明或流动应用程序的条款和条件（例如与其他应用程序或机构共享）中订明的正确方式使用收集得到的数据，则个人资料会造成数据泄漏的风险。除非用户事先同意，否则个人资料仅应用于原本数据收集目的或直接相关目的。

- **数据保留**。当用户卸除流动应用程序时，流动应用程序通常会删除所收集的数据。为了防止收集到的个人资料传输到其他应用程序或机构，与应用程序相关的所有个人资料的保留时间均不超过达致原来目的实际所需时间。

- **数据传输**。应将所有与流动应用程序相关的个人资料储存在流动装置或指定的储存服务器中，并由流动应用程序开发者加密。除非事先获得用户同意，否则流动应用程序数据（尤其是个人资料和其他与流动应用程序相关的数据）不得外判、转移、上传或储存在其他后端服务器、公共云端储存和其他平台 / 地点以及第三方机构。

4.1.3 流动装置的停止使用

于流动装置管理最后一个阶段，装置可能因为实体受损、停止支持、再分配给其他人员或决策局 / 部门等，而需要停止使用。决策局 / 部门应订立装置停用程序，包括安全删除数据、重设流动装置至出厂设定，以及弃置，令装置能在没有泄泄露数据的情况下重用或弃置。流动装置用户及管理员应遵照程序，以妥善保护政府数据和减低数据外泄到未授权人士的机会。

管理员

管理员应跟从以下的良好作业模式：

- 检查收回装置的状况。
- 检查流动装置是否曾经处理及／或储存敏感数据。如有怀疑，则当流动装置曾经处理及／或储存敏感数据来处理。
- 于弃置、重用或维修流动装置前，须完全删除或销毁政府数据。若装置存有敏感数据，管理员须依照政府安全的要求来处理敏感数据。如装置实体受损，用户应通知管理员储存在受损流动装置中数据的保密级别。
- 设回原厂设定（如有）

流动装置用户

用户应跟从以下的良好作业模式：

- 为决策局／部门进行所需的数据备份。
- 由于管理员未必有权访问装置内的数据，所以在归还流动装置前，要完全清除或销毁装置内的数据。有关删除数据的详情，请参阅《信息技术安全指南》及《销毁及弃置储存媒体实务指南》内的相关章节。
- 尽早归还流动装置。
- 建议用户从官方网站、流动应用程序商店（例如 Apple 的 App Store、Google Play 或 Microsoft Store）或其他已获得批准的可信任来源下载软件和流动应用程序前，先仔细阅读私隐政策和条款及条件。

4.1.4 安全意识培训

用户培训是加强用户安全意识的重要一环。政府人员应从流动装置用户角度理解安全要求，从而将人为错误减至最低。应为流动装置用户提供培训，让他们对关乎流动装置的安全威胁、安全要求及安全政策有一定程度的认识。

一般而言，流动装置用户的意识培训应包括：

- 流动装置内敏感数据的保密级别，以及相应的安全要求。
- 流动装置使用及停用阶段的安全要求。
- 遗失或被盗流动装置的通报机制。
- 流动装置安全的最新消息及趋势。

4.2 流动装置管理方案

流动装置管理方案有助于远程管理使用不同流动平台的流动装置。 决策局 / 部门应考虑采用流动装置管理方案，以简化支持流动装置的工作，并使流动装置有更好的安全控制。

应注意由于流动装置管理方案软件主要是为流动电话和平板计算机平台而设计的，因此有关方案大多数无法用于管理安装了桌上计算机平台的便携式计算机。决策局 / 部门应查看方案的最新功能。

4.2.1 流动装置管理方案的功能

流动管理方案对流动装置（如流动电话及平板计算机）的政策、库存、安全及服务各方面提供管理功能。以下列出的一些技术功能只供参考，不应视为强制性要求。选择流动管理方案时，决策局 / 部门应按其自身的业务和营运环境，考虑实施安全控制的需求。

- 按所制定的配置设定，来部署及配置流动装置。
- 远程访问流动装置并推送最新的修补程序[2]和配置，以增强装置的安全控制。
- 流动应用程序的管理，例如安装及移除。
- 为数据访问提供详细的审计追踪。
- 执行安全控制，如在使用无线网络传送数据时使用虚拟专用网络为数据加密。
- 监察异常活动。
- 重复登入失败后清除装置内的数据。
- 当流动装置遗失或被盗时，遥距清除装置内的数据。
- 容器化 — 通过实体、虚拟、或应用程序容器，提供一个隔离的环境处理数据（请参阅**附件 B**）。

[2] 用于流动装置平台的修补程序通常由平台供货商提供。如果流动装置制造商已特设平台，则可能无法应用由流动装置平台供货商提供的修补程序，因此可能无法及时修复漏洞。

4.2.2 流动装置管理方案的良好作业模式

以下列举一些以流动装置管理方案作流动装置安全管理的常见良好作业模式。

- 严格执行安全政策

  根据部门信息技术安全政策及其他相关政策、程序及指南执行技术性措施，透过流动装置管理方案，可以统一地设定于决策局 / 部门所提供的流动装置上。应记录及定期覆检已制定的流动装置管理安全政策。

- 用户及装置验证

  当访问内部资源时，应透过以网络为基础的装置验证、密码验证、以令牌为基础的验证等不同的方法来验证用户及装置。当装置闲置一段预定的时间后，应自动上锁。应开启遥距上锁功能，以便在装置相信已遗失、被盗或置于不安全的地点时，管理员可以为装置遥距上锁。

- 安全的数据通讯及储存

  应以严谨的加密方法，例如虚拟专用网络技术，来保护受管理流动装置与决策局 / 部门终端服务间的数据通讯，亦应使用严谨的加密方法保护装置内建记忆储存器及抽取式储存媒体内的数据。容器内的数据也应该加密。不允许在流动装置管理领域之外作复制 / 贴上和剪下 / 贴上。应启动遥距清除功能，以应对流动装置遭遗失或被盗。装置应在多次验证失败后自动清除装置内之数据。

- 流动应用程序管理权限

  用户应注意流动应用程序所要求的权限。当用户下载或安装流动应用程序时，程序可能会要求用户授予权限，访问流动装置上的数据，例如访问联络人，收集到过的地点或到过的网站。一些权限对于应用程序的操作不是绝对必要的。另外，在默认模式下，一些流动应用程序可能会要求授予所有功能（例如相机、联络人、位置、麦克风、储存和电话）的所有权限。此类要求可能会带来个人资料私隐问题。

  以下列出了与应用程序权限相关的一些做法：

  - 限制分配给每个应用程序访问资源（例如摄像机、麦克风、位置）的权限，以保障私隐。

- 限制应用程序的同步和共享服务（例如本地装置同步、远程同步服务和网站）。
- 如无需要，停用流动应用程序的同步服务。
- 当装置层面的加密遭受破坏或未启用时，启用应用层面的加密以防止未经授权的访问。
- 验证应用程序上的数字签名，以确保在装置上只安装来自可信任来源的应用程序以及程序源码并未修改。

- 分发和管理流动应用程序

  - 在流动装置上启动遥距清除未经授权或可疑的流动应用程序。
  - 将流动应用程序行入白名单，以确保用户只使用机构批准的应用程序（包括内部开发或捆绑在流动装置的流动应用程序）。

- 数据驻留

  - 流动装置管理方案可以是以云端平台或机构处所为基础的。一些数据（例如，流动装置信息、位置）将被收集并驻留在流动装置管理方案。如果数据被认为是敏感的，则应首选机构处所的方案以保护数据。

4.3 指定情景的安全指南

本节集中为政府人员使用流动装置的不同情景提供安全指南，包括安装流动安全软件、流动安全风险评估、处理敏感数据、决策局 / 部门内部共享流动装置、流动装置遗失、被盗或发生其他涉及流动装置的安全事故。与第 4.1 节的良好作业模式不同，这些情景可能在日常运作中经常发生，也会对流动装置安全带来明显影响，例如不当处理敏感数据、由于共享装置而导致数据泄露给其他部门，或因装置遗失、被盗及因程序漏洞而导致流动装置被攻击而导致数据外泄。

4.3.1 流动安全软件功能

流动安全软件（例如防毒软件）可在流动装置上进行安全扫描，以防范有害病毒和恶意活动，并保护流动装置上的个人资料。软件可在流动应用程序安装之前先加以扫描，还可以阻止已安装的流动应用程序访问其他应用程序。

流动安全软件的功能包括但不限于：

- 防盗 / 遥距锁定（装置或流动应用程序）
- 阻止滥发短讯 / 来电
- 权限管理器（跟踪和管理流动应用程序权限，以保护流动应用程序和装置）
- 私隐顾问（审查安装在流动装置上的应用程序，并确保不会泄露敏感数据）
- Wi-Fi 安全检查
- 实时扫描
- 防病毒保护
- 恶意软件检测
- 反网络钓鱼防护
- 安全的浏览模式（例如网络过滤功能，阻止用户浏览具恶意或钓鱼软件的网站或提醒用户此事）
- 私隐清理器（稳妥地清除浏览记录）

4.3.2 流动安全风险评估

流动安全风险评估旨在帮助用户在更新白名单及安装授权软件和流动应用程序之前，自我评估流动安全。这可以帮助决策局 / 部门在安装授权软件和流动应用程序之前评估流动装置的安全风险。

建议各决策局 / 部门制备一份安全检查列表供用户参考。各决策局 / 部门应根据业务操作及安全考虑因素，清楚地拟定他们的清单。清单应包括但不限于以下内容：

- 授权用户（例如所有员工、指定的小组 / 员工或管理员）。
- 流动应用程序所需的权限（例如遵从「最小权限」原则，没有错误配置的权限）。
- 访问、收集和使用流动数据。
- 流动应用程序身份认证（例如双重认证）。
- 流动应用程序的安全（例如数据加密、已知安全漏洞）。
- 数据保护的安全（例如在传输过程中进行加密、不上传也不传输来自流动装置的数据）。
- 流动应用程序的数据储存（即与流动应用程序相关的数据仅储存在流动装置或指定的数据中心）。
- 可供下载的流动应用程序来源（例如官方网站、供货商的应用程序商店）
- 安全的网络连接（例如流动装置停用自动加入连接功能）。
- 通过流动应用程序安全漏洞测试工具检测（即检测不到流动应用程序有安全漏洞或恶意行为，因此通过了测试）

4.3.3 处理流动装置内的敏感数据

为遵守政府的安全要求，决策局 / 部门须加倍留意政府的安全规定及文件。此外，决策局 / 部门应采纳以下安全作业模式，以保护流动装置及数据，抵御常见的安全威胁：

- 不要在流动装置上处理绝对及最高机密数据。
- 不要在私人拥有的流动装置上处理机密或限阅数据。
- 在流动装置上储存或传送敏感数据时加密数据。
- 尽量避免于流动装置上储存敏感数据。
- 除非数据得到适当安全措施的保护，否则不要在流动装置上储存敏感数据。

- 不要将流动装置内的敏感数据与公共云端储存服务、私人拥有的信息技术设备或其他未获授权的装置同步。
- 停止使用流动装置时，将装置内的敏感数据彻底删除或销毁，并在丢弃或重用装置前妥善保护管理储存装置。
- 不要在私人拥有的流动装置上储存敏感数据。
- 若未能看管存储有敏感数据的流动装置，就要将装置放于一个安全的地方。
- 使用屏幕防窥片减少屏幕可视角度。在使用流动装置时小心调校屏幕位置，避免其他未经授权人士偷窥屏幕上的敏感数据。
- 在可行的情况下，在使用流动装置及访问敏感数据配置时，设置多重密码控制。
- 不要撷取有显示敏感数据的屏幕。
- 不得将敏感数据传送到公共信息技术服务设备及供货商备份服务设备上。
- 提醒政府流动装置用户在遗失流动装置、装置被盗或装置有损坏时，要立即通知管理员或负责人员。流动装置用户要负起安全责任，在任何时间应保护装置免于被盗、失窃及损坏。

4.3.4 共享流动装置

应禁止共享政府流动装置，除非所涉及的人员均获授权访问装置内的所有数据。应按照运作需要来决定共同访问的授权，例子包括部门流动装置访问小组内的数据、流动应用程序开发的测试装置，及外出或轮班工作如数据中心操作等。若需要共同访问，决策局 / 部门应确保所有涉及敏感数据的活动都被审计追踪及被逻辑访问控制软件所追踪。

若政府人员因操作需要而共享流动装置，有关人员应遵守以下良好作业模式：

- 根据「有需要知道」原则来储存数据。
- 未经授权不可进行任何备份。
- 在使用完毕或转交其他人员时注销所有应用程序。
- 不要配置或储存个人电邮帐户及密码。

4.3.5 遗失、失窃及安全事故

流动装置因体积小而容易遗失或被盗。决策局 / 部门应检讨及修改其安全事故处理程序，为处理装置遗失或失窃事故作出必要的调整。当发生安全事故，装置用户应根据安全事故处理程序立即报告及升级处理。

决策局 / 部门应考虑以下良好作业模式处理遗失或被盗的流动装置：

- 撤销可能被破解的账户。
- 在技术上可行的情况下，遥距清除遗失或失窃装置内的数据。
- 制定、测试及定期覆检有关遗失或处理失窃流动装置的程序。
- 如涉及敏感数据时向政府信息安全事故应急办事处汇报事故。

4.4 私人拥有的流动装置的安全指南

在机构内使用私人拥有的流动装置，其中一个基本的安全问题是拥有权的界定。由于私人拥有的流动装置只由持有装置的员工控制，员工可以随意安装任何流动应用程序，这样可能将恶意软件带进装置内。另外，人员可能借着修改流动装置的启动软件及 / 或固件，覆盖供货商的安全控制以得到更多控制权限及使用上的弹性。这些装置如在没有适当保护措施的情况下连接政府内部网络，可能成为安全漏洞，包括外泄保密数据，以及在政府内部网络传播恶意软件，或者成为被恶意软件控制的攻击装置。就以上安全风险，加上遗失装置所导致数据外泄的风险，在欠缺适当保护下，应禁止于业务上使用私人拥有的流动装置。

决策局 / 部门在考虑采用流动装置方案而涉及私人拥有流动装置时，应遵照政府安全要求内有关使用私人拥有信息技术设备的条文。另外，《基准信息技术安全政策》[S17] 第 20.1.3 节要求，没有列入任何保密类别的数据也应保护，以防止不慎外泄。

就处理非保密资料，在使用私人拥有流动装置时，流动装置管理及流动数据遗失防护是可行的技术方案，以保护流动装置内的数据免受非授权访问。流动装置管理着重于管理装置以及流动应用程序，而流动数据遗失防护则着重于数据控制。决策局 / 部门宜参照《数据遗失防护实务指南》，就不同情景加入额外考虑以保护流动装置内的数据。本文第 4.2.1 节已列出一般流动装置管理方案的安全服务。

4.5 流动装置的限制及访问级别

决策局 / 部门应在流动装置安全政策中就流动装置科技的使用订明业务及安全要求，例如决策局 / 部门宜限制流动装置的种类（如根据操作系统版本、流动电话品牌 / 型号等），并要求多层访问级别，如容许政府流动装置访问较多资源，而让运行于决策局 / 部门流动装置管理客户软件的私人拥有流动装置则访问有限的资源。

决策局 / 部门应按风险决定那种类型的流动装置可以授予那种访问级别。在设定流动装置安全政策时，决策局 / 部门应考虑以下几项因素：

- 对政府安全要求的遵行

  除非已根据政府安全要求执行适当的保护，否则不容许业务上使用私人拥有的流动装置。

- 工作的敏感程度

  部分工作需要访问敏感数据或资源，有些则不然。决策局 / 部门宜按业务需要为工作设立限制性要求。

- 技术上的限制

  部分情况可能需要指定流动装置类型或操作系统，例如一些建基于硬件的安全功能又或一些执行某些特定的流动装置管理客户软件的情况。

- 工作地点

  装置用于决策局 / 部门直接管辖的环境内，风险比用于其他不同的地点为低。

5. 流动应用程序开发安全

本节适用于参与开发流动应用程序周期的开发人员。对于需要使用和采用流动装置和相关管理解决方案的用户和管理员，请参阅第 4 章 -流动装置安全管理。

5.1 开发流动应用程序的安全考虑

由于现今流动应用程序会用作访问敏感数据和进行重要商业活动，因此亦可能受到不同的威胁。作为良好作业模式，为开发和维护安全的流动应用程序，在开发流动应用程序的不同阶段须作出各项安全考虑和采取安全措施（包括技术与管理层面）。

软件开发的方法正不断演变，敏捷软件开发或 DevOps / DevSecOps（结合「开发」、「安全」与「操作」）等利用反复式开发程序达致持续整合和持续交付的目的，以更快速及 / 或更安全地建立流动应用程序。这个方法着重持续的沟通、整合、测量和交付，以促进程序开发、测试及质素保证之间各个程序。无论使用何种方法，都应将安全的流动应用程序的设计嵌入到开发周期的每个阶段，尤其是早期阶段，以尽量减少安全风险并避免因设计缺陷而导致的重复工作。

为方便找出在流动应用程序开发过程中的潜在安全风险，以下会探讨发展周期的一般阶段和主要安全考虑：

发展周期	**安全考虑**
要求	在本阶段应连同功能要求一并订定安全要求，并在软件开发其他阶段进一步加入安全因素。
设计	根据要求阶段所定的规格设计应用程序架构。
开发	遵从安全编码良好作业模式开发流动应用程序和进行源码安全评估。
测试	确认系统功能的效能和准确性。
推出前	进行安全风险评估和安全审计。
维护与支持	通过不断的测试和适当的安全控制措施维持安全保证。
停止使用	在程序不再符合目标时，停止使用程序。

5.2 流动应用程序开发周期

5.2.1 要求阶段

在要求阶段应考虑安全因素，以致安全概念可纳入整个开发周期。应连同功能要求一并订定安全要求，并在软件开发其他阶段进一步加入安全因素。如能妥善订定安全要求，便可于早期阶段解决已确定的风险，大大减少后期阶段的额外工作和补救工作。在订定安全要求时应考虑以下各个方面：

- 架构、设计和威胁模型要求

  应制定程序，确保在规划流动应用程序的架构和设计时已明确处理安全注意事项。每项组件的功能和安全角色均应清晰界定，并涵盖威胁模型、安全开发和密码匙管理等项目，例如在实施前采取相关及足够的安全控制措施保护数据和交易。

- 数据储存和私隐要求

  开发者应充分了解所处理数据的类型和敏感度，以及是否涉及关键交易。敏感数据可能意外地披露予同一装置上的其他应用程序，数据亦可能在传递期间外泄。此外，与其他类型装置比较，流动装置较容易遗失或被盗取。开发者应依循有关私隐的法律和规例（例如《个人资料（私隐）条例》），订定合适的数据储存和私隐要求。如流动应用程序对私隐有重大影响，应进行私隐影响评估。

- 加密技术的要求

  应采用加密技术保护在流动装置储存和处理或在装置与服务器之间传输的数据。确保流动应用程序按照业界良好作业模式采用加密技术，包括：

  (i) 使用经核实的加密库。
  (ii) 正确选择和配置加密函数。
  (iii) 避免重复使用同一组密码匙作多种用途。
  (iv) 使用安全的随机数字产生器产生随机数值。

- 认证和对话管理要求

  应妥善认证和管理用户帐户和对话，包括使用随机产生的访问令牌认证客户端的请求、执行明确的密码政策，以及在发现过多登录尝试时锁定账户等。应用程序状态变更也应妥善处理，例如在应用程序从后台恢复时需要重新认证。

- 网络通讯要求

  开发者应确保流动应用程序与远程服务端点之间所交换数据的机密性和完整性。处理所有应用程序数据时应使用运用已适当设置的传输层安全（TLS）协议的加密频道。在使用 TLS 时，程序必须执行证书确认功能，不应接受任何自签及 / 或不可信赖的证书。另外，程序亦应可侦测有否使用未获授权证书，以防范网络攻击（例如中间人攻击）。

- 环境互动要求

  应考虑以安全的方式使用平台应用程序界面和标准组件，包括应用程序之间的通讯（程序间的通讯）。

- 程序代码质素和建立设置要求

  开发应用程序时应遵从安全编码作业模式，例如程序应以可信赖的证书签署。证书应有有效期。续签后，应审查证书的安全要求（例如密码算法、密钥长度），以确保一些常见的安全漏洞不会继续存在于新签发的证书中。流动装置的默认访问权限应降至最低（例如停用相机 / 麦克风和默认启用「不追踪」功能）。

- 抵御还原工程能力的要求

  如流动应用程序会处理或访问敏感数据，应采取保护措施以增强程序抵御还原工程的能力。应考虑采取一系列混淆控制措施，如「应用程序隔离」、「阻止动态分析和窜改」、「装置绑定」和「仿真器侦测」等。

5.2.2 设计阶段

设计阶段涉及根据要求阶段所定的规格设计应用程序架构。建立程序架构后，开发团队应参照订定的安全要求，通过识别潜在的遵行要求问题及安全风险审查相关系统设计。这包括为特定类型的数据设计适当的安全控制措施，并结合威胁模型以识别和处理与应用程序有关的风险。

安全审查亦应在设计阶段进行，作为一个检察点，确保已识别所需的安全要求并将之纳入系统设计。

5.2.3 开发阶段

经常留意安全编码标准有助改善安全状况，并减少发生可导致违反安全事件的常见错误。在开发阶段进行安全评估，还有助确定所需的安全控制措施，并适时向开发者提供有关程序代码安全的意见。此外，应进行源码安全评估，及早了解程序代码的质素，以便制作统一和优质的流动应用程序。

5.2.4 测试阶段

除用户验收测试外，系统测试、压力测试、回归测试和单元测试均对确认系统功能的效能和准确性大有帮助。由于相关平台和测试环境各有不同，与网上应用系统比较，流动应用程序的测试可能更具挑战性。开发者应建立全面的测试计划以设计测试方式，并订定「什么」、「何时」及「如何」等测试细节。

5.2.5 推出前阶段

在应用程序推出前和作出重大变更后，应进行安全风险评估和安全审计。每次进行安全漏洞修复时均可能需要更新程序代码，因而可能带来新的安全漏洞。因此，必须持续评估相关风险和影响，以确保流动应用程序安全。

5.2.6 维护与支持阶段

应用程序的新增功能或对现有功能的更新都可能为系统带来变更，因此应制定、记录、测试和审查安全措施，确保系统得到妥善保护或免被破坏。持续测试对保障安全十分重要，可保护应用程序免受大部分攻击。应定期审视应用程序，确保有足够的保障。

5.2.7 停止使用阶段

如应用程序不再符合预定目标或有其他应用程序更能达到预期目的，应考虑停止使用程序。停止使用计划的建议如下：

- 制定通知方案知会所有相关持份者（例如应用程序用户）
- 从正式运作环境移除应用程序（例如流动应用程序商店）

5.3 安全设计与数据保密

安全设计与数据保密的概念应纳入整个应用程序系统设计及开发程序，以保障数据和个别人士的私隐权。开发者应确保已将安全考虑纳入为基本架构设计的一部分，并应审视因应潜在安全问题而作的详细设计，以及决定和制定应对潜在威胁的缓解措施。在订定私隐要求时，亦应遵从相关法律、规例和条例（例如《个人资料（私隐）条例》）。在系统设计阶段，开发者应注意以下良好作业模式，以保障用户私隐：

通知用户

- 知会用户应用程序将收集什么数据 / 数据、有关数据将作什么用途，以及将如何处理该些数据。
- 容许用户选择不查阅 / 使用个人资料。
- 在用户要求移除应用程序或删除帐户时，让用户可选择删除所有应用程序相关数据及与帐户相关的数据。
- 在流动应用程序的安装页面上向用户显示私隐政策声明，以解释数据收集、访问和使用的目的，从而增强用户的信任度。

数据处理

- 尽量减少收集个人资料（特别是敏感个人资料），并将流动装置功能（例如相机和位置追踪）的权限降至最低。
- 采用严谨的加密功能和访问控制措施保障用户的个人资料，以免在未获授权的情况下被访问、外泄或使用。避免将个人辨识数据（例如身分证明文件、通讯记录）或其他敏感数据储存在用户装置上。
- 未经用户许可，切勿将敏感数据上载或同步传输至外部系统或装置。
- 在完成声明用途的数据使用后，清除敏感数据（例如地理位置数据）。

5.4 开发流动应用程序的测试

由于流动操作系统、硬件组件和网络环境各有不同，因此在流动装置上测试流动应用程序较在个人计算机上测试网上应用系统更具挑战性。测试流动程序时应考虑以下各个方面：

测试流动应用程序的功能

为了确保流动应用程序能在支持的装置上正常运作，应进行功能测试，以验证应用程序的功能规格。此外，亦需考虑进行不同类型的流动应用程序测试：

- 兼容性测试：确保应用程序能在支持的装置（如配备 iOS 和 Android 等不同流动平台，以及不同屏幕尺寸和操作系统版本的装置）上正常运作。
- 效能测试：测量应用程序的效能，如响应速度、可接受的用户负载和程序稳定性等。
- 系统测试：确保流动应用程序能找出并处理可能出现的异常情况，并能从意外终止事故中恢复正常运作。

测试程序代码质素

开发者在流动应用程序开发过程中会使用不同的编程语言和框架，如没有遵从安全编码作业模式，应用程序可能会出现常见的漏洞（例如弱点插入、内存损毁和跨网址程序编程）。举例来说，注入式攻击多数利用流动装置的跨进程通讯（IPC）界面，以恶意应用程序攻击在该装置上运作的另一应用程序。程序的测试，应可发现可能容许不可信赖输入的进入点，或发现调用已知的危险源码库应用程序界面的地方。

为确保流动应用程序的源码不会因安全漏洞而受到损害，应尽早进行常规源码扫描，以检测任何可能对流动装置构成风险的安全漏洞或缺陷。

流动应用程序的加密技术

加密技术对于保护用户在流动网络环境中的数据至关重要，尤其当攻击者或可实体访问用户装置的情形。开发者应采用妥善的加密方法或合适的密码匙储存应用程序界面储存敏感数据。不要使用任何包含已知漏洞的加密算法或协议。采用良好作业模式和安全配置，确保有关加密算法是最新的，并且符合行业标准。切勿使用过时的加密法（例如 DES）或哈希函数（例如 SHA1）。应妥善处理不当的配置问题，如密码匙长度不足、硬编码的密码匙和不严谨的密码匙产生函数等问题。

流动应用程序的认证

前端客户及后端服务器均应整合和进行适当的身分认证，以防止遭受密码字典攻击或暴力攻击。一般而言，属非敏感性质的应用程序可考虑以用户名称 / 密码认证；至于属敏感性质的应用程序，则通常会考虑使用双重认证（例如短信和令牌）。应进行测试，确保前端用户及后端服务器均贯彻执行有关认证程序。

应按以下步骤测试应用程序的认证和授权方法：

- 确定应用程序使用的附加认证方法。
- 找出提供关键功能的所有端点。
- 验证已在所有服务器端点严格执行该些附加的认证方法。

测试网络通讯

流动装置与服务器之间的网络通讯通常在不可信赖的网络上进行，因此流动应用程序可能会蒙受网络攻击（如小包探取法或中间人攻击）的风险。在处理敏感数据时，应使用加密连接（例如 HTTPS），以确保网络数据的机密性和完整性。拦截接受测试的应用程序所接收和传送的网络通讯，并确保通讯已加密，例如利用数据包分析器收集网络通讯，并利用网络协议分析器以人类可读格式显示收集所得的通讯。最后，验证服务器已按照良好作业模式进行配置。

5.5 开发安全流动应用程序的注意事项

流动应用程序与其他应用系统一样，有类似的安全考虑和风险，因此一般有关程序开发的良好作业模式亦适用于开发流动应用程序。因应不同的用途、使用模式和流动平台，流动应用程序开发者亦应留意远程网络服务、平台整合和流动装置的不安全性。开发者在建立安全的流动应用程序时应考虑以下各个方面：

- 一般考虑
- 系统 / 软件
- 数据
- 网络管理

5.5.1 一般考虑

- 处理敏感资料时必须紧记安全及提供充分的保护。
- 知会用户应用程序将访问和上载什么数据，以及有关数据将作什么用途。
- 如会收集个人资料，应提供收集个人资料声明。
- 采取「最小权限」原则，以最小的系统权限及访问权限执行应用程序。
- 按照良好作业模式开发和执行应用程序。
- 设计和提供方法，让应用程序能进行安全修补程序更新。
- 如流动应用程序会处理关键 / 敏感数据，一旦发现已被越狱或破解根权限，应拒绝执行应用程序或向用户发出警告。
- 在处理数据前，必须确认所有客户端提供的数据，并检查数据是否在预期类型、范围和长度的范围内。
- 在程序活动使用大量数据时知会用户和得到用户的同意。

5.5.2 系统 / 软件

认证和对话管理

- 避免只使用装置所提供的标识符（如 UID 或 MAC 地址）识别装置，而应利用应用程序和装置特有的标识符。
- 采用适当的认证机制，并根据流动应用程序风险评估结果，在处理敏感或财务交易时考虑使用双重认证。
- 避免储存密码；完成计算密码的哈希后，应立即清除 / 删除载有密码的内存位置。
- 充分利用由流动平台所提供的最新安全机制，以保护用户的凭证。
- 在每个活动 / 画面开始时检查用户是否已在登入状态，否则应切换到需登入状态。
- 在应用程序的对话超时或用户注销时，清除和删除所有与用户数据有关的内存和用作数据解密的主密码匙。

服务器控制措施

- 评估流动应用程序的后端服务以找出安全漏洞，并确保后端系统执行已强化的配置和安装最新的安全修补程序。
- 确保后端服务器已保存足够的记录或数据，以作安全事故侦测及应急和进行调查。
- 检视应用程序的程序代码，以避免在流动应用程序与后端服务器之间不慎传送数据。

程序代码混淆 / 还原工程

- 于应用程序启动时验证应用程序的标识符，以确保程序代码没有被更改或破坏。
- 如程序代码没有被编制成机器码格式以防止还原工程，应尽量使用混淆软件，以保护源码和隐藏应用程序数据。
- 对包含敏感数据的应用程序采用抗调试技术（如防止调试程序附加至程序程序）。

使用第三方 / 开放源码库

- 使用可靠及 / 或官方版本的软件开发工具（例如软件开发套装、软件库），以避免在不知情的情况下引入木马程序或后门程序。
- 留意流动应用程序所使用的第三方框架 / 应用程序界面的最新发布，以安装安全修补程序和进行升级。
- 应先确认所有经不可信赖的第三方应用程序往来的数据（如广告网络），才在流动应用程序中使用。

5.5.3 数据

数据储存和保护

- 只收集和披露程序业务用途所需的数据。
- 按数据的敏感度对数据储存进行分类和采取相应的控制措施，并根据分类处理、储存和使用数据。
- 基于「最小权限」和「有需要知道」的原则，应将个人资料加密和对其访问控制有所限制。
- 除非已采取适当的安全措施（例如严谨的加密），否则不应将应用数据储存至外置储存器。
- 将敏感数据储存或暂存至非挥发性内存时，使用适当的算法和密码匙长度进行加密，并将流动应用程序所需使用的数据减至最少，以保护数据。
- 对应用程序可接收数据的相关区域进行输入确认和检查，以防止客户端程序代码注入或屏幕劫持。
- 在不再需要敏感数据时，清除和删除内存中所有敏感数据。
- 采用沙盒技术隔离应用程序，通过防止其他应用程序与受保护的应用程序进行互动，提高程序的安全性。

网上支付

- 就使用应用程序将会涉及的费用向用户发出警告并获取其同意。
- 如涉及付款资源，应推行安全控制措施（如白名单或重新认证），以防止在未经授权或意外的情况下访问有关资源。
- 如需进行网上支付，应使用安全的流动支付服务。使用由官方提供的应用程序界面 / 模板，并严格遵从其执行指南。
- 知会用户流动装置必须支持的最低技术规格（例如 TLS），以进行支付服务。
- 在开发设有网上流动支付服务的流动应用程序时遵守特定的数据安全标准（例如《中华人民共和国个人信息保护法》，PCI DSS）。

5.5.4 网络管理

通讯安全

- 任何敏感数据（例如个人资料或信用卡数据）的传递均应使用端对端加密方法（例如 TLS）以作保护。
- 在使用 TLS 时，程序必须执行证书确认功能，不应接受自签及 / 或不可信赖的证书。

- 如得悉应以保密超文本传输协议（HTTPS）连接，侦测每项要求的连接是否均已使用 HTTPS。
- 启动应用级虚拟专用网络（per-app VPN），安全地从任何地方和在任何流动装置访问内部网络资源。

5.6 开发 iOS 和 Android 安全流动应用程序的良好作业模式

开发人员还可以参考由个人资料私隐专员公署发布的开发流动应用程序最佳行事方式指南，指南可在个人资料私隐专员公署网站上找到。(https://www.pcpd.org.hk/mobileapps/practice.html)

*** 完 ***

附件 A: 安全强化配置模板

建议用以下流动装置强化的安全配置作参考。该安全配置宜按决策局 / 部门的业务需要进行加强及修改。部分配置需要利用额外安全方案来加强，如流动装置管理或数据遗失防护方案。决策局 / 部门宜在有需要时，就安全强化咨询产品供货商或第三方的顾问。

控制[3]	手提电脑	流动电话及平板计算机
密码		
需要密码	是	是
需要复杂密码（如大小写不一的字母、数字及特殊字符）	是	是
最短密码长度	8	8
容许输入失败次数	5	5
最长密码使用期	每三个月到六个月	每三个月到六个月
密码历史	8	8
装置闲置时限	最多 5 分钟	最多 5 分钟
其他装置设定		
侦查装置有否越狱、根权限被破解，或违反软件版本	是	是
容许安装来自可靠来源的应用程序	是	是
容许安装来自不知明来源的应用程序	否	否
容许备份至供货商的云端服务	否	否
容许备份钥匙串及钥匙存库	否	否
容许分享相片	否	否
容许透过通用串行总线传送档案	若加密，是[4]	若加密，是 [4]
容许用户接受不可信传输层安全协议证书	否	否
容许修改账户设定	否	否

[3] 所列项目均是用于控制流动装置（包括手提电脑、流动电话及平板计算机）的控件目模板。项目未必全面详尽，因此决策局 / 部门应按业务需要修改成最合适的要求清单

[4] 应加密所有储存在流动装置或抽取式媒体内的数据

控制[3]	手提电脑	流动电话及平板计算机
容许网络共享设定	否	否
容许利用生物特征为装置解锁	否	否
在锁定画面显示讯息	否	否
修改蓝牙设定	否	否
容许传送诊断性数据及使用性数据至流动装置供货商	否	否
装置需要加密（例如，全磁盘或档案为本的加密）	是	是
启用审计追踪	是	是
使用自动时间或与可靠时间服务器同步	是	是
强制加密备份	是	是
启用遥距清除功能	未能使用 [5]	是
启用多次登入失败本机清除功能	未能使用 [5]	是
容许邮件预览	否	否
容许讯息预览	否	否
启用自动连接 / 自动加入网络	否	否
启用询问是否加入网络	是（如有）	是（如有）

[5] 手提电脑操作系统未必能提供遥距及本机清除功能，因此决策局 / 部门宜考虑手提电脑失窃的风险，并采用加密方法作为补偿控制

附件 B: 容器化技术

流动装置管理策略的核心目标，是为私人拥有流动装置内的个人和业务用应用程序及相关数据划分界线，即现在所称的容器化，将业务应用程序和相关数据安放于数字容器（实体或虚拟）内，以规管应用程序的行为，并防止应用程序与个人应用程序间有未授权的互动。

不同供货商提供的不同容器可以分为三种类别：实体容器、虚拟容器，及应用程序容器。

实体容器

实体容器于流动装置芯片组或核心层面将业务应用程序（及其数据）与个人应用程序分隔。实体容器于硬件层面分开流动装置用户的业务环境与个人环境。这意味于核心层创建一个个别的操作系统层迭，专门储存及操作业务应用程序。这操作系统层迭与用户一般应用程序所使用的操作系统层迭截然不同，亦因此管理员可在这「实体容器」内执行个别机构的安全规定。实体容器其中一个主要安全重点是操作系统层叠一般需要借助个别处理器的处理能力。

实体容器其中一个最大优点是其彻底的安全隔离。由于实体容器将另外的操作系统层迭从正常操作系统层迭隔离，因此完全断绝业务与个人应用程序间的互动。亦由于这是一个分开的平台，所以不会继承该流动装置上的漏洞。

但层迭层面的分隔亦为实体容器方案带来一个主要缺点中断了用户的体验。每当用户登入流动装置的正常操作系统层迭后，都需要注销然后登入另外的操作系统层迭才能使用业务应用程序；而当用户想用回个人应用程序时，又需要将过程反复重复一次。不断的转换不但为用户带来不便，亦会在一段时间后对用户生产力造成影响。现时，实体容器方案依赖操作系统支持；第三方及内部软件开发者需要个别调整应用程序以支持实体容器。

虚拟容器

业务应用程序被分隔储存在操作系统中的一个加密工作间内，尤如一个执行多个应用程序的沙盒。在虚拟容器内，政策管制应用程序间可以进行甚么类型的互动。所有容器内应用程序间的互动只能在容器内发生，而所有虚拟容器内应用程序的数据于虚拟沙盒范围内仍然保持安全。

流动装置用户需要输入另外的密码来验证容器以进行业务活动。在使用虚拟容器的情况下，业务应用程序与个人应用程序之间的逻辑分隔由操作系统及核心负责。由于容器于流动装置内运行，因此装置操作系统的漏洞可能影响容器的安全。此外，此方案需要第三方及内部软件开发者个别调整应用程序，以支持个别供货商的容器环境。虚拟容器策略亦需要个别技能及额外的行政工作来持续支持。

应用程序容器

应用程序容器为每个独立应用程序及相关数据提供一个独立的安全沙盒，并能让管理员提供更仔细的控制以保护机构数据，同时给用户提供无缝的用户体验。在此方案下，管理员可以选择配置适用于所有应用程序的一般政策、个别应用程序的专属政策，或结合以上两者。管理员亦能仔细控制每个应用程序的数据流向，例如进入与外出的通讯。另外，由于每个容器内的应用程序数据都是独立地加密及由政策保护，因此即使流动装置感染恶意软件，业务应用程序仍能得到保护。

由于容器是在应用程序上执行，用户一般无需经常进出容器内外的环境以转换个人及业务应用程序。无论是个人或业务应用程序，用户都能够轻易看见及访问获准使用的应用程序。混合使用应用层面的政策管制及加密，能给决策局 / 部门更高的安全水平以保持业务应用程序及数据安全。

附件 C: 评估授权流动应用程序的指南

1. 评估流动应用程序的指南

为了评估流动应用程序是否适合安装，建议各决策局 / 部门了解流动应用程序是否可以满足业务或操作需求，以及流动应用程序的安全是否足够。一个重要的考虑因素是安装流动应用程序后，不应导致现有流动环境的安全程度受损或导致数据外泄。

建议各决策局 / 部门采取风险为本模式，循以下各方面评估流动应用程序：

- 流动应用程序的功能

  决策局 / 部门除了解流动应用程序是否适用于支持业务或操作，还应评估流动应用程序提供的所有功能（包括那些额外功能）是否存在任何风险，这些风险可能会影响流动环境的安全程度。 如果可能的话，请停用不必要的功能。

- 流动应用程序的声誉和可信度

  现成的流动应用程序必须是在官方流动应用程序商店（如 App Store 或 Google Play）可供下载的。此外，必须从可信任的流动应用程序商店下载以进行安装。最好能显示该应用程序有大量下载或获取安全验证证书，例如 ISO / IEC 15408，通用标准。

- 没有恶意软件

  决策局 / 部门下载了流动应用程序后，应用流动平台提供的安全工具扫描该应用程序，以检查是否不含病毒，间谍软件，恶意软件等。

- 流动应用程序所需的合理权限

  流动应用程序权限可让应用程序访问流动装置的资源（例如联络人，讯息，相机，位置，电话，储存空间等）以及与该流动装置的其他流动应用程序（例如浏览器）进行互动。决策局 / 部门应检查授予流动应用程序的权限是否合理。

- 与后端平台的连接

  决策局 / 部门应评估流动应用程序是否会自动连接到外部后端服务，网站或云端平台，以了解将要与之作互动的网站或云端平台是否合宜，是否涉及自动收集数据（例如了解有关征求用户同意的披露协议），以及是否涉及任何潜在的敏感数据。

以上准则仅作为一般指南，并非详尽无遗。建议各决策局 / 部门定期监察流动应用程序的更新，例如该程序在官方流动应用程序商店是否仍可供下

载。对于更严格的安全要求，建议各决策局 / 部门进行安全风险评估及审计以及流动应用程序源码扫描，以了解流动应用程序源码的安全程度，以及第三方工具（软件库，广告网络，API 等）的适当用法。

2. 更新用于业务的应用程序白名单

关于白名单的订定，一些决策局 / 部门可能会采用软件资产管理来备存软件清单和软件特许使用权，以确保决策局 / 部门使用获授权的软件和流动应用程序。软件资产管理可以帮助决策局 / 部门控制软件的采购，减少误用流动装置和并非蓄意侵犯版权的风险，并尽量提高用户的工作效率。软件资产管理中的获授权列表可以视为供用户在决策局 / 部门的流动装置安装获授权软件和流动应用程序的白名单。另外，亦可考虑在决策局 / 部门流动装置所预安装的流动应用程序列表。这两个清单应定期作检讨，以确保获授权软件和流动应用程序的列表是最新的。

如软件或流动应用程序不在应用程序白名单中，用户应提交请求和相关理据（例如支持业务需求 / 操作，提高工作效率）。建议决策局 / 部门按 4.3.2 节中所订明的要求，为流动应用程序进行流动安全风险评估。所有决策局 / 部门均应遵从所有软件和流动应用程序的特许使用权，购买协议和知识产权署所建议有关版权的现有法例。建议各决策局 / 部门仔细阅读私隐政策以及软件或流动应用程序的条件和条款。如有疑问，建议各决策局 / 部门咨询软件供货商或知识产权署。各决策局 / 部门在通过审批机制获得决策局局长 / 部门首长的批准后，必须相应地更新应用程序白名单。

3. 白名单和黑名单样本

白名单列出受信任和获授权的软件或流动应用程序，这些软件被认为是可以安全地安装在各决策局 / 部门提供的流动装置上。在制订应用程序白名单时，各决策局 / 部门应参考其备存的软件资产管理的软件清单。此外，应定期更新和检讨应用程序白名单。

黑名单与白名单相反，列出禁止在流动装置上安装或运行的软件和流动应用程序，因为可能会导致网络安全威胁。但要更新黑名单得花费不少工夫。

通常白名单和黑名单应包括以下数据以供参考。

白名单配置（包括政府自行开发 / 授权的应用程序）

序号	配置设定	样本值
1.	白名单流动应用程序 – 名称	GovHK Notifications
2.	白名单流动应用程序 – 开发人员 / 供货商	HKSARG
3.	白名单流动应用程序 – 版本	2.1.0

序号	配置设定	样本值
4.	平台 (例如 iOS, Android, Windows 10)	iOS / Android
5.	装置 (例如 iPhone, iPad, Android phone, Android tablet, laptop)	iPhone/iPad/Android phone/Android tablet
6.	尝试安装白名单流动应用程序时要执行的操作	允许访问/ 启用
7.	授权访问的用户组（例如所有用户、指定小组的用户、高级经理或更高级别）	所有用户
8.	理据	用于测试不同应用程序上的互用性
9.	软件类型（例如从网站上免费下载，通过流动应用程序商店免费下载，个人购买的特许使用权）	通过流动应用程序商店免费下载
10.	条款和条件的网页连结	https://www.xxx.com/licensing.html
11.	批准日期（YYYYMMDD）	20201213
12.	批准的到期日（YYYYMMDD）	20221213
13.	开源软件（例如 Y、N）	N
14.	免费软件，共享软件或已购买	免费软件

黑名单配置

序号	配置设定	样本值
1.	黑名单流动应用程序 – 名称	MyGame
2.	黑名单流动应用程序 – 开发人员 / 供货商	GameDeveloper
3.	黑名单流动应用程序 – 版本	1.0.3
4.	平台（例如 iOS, Android, Windows 10）	iOS
5.	装置（例如 iPhone, iPad, Android phone, Android tablet, laptop）	iPhone/iPad/Android phone/Android tablet
6.	尝试安装黑名单流动应用程序时要执行的操作	禁止访问
7	加入黑名单的日期（YYYYMMDD）	20201220