政府资讯科技总监办公室

信息安全

Wi-Fi 安全

实务指南

第 1.1 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	更新縮寫及術語	1	1.1	2021 年 6 月

目录

1. 简介

此文件旨在为不同的羣体服务，例如管理人员、系统拥有者、信息科技安全管理员、区域网域网络/系统管理员和信息安全持份者，他们负责设置和管理政府内部的 Wi-Fi 网络。

一些决策局 / 部门用户可以使用具有多种通讯技术（包括 Wi-Fi）的流动装置。有关采用流动装置和相关管理的安全指南的详细信息，请参阅《流动安全实务指南》第 4 节。

1.1 目的

本文件的目的是为决策局 / 部门提供常见的安全注意事项和良好作业模式，以说明设计、管理和操作在政府里的 Wi-Fi 网络。本文件第 4 节介绍良好作业模式。

1.2 参考标准

以下参考文件对于本文件的应用是不可或缺：

- 香港特别行政区政府《基准信息科技安全政策》[S17]
- 香港特别行政区政府《信息科技安全指南》[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

1.3 定义及惯用词

本文件将会采用《基准信息科技安全政策》，《信息科技安全指南》和以下的术语及惯用词。

缩写及术语	
Wi-Fi	Wi-Fi 是基于 IEEE 802.11 系列的无线通信技术
5G	5G 是指第五代的流动通讯技术，它是由国际电信联盟为发展新一代流动科技而制定的。

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各项功能的领域：

- 安全管理框架和组织；
- 治理、风险管理和合规；
- 安全操作；
- 安全事件和事件管理；
- 意识培训和能力建设；和
- 态势感知和信息共享。

安全管理框架和组织

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。

治理、风险管理和合规

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。

意识培训和能力建设

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计算机安全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. Wi-Fi 安全概述

3.1 Wi-Fi 网络简介

Wi-Fi 是基于 IEEE 802.11 系列的无线通信技术，通常用于各种信息科技设备例如流动电话、便携计算机、全球定位系统设备以及物联网装置等，以存取局部区域网络或互联网。

Wi-Fi 使用高频无线电波（而非有线），令信息科技设备和装置之间进行通讯。无线讯号的特点是有关讯号普遍在无线局部区域网络所覆盖的范围内通过空气传输，并且可以穿透实体边界，如建筑物墙壁和窗户。因此，除非已采取安全措施防止透过无线传递不被「窃听」，否则任何人都可以在实体边界之外读取此类讯号，带来潜在的安全风险。连接到政府内部网络的 Wi-Fi 须采取充分认证和传递加密措施，并辅之以适当的安全管理程序和良好作业模式。

3.2 典型的 Wi-Fi 网络

此节简要介绍典型的 Wi-Fi 网络供参考。决策局 / 部门应根据业务需要和运作，决定其 Wi-Fi 网络的配置。

典型的 Wi-Fi 网络可以有四个主要部分：客户端装置、Wi-Fi 存取点（存取点）和网络路由器/交换机、管理系统和互联网网关。客户端装置的例子包括笔记本电脑、平板计算机和智能手机。存取点提供客户端装置与网络之间的无线连接。网络路由器在后端连接存取点和管理系统。管理系统监察和控制 Wi-Fi 网络上的活动。它通常包括无线入侵防御系统、无线网络管理系统、认证系统和抗恶意软件程序系统。管理系统须要处理网络和应用层面的安全威胁，例如未获授权访问和恶意活动。互联网网关管理与互联网服务供货商的连接。它还包括防火墙、入侵检测或防御系统以及将内部网络连接到互联网的路由器。

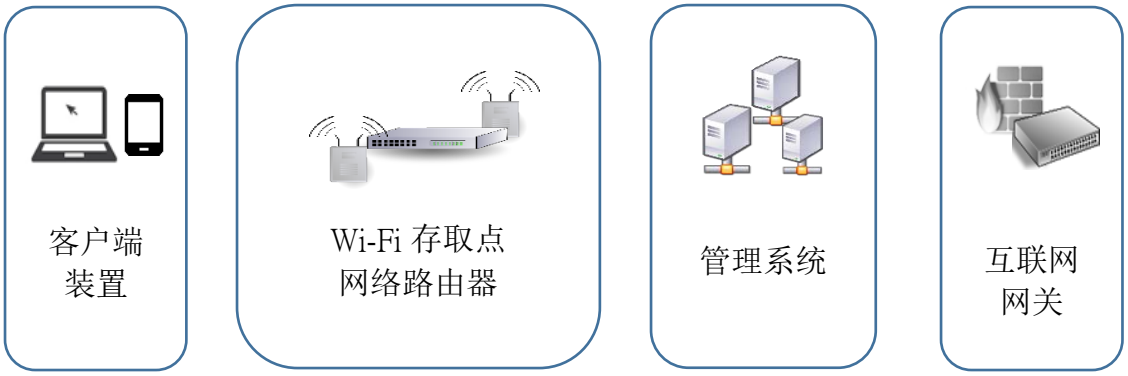

图 1 典型 Wi-Fi 网络的四个主要部分

4. Wi-Fi 网络面对的威胁和漏洞

4.1 威胁和安全漏洞

现今无线连接藉其从大型机构到个人使用的计算机以及网络等各个方面都被广泛采用的优势，令其得以起着重要的作用。然而，随着无线网络的可用性提高，也意味着遭受攻击的危险也会相对增加，同时也为机构、信息科技人员和信息科技安全专业人员带来更多挑战。攻击者可能试图掌握关于网络的信息，以利用网络安全漏洞。对网络而言，这也是一项安全威胁。Wi-Fi 网络的安全威胁描述如下。

Wi-Fi 存取点

- 破解有线等效保密协议/无线保护访问

  采用以前版本的安全协议（如有线等效保密规约或无线保护访问）作保护的无线网络，因应现今的技术而言是不安全的。

- 存取点有不妥善的配置

  若存取点有宽松或不正确的设定，会容许未获授权的装置联机或使连接的通讯暴露在嗅探攻击和回放攻击中。

- 无线窃听

  如果不妥善设定存取点而网络通讯亦未经加密，敏感的通讯或系统事项将受到威胁。如果网络通讯包含清晰的文字，恶意攻击者便能够使用窃听工具取得敏感数据，如密码或信用卡号。

- 「邪恶双胞胎」（仿冒）

  「邪恶双胞胎」是一个假冒的 Wi-Fi 连接，它欺骗用户，令其相信这是合法连接，目的是进行仿冒诈骗攻击以及利用数据交易找出安全漏洞。就「邪恶双胞胎」的攻击，攻击者收集有关该合法存取点的信息，然后设置其系统以仿冒该合法存取点。攻击者使用比合法存取点更强的广播讯号，让无戒心的用户连接到其存取点。

- 恶意存取点（未经授权的装置）

  恶意存取点是未经网络管理员明确授权所安装的存取点。它可能造成中间人攻击，让网络安全受到破坏。

Wi-Fi 讯号

- 「背负式」

  存取点的广播范围可以在建筑物的墙壁和窗户之外提供无线连接。如果未能妥善配置无线网络，则在该存取点范围内，任何人只要有已启用无线功能的计算机，就可以使用该连接。这些用户能够进行非法活动，监视与撷取网络信息，或从网络窃取档案。

- 「战争驾驶」

  类似「背负式」，「战争驾驶」是指实体地搜索不安全的无线网络或容易受到破坏的网络。

- 拒绝服务

  拒绝服务是指一种攻击，旨在剥夺某一个体的服务之可用性。攻击者利用无线电干扰讯号，直接损害无线连接或设备，使它们保持忙碌。

- 窃听

  窃听是指秘密收听通讯的行为。对于客户端设备和存取点之间的网络通讯，未经授权的监察容易导致通讯被窃听，并且没有实体拦截的迹象。

具有 Wi-Fi 连接的流动装置

- 互联网连接共享和桥接客户端

  一个装置若能分享互联网连接或允许同时连接多个网络，就可用于绕过网络监察和安全控制。这可能会导致丢失数据或提供了安全不妥善的网络进入点给攻击者。

- 流动装置被窃

  采取保护措施去避免丢失或盗去具有 Wi-Fi 连接的流动装置是非常重要的。通过实体窃取流动装置，攻击者可以不受限制地访问装置上的所有数据以及任何已连接的云端账户。

5. Wi-Fi 网络设置和操作的安全考虑

一般来说，有线网络设置和操作的安全考虑亦适用于 Wi-Fi 网络。具体来说，决策局 / 部门应制订 Wi-Fi 安全政策，以及遵行本节就 Wi-Fi 网络所描述的安全措施之作业模式。在计划过程中，在 Wi-Fi 网络的设置和操作方面若有考虑安全事宜，就会减少网络暴露于较常见的攻击。

5.1 设置 Wi-Fi 网络的安全考虑

应部署安全措施和控制以保护 Wi-Fi 网络。以下是一些相关的人员，如网络拥有者、网络管理员和终端用户常见的安全考虑。

网络拥有者

- Wi-Fi 网络的用途

  应清楚说明 Wi-Fi 网络的目的和功能要求。如果 Wi-Fi 网络是独立的，只供外部用户访问互联网，该 Wi-Fi 网络须实体上与决策局 / 部门的网络分开。应为不同类型的用户和要传递的数据类型及其数据安全级别，分别指定 Wi-Fi 网络的访问控制。

- Wi-Fi 安全策略

  应制定 Wi-Fi 安全政策，以处理无线网络的所有使用选项，以及可传递的信息类型。应定期检讨这项政策，以应付最新的科技及业务发展。该政策应包括但不限于定义 Wi-Fi 管理者的角色和责任、安装和使用程序以及操作指南。

  例如，使用策略应订明如当 Wi-Fi 功能不再使用时，就应关掉，并且不应分享或披露用于接达 Wi-Fi 网络的加密密钥或凭据。应分配独立无线局部区域网络供访客。职员不允许设置自己的存取点。

- 数据保护和配置备份

  此项措施包括数据储存时加密，安全的数据传递和定期备份所有在客户端装置和端点有用之数据，以及在网络装置内的配置档案。

- 信息科技安全风险评估和审计

  Wi-Fi 网络须定期接受安全风险评估和审计。各决策局 / 部门须按在安全风险评估和审计中发现的任何安全漏洞，采取必要的补救措施。因应 Wi-Fi 技术的迅速变化，Wi-Fi 网络的安全风险评估和审计须每年进行一次。

- 监测和预防

  这些措施包括记录和审计网络活动、漏洞扫描、有效的信息发布机制和向所有工作人员提供关于 Wi-Fi 安全政策的安全意识培训。应将活动记录转移到远程记录服务器，并确保所有记录的全面性和完整性。应定期审查和检查记录，以及发现任何可疑活动时进行分析。

- 安全事件处理

  决策局 / 部门需要遵守现行的信息安全事件响应机制，将与 Wi-Fi 网络相关的任何安全事件报告给政府信息安全事件应变办事处。还应定期更新该机制，以处理新的潜在安全威胁。决策局 / 部门还需要提供一个联络点，以便在紧急情况下，决策局 / 部门在短时间内关闭受影响的网络。

- 保留清单并定义硬件弃置原则

  保持一个准确的 Wi-Fi 组件库存，包括网络交换机、路由器、互联网网关、存取点和其他相关组件，以确保只有授权用户装置才能连接到 Wi-Fi 网络。一旦装置遗失，应立即更改加密密钥和服务设定标识符。

  在硬件弃置策略中，当弃置所有硬件（包括任何 Wi-Fi 组件或装置）时，应要求对装置上的所有敏感信息（如系统配置、预定的共享密钥、数字证书和密码）进行清理。

- 定义修补程序管理原则

  定期测试和更新所有硬件、设备和软件程序的最新韧体和安全修补程序，以防止因疏忽而造成的漏洞及恶意攻击。

网络管理员

网络管理员应考虑在多方面采取以下安全措施，以保护 Wi-Fi 网络的可用性以及信息的机密性。

- Wi-Fi 网络容量

  为确保 Wi-Fi 网络的可用性，应考虑 Wi-Fi 网络用户数量的多少和应用程序的类型（例如，语音/视像会议或网上浏览），评估无线连接的容量。

- 存取点的实体保护和位置

  无线讯号通常不会覆盖在特定区域中。过度覆盖可能让恶意用户对网络构成重大的威胁和增加攻击的机会。因此，存取点的位置和无线讯号的强度应经过小心设计，在实际可能的情况下使在设计区域之外不提供无线讯号。例如，应考虑将存取点安装在远离窗户或门的地方，以防止来自公共地方的区域网络窃听。还应避免对同地域无线网络的相互干扰。建议进行场地勘察，以确定 Wi-Fi 基础设施的覆盖范围、存取点的数量及其位置和讯号覆盖范围和质量。

  网络设备（如存取点）应安装在具有严格实体安全控制的设施中，以防止盗窃、破坏或篡改，特别是对于放置在开放区域的存取点。应考虑将存取点安装在天花板上，并锁定配线设施。此外，应考虑使用任何锁定机制来实体限制对存取点的电源按钮、重置按钮或端口（例如通用串行总线）的访问。

- 网络分段

  应为访客、应用开发和内部网络进行 Wi-Fi 网络分段。存取点覆盖区域的分段还可以平衡 Wi-Fi 网络上的负载，从而最大限度地降低可用性的风险。此外，应限制 Wi-Fi 和有线网络之间的互连。应采用分段 Wi-Fi 网络之间的访问控制（例如防火墙、端口/应用程序/媒体访问控制的地址过滤）。

- 传输标准

  Wi-Fi 网络的传输标准是基于 IEEE 802.11 标准，如 802.11g、802.11ac、802.11i、802.11n 和最新标准 802.11ax。从安全角度来看，802.11ax (Wi-Fi 6) 与 Wi-Fi 保护接入 3 (WPA3) 协议引入增强的认证和加密功能。

  Wi-Fi 6 是 Wi-Fi 技术的最新标准。它的设计是为了响应全球越来越多的无线装置和小工具。与之前的版本 (802.11ac) 相比，它的功能和特点都改进了。应考虑使用最新版本的通讯协议 (如 IEEE 802.11ax) 来构建 Wi-Fi 网络，尤其是物联网系统，它可能连接多达数千台将会要连接的装置。

Wi-Fi 保护接入 3 (WPA3) 有两种模式，即 Wi-Fi 保护接入 3 (WPA3)-企业模式和 Wi-Fi 保护接入 3 (WPA3)-个人模式。建议使用 Wi-Fi 保护接入 3 (WPA3)-企业模式，因为它提供了增强的安全功能来构建 Wi-Fi 网络。若使用 Wi-Fi 保护接入 3 (WPA3)-个人模式，应定期更改加密密钥。

- 互联网网关

  互联网网关的安全措施包括防火墙、入侵检测系统和入侵防御系统，用于检测和防止任何可疑活动。应安装防火墙以防止网络攻击和入侵。视乎情况，决策局 / 部门还应扫描/监察网络通讯，并筛选可疑的协议、数据报和内容。

- 管理系统

  位于用户区域的合法 Wi-Fi 存取点，应启用认证。应实施用户身份认证，特别是无线装置。应安装主机级的防火墙和抗恶意软件程序的防护。还应在 Wi-Fi 和有线网络上安装入侵防御系统，以检测任何可疑活动。

- 存取点的配置

  存取点是 Wi-Fi 网络的核心组件。需要为存取点制定基准安全配置标准，以采取适当措施保护它们。建议的控件包括但不限于以下各项：

  - 更改存取点的默认设定。例如更改默认管理帐户和密码，禁用存取点上的不必要或不安全的服务、协议和未使用的管理界面。
  - 确保所有存取点具有严谨、独一无二的管理密码，并定期更改密码。
  - 将预设服务设定标识符 (SSID) 的名称更改为适当且不显眼的名称 (例如，Wi-Fi.HK)。SSID 的名称应防止披露网络的系统详细信息，如产品名称/型号。
  - 如果独立 Wi-Fi 网络仅供获授权的默认装置使用，则不要广播 SSID。如果需要广播 SSID，则只能覆盖在指定的范围内。
  - 在用户区域中对合法存取点进行认证。

- 客户端装置

  应隔离个别客户端避免点对点通讯，以防止恶意软件攻击。应使用具有 Wi-Fi 防御的流动装置的客户端数码证书，以便只允许授权装置存取部门网络或资源。

5.2 Wi-Fi 网络运作的安全考虑

就 Wi-Fi 网络的不同组件，各方人员（如网络管理员和用户）应采取以下 Wi-Fi 网络操作的安全措施。

网络管理员

网络管理员应在客户端装置、管理系统和连接中实施以下技术安全措施。

客户端装置

网络管理员应保护部门网络，避免受来自客户端装置的恶意软件程序感染，并限制只供已获授权的客户端装置使用。定期变更存取点的加密密钥。

管理系统

应记录用户活动和监察事件，以检测任何恶意活动并作进一步调查。应该修补存在网络装置的安全漏洞，因这些安全漏洞可能会被入侵者利用；定期扫描 Wi-Fi 讯号，以侦测恶意存取点是否已安装在 Wi-Fi 网络的覆盖范围内；和侦测可疑网络流量和恶意攻击。

客户端装置与连接

就与客户端的连接，终端用户应把经无线方式传递的数据加密，以保护数据的机密性。客户端装置应避免连接不可信任的/不知名的存取点，和不要以 Wi-Fi 热点或临时模式联网，分享或扩展政府内部网络。

终端用户

以下是终端用户在存取 Wi-Fi 服务时的最佳实务 —

设置

- 将默认的互联网连接设定为手动模式，而不是自动模式。
- 关闭点对点/临时模式联网。
- 启用客户端装置电源接通时的登入，以便访问该装置时要求密码。
- 安装并启用个人防火墙、防病毒软件和防间谍软件。

使用

- 不要让客户端装置无人看管。
- 未使用时关闭无线连接。
- 验证强制网络门户的证书，以确保它不是一个假的门户。
- 不要连接到不认识的 Wi-Fi 网络。
- 当有可疑活动时，把 Wi-Fi 网络连接断开。

维护

- 当客户端装置的应用程序和驱动程序有安全修补程序时就应采用。
- 定期备份数据。
- 在弃置之前，删除客户端装置上的所有数据和敏感配置信息，如 SSID 或加密密钥。

5.3 通过 Wi-Fi 网络进行远程访问

若数据透过 Wi-Fi 传递但未获保护便容易受到攻击。在无线装置之间传递的敏感信息如未加密（或使用的加密技术较弱），就可能会被截取和披露。因此，传送敏感信息时须采取安全措施。

对于经无线通信访问敏感信息时，应考虑将所有无线访问视为不可信任的连接。因此，以无线通信访问内部系统时，只能授予透过指定的通讯网关（例如虚拟专用网络网关），并且有妥善的认证、加密和实施了用户级别的访问控制和记录。

必须推行足够的认证和加密措施，来进行远程及经 Wi-Fi 至内部网络的访问。当连接到政府内部网络时，决策局 / 部门必须采用安全的渠道（例如虚拟专用网络、通过保密超文本传输规约的虚拟专用网络），并通过双重认证。以下是一些建议措施：

- 更新 Wi-Fi 联机端点（例如流动装置）上抗恶意软件软件的定义至最新版本。
- 安装最新的安全修补程序。
- 开启主机级的防火墙或入侵防御系统。
- 开启端点装置上储存加密的功能。
- 在虚拟专用网络客户端访问的列表上注册端点装置。
- 虚拟专用网络帐户采用严谨密码。
- 开启使用令牌或一次性密码的双重认证。
- 启用闲置超时（例如 10 分钟）功能以中断虚拟专用网络连接。
- 为所有连接 Wi-Fi 的虚拟专用网络，开启纪录功能。
- 如果媒体访问控制地址过滤功能已启用，则注册端点的媒体访问控制地址。

6. 新兴技术

6.1 5G 简介

5G 是指第五代的流动通讯技术，它是由国际电信联盟为发展新一代流动科技而制定的。5G 的流动技术功能超越了 4G。5G 流动技术的最高数据传输速度可达到每秒 20 兆数元，然而用户所体验的数据速率可能因流动装置所处的环境而有所不同。由于 5G 网络是建立在现有电讯网络之上的，在可预见的将来，预期 5G 的网络基础设施仍会继续用于提供 3G/4G 服务。

5G 的新容量和特性

物联网应用程序的促成

5G 网络的下载和上传速度显着提高。5G 网络的延迟 [1]也减少了。5G 还使大量机器之间的通讯能够进行，它允许更多的装置，特别是物联网装置，在一个小范围内连接到网络。

以软件为基础和虚拟化技术

5G 是透过网络功能虚拟化、软件定义网络和网络切片，在网络管理功能上采用新的软件程序 [2]和虚拟化技术 [3]。这些技术使 5G 能够支持共存，以及隔离不同需要类型的 5G 网络服务的应用程序，但这些应用程序能同时共享相同的基础架构。例如，流动宽带服务需要更高的数据传输速度，而智能汽车应用需要快速响应（低延迟）与传感器之间的数据通讯。

6.2 5G 流动网络服务的威胁与网络漏洞

5G 流动网络服务及其底层基础设施是由公共通讯网络营运商提供。与其他通讯网络（如 4G、Wi-Fi 或电话线）一样，5G 网络视为不可信任的通讯网络。通过任何公共通讯网络传递信息都可能会面临安全风险，因为恶意攻击者可能会利用通讯网络的漏洞获取保密数据，甚至闯入政府网络。公共通讯网络的威胁同样适用于 5G。此外，以下将详细阐述 5G 特有的一些威胁。

[1] 延迟是指从基站发射数据到目标装置(例如流动电话)接收数据之间的时间间隔。

[2] 软件定义网络和网络功能虚拟化的部署是透过允许对传统网络架构进行分区，从而提供更大的网络灵活性。

[3] 通过切片方式，公共网络营运商经基础设施为客户提供专用虚拟网络。网络切片的用户体验与实体上独立的网络是相同。

新增 5G 应用程序与网络技术的漏洞

由于 5G 网络提供更阔的带宽和更高的数据传输速度，它促进了能利用这些先进科技优势的创新应用程序，得到广泛增长。随着新应用程序的到来，但也带来一些安全风险。此外，5G 架构涉及各种功能层，并且通过基于软件和虚拟化技术实现。但是，使用这些新软件技术也意味着带来网络操作中的安全漏洞。如果决策局 / 部门的网络未妥善连接和保护，5G 基础架构软件的新安全漏洞就可能会影响决策局 / 部门。

5G 装置的威胁层面增加

5G 网络有能力支持更多的网络联机，从而允许大量类型的装置，尤其是物联网装置同时地相互连接。由于在短时间内推出市场和成本考虑，有些连接上网络的装置可能只达到较差的安全标准和功能，这能导致威胁层面扩大。如果某一个已连接上网络的装置存在漏洞，恶意攻击者可能会入侵并且控制该装置。再者，攻击者可以危及网络上其他的装置，并执行对整个网络的攻击。

具有 5G 连接的装置的配置错误

随着采用 5G 的流动装置或物联网装置日益增多，这些装置可能内置 5G 连接功能。由于 5G/物联网技术可以方便地实现动态连接，用户应注意装置更容易受到各种潜在风险的影响。例如，用户可能会将物联网装置连接到政府网络，并无意中对外披露敏感数据。此外，攻击者可以利用 5G 功能来进行其他攻击，如恶意软件程序传播，分布式拒绝服务攻击，仿冒诈骗和垃圾邮件攻击等。

流动装置，例如手提电话、平板计算机和笔记本电脑，一般透过通讯网络（包括 5G）连接到互联网。如果没有适当管理安全风险，保护措施不够和未能有效实施，就会增加机会令到数据、流动装置和相关通讯网络容易遭到未经授权的接达、修改、丢失、被盗或泄露，甚至流动装置也很有可能成为发起攻击网络的一部分。

5G 基站的风险因素

由于 5G 基站的运作是使用高频率讯号，所以 5G 基站的密度会比现时蜂窝式电讯网络为高。因此，流动网络营运商可能要求将 5G 基站和天线单元安装到政府处所，以提供更好的 5G 网络服务。当这些非政府拥有的设备在政府处所内未得到妥善管理，而这些流动网络营运商的人员或承包商也不是由政府直接管理，这可能会给政府带来安全风险。

6.3 使用 5G 流动网络服务的安全注意事项

公共 5G 网络的部署不应与其他传统网络（如 4G、3G 和固网电讯）有重大区别，并应假定所有公共或流动网络都不可信任。通过公共或流动网络进行的任何政府通讯，都应根据保密资料分类受到额外安全措施的保护，例如加密、身份认证、接达控制等。此外，在采用新技术后，所有相关的持份者应关注新技术可能带来的信息安全威胁，并及时采取有效措施，包括采用最新标准或安装修补程序。

新的 5G 应用程序与网络技术

5G 网络

就将公共网络连接到部门网络的安全考虑，应参考《互联网网关安全实务指南》。例如，决策局 / 部门应要求系统集成商或流动网络营运商提供安全控制，包括但不限于接达内部网络时安装安全网关或非军事区；传输数据时加密；监察系统和网络，防止任何恶意攻击，如分布式拒绝服务攻击和中间人攻击。决策局 / 部门还应启用安全监察和管理解决方案，以便更好地监控网络和任何攻击。

就新的 5G 网络虚拟化技术，依靠这些新网络技术的应用意味着网络的运作有可能存在漏洞。尽管这些新技术的许多安全责任都是由流动网络营运商或虚拟化平台拥有者承担，但决策局 / 部门应注意这些易受攻击点所引致的漏洞，并要求系统集成商或服务提供商在涉及 5G 应用程序时提供安全控制。决策局 / 部门应通过订阅安全新闻、警报、报告和其他信息安全出版刊物，清楚地了解此类有关 5G 连接而出现新的安全威胁和相关风险，以便决策局 / 部门能够尽早收到警报并针对此类威胁实施适当措施。

下面重点介绍 5G 网络的部署和管理相关的一些注意事项：

- 如果没有预计连接 5G 网络，应停用网络设备中不必要的内置 5G 功能。
- 制定在业务中采用 5G 服务的营运计划，包括但不限于评估 5G 应用和网络技术的成熟度、资产管理的考虑、接达控制、实体安全、操作安全、通讯安全、加密控制、与外部网络活动的记录以及外包、应用程序开发、业务连续性、事件管理和法规遵循性方面的考虑，以及决策局局长 / 部门首长的批准。
- 将连接到 5G 服务的网络分段与其他网络分段隔离。如果网络分段上的一个经 5G 连接的主机受到损害，这样就会将攻击层面减少。
- 可以将敏感和内部子网络与一般网络分离，以增强动态网络连接下的安全管理。
- 考虑聘请在 5G 网络方面具有专业知识的独立审计师，来审查和检查连接到 5G 网络的配置和实现。

5G 应用

5G 促进创新应用的发展，特别是物联网和流动应用。若在设计层面时已考虑安全要求，就能识别应用程序系统的潜在风险，并在项目的早期阶段进行适当的补救。建议各决策局 / 部门参考《流动安全实务指南》的第 5 节「流动应用程序开发安全」，该章节为开发用于业务的流动应用程序，提供指导说明；以及《物联网安全实务指南》，该指南重点介绍采用物联网以及各种相关安全领域时，常见的安全考虑和良好作业模式。对于部署使用 5G 连接的应用程序，应遵循在政府安全文件内就一般应用程序所订明的安全要求。以下列出数项要点供各决策局 / 部门考虑：

- 留意在安全方面的技术发展，并研究和评估安全机制和功能，以选取能符合安全要求的应用。
- 只采用必要和安全的功能。不启用不需要的功能，尤其是物联网装置。
- 避免收集和储存超过要求所需的敏感数据。
- 为保护敏感数据，确保数据在不同端点和传输过程中受加密保护。
- 启用认证和授权，以确保服务的使用者和提供服务者也是获授权的。

5G 装置

事实上适用于流动装置的一般安全实务、措施和控制，亦适用及有效地保护 5G 装置。建议决策局 / 部门参考《流动安全实务指南》第 4 节「流动装置安全」，该章节提供在业务中使用和采纳流动装置的安全指南。这些措施的例子包括平台和装置的独特识别，反检查机制，以防止装置的任何错误设定，接达装置的控制，储存和传输加密，以及加密密钥的有效性和其在失效前的续期。用户、应用程序开发人员或管理员分别负责保护其流动装置、数据资产和相关信息科技基础设施。

应定期提供培训，以增加用户对正确使用 5G 装置的认知，其方式与流动装置或物联网装置类似。以下是培训中一些建议的内容，以提高他们的意识。

- 5G/物联网技术促进动态连接，用户应注意其装置更容易受到各种潜在风险的影响（例如，将私人拥有的物联网装置连接到载有敏感政府数据的网络）。
- 用户应该知道，使用有安全漏洞以及安全设置较差的装置，会产生更大的网络攻击风险。
- 用户应部署有技术支持（如提供安全装置修补程序）的设备，以便保持该设备的安全。
- 用户应仔细检查装置的网络设定，并仅允许必要时连接到 5G 网络或设备。
- 用户不应在未获批准前将其 5G 装置直接连接到部门网络。

5G 基站

在频谱方面，5G 运作所需的频率高于 4G。由于高频讯号的穿透能力较低，所以设置 5G 基站和天线单元时，就需要较密集和近距离的，以令所提供的服务能有可接受的表现。如有需要将基站安装在政府处所内，应考虑采取下列安全措施：

- 在安装前，应明确界定政府和流动网络营运商的拥有权、角色和责任。流动网络营运商会为处理这些设备而提供相关的项目和服务。因此应就管理该些项目和服务，制定适当的安全程序。
- 对于启用 5G 的网络设备，应建立适当的实体接达控制，并且应指定工作人员来监察。
- 应制定适当的实体环境的安全程序，以控制和记录以下工作：安装、日常维护、更改配置和所有由工作人员为 5G 网络组件所进行的检查。工作人员的例子有外部顾问、承建商和临时工作人员。
- 向流动网络营运商阐明营运商的高级技术人员（如特许工程师）已批准和验证将会安装在 5G 基站的更新/修补程序。
- 5G 基站或相关设备并不是信息通讯科技基础设施中常见的网络设备。若果有不确定的情况，在安装前请先向电讯工程师，就其专业领域咨询安全建议。

事故处理

应检讨安全事故处理程序及进行必要的修改，以处理各种可疑活动的情况，例如 5G 网络因漏洞而受到损害和基站遭到破坏。此外，记录应受到完全控制，并得到充分的保护。如果发生了安全事故，不论来自外部或内部攻击的，系统记录和使用记录对于调查是关键的。

*** 完 ***