数字政策办公室

信息安全

物联网安全

实务指南

第 1.2 版

2024 年 7 月

©中华人民共和国
香港特别行政区政府

中华人民共和国香港特别行政区政府保留本文件内容的所有权，未经中华人民共和国香港特别行政区政府明确批准，不得翻印文件的全部或部分内容。

版权公告

© 2024 中华人民共和国香港特别行政区政府

除非另有注明，本出版物所载资料的版权属中华人民共和国香港特别行政区政府所有。在符合下列条件的情况下，这些资料一般可以任何格式或媒介复制及分发：

(a) 有关资料没有特别注明属不可复制及分发之列，因此没有被禁止复制及分发；
(b) 复制并非为制造备份作售卖用途；
(c) 必须准确地复制资料，而且不得在可能误导他人的情况下使用资料；以及
(d) 复制版本必须附上「经中华人民共和国香港特别行政区政府批准复制／分发。中华人民共和国香港特别行政区政府保留一切权利」的字眼。

如须复制资料作上述核准用途以外的用途，请联络数字政策办公室寻求准许。

修改记录				
修改次数	修改详情	经修改页数	版本编号	日期
1	更新物联网装置的定义一节、资产管理一节以及图4.1、7.1和7.2	3-1，4-2，5-2，7-1，7-2，	1.1	2021年6月
2	将「政府资讯科技总监办公室」更改为「数字政策办公室」		1.2	2024年7月

目录

1. 简介

1.1 目的

本文件旨在协助各局及部门采用物联网技术，并提供指南给多元的受众，例如管理人员、信息技术管理员、系统拥有者和信息安全持份者，因他们负责评估在使用物联网装置储存、处理或传递政府的信息时，对政府信息系统安全造成的影响。

本文件重点介绍采用物联网时常见的安全考虑因素和良好作业模式，以加强对物联网安全的基本理解。

由于每种物联网装置应用都有其特点和需要，建议决策局 / 部门采取风险为本的方法，实施适当的安全措施，以保护数据资产。

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

1.3 定义及惯用词

本文件将会采用《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	
物联网装置	具有网络连接和运算功能的装置，通过感应或致动的方式自动与实体环境互动。

1.4 联络方法

本文件由数字政策办公室编制及备存。如有任何意见或建议，请寄往：

电邮： it_security@digitalpolicy.gov.hk

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

CCMP 电邮： IT Security Team/DPO

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，以保护数据资产的机密性、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，以及确保数据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功能领域：

- 安全管理框架和组织；
- 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。

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。

各决策局 / 部门须定期和必要时对信息系统和生产应用进行安全风险评估，以确定与漏洞相关的风险和后果，并为制定具有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、应变和复原」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；
- 应变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变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／部门可以利用威胁情报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. 物联网概述

3.1 物联网装置的定义

市场上所提供的物联网装置种类繁多，例如传感器、执行器等。 由于物联网技术的不断发展，物联网装置没有一个全球都普遍接受的单一的定义。在本指南中，物联网装置是指有网络连接和运算功能的装置，这些装置通过感应或致动方式自动地与实体环境互动。对于可以配置为与互联网或企业网络有网络连接的装置，无论它们是否连接到此类网络，都被视为物联网装置。以下是物联网装置的一些例子：

- 具有网络连接的传感器（例如空气质量、温度）;
- 具有网络连接的智能计量表（例如电、水）;
- 具有网络连接的智能设备（例如雪柜、电视、电灯）。

现今，很多信息技术设备都内置了物联网功能。本指南，将集中讨论那些在政府会用作一般应用的物联网装置。 对于有专门工业用途的物联网装置，例如智能电机或智能泵等致动器，它们一般会集成于操作技术内，以监察和控制工业设备、过程和日常操作。操作技术不在本文件涵盖的范围。传统的信息技术设备，如流动装置、网络设备、工作站和服务器不是本文件重点关注的装置，因为《基准信息技术安全政策》和《信息技术安全指南》以及相关的实务指南已提及如何在这些设备推行安全措施。然而，如果传统的信息技术设备被用作为物联网装置，例如内置摄录机的计算机被用作为监察系统，或流动装置的全球定位系统/蓝牙功能被用作为位置追踪器，则本文件对物联网装置的安全措施亦同样适用。此外，由于很多信息技术设备是建立于不同的组件上，因此需要尽职覆检审查组件的功能，并判断这些组件的安全控制措施是否已被妥善实施或者在不需要的情况下其相关物联网功能已被适当地停止使用。

由于局 / 部门可能已部署了一些物联网装置，局 / 部门可从以下角度对其物联网装置进行安全评估：

- 物联网装置所处理和储存的数据；
- 物联网装置所连接的网络与其他相连装置；和
- 物联网装置自身的保护。

在评估办公环境中使用物联网装置的安全时，应考虑以下因素：

- 物联网装置是否会处理或撷取敏感数据；
- 物联网装置是否会连接到部门网络或决策局／部门拥有的设备；
- 在办公环境中有否安装物联网装置；
- 物联网装置是否会与互联网或者其他外部设备连接以交换敏感数据；和
- 如果没有妥善管理，物联网装置是否对安全有影响而影响政府形象。

决策局／部门应评估物联网装置所构成的风险，以及一旦发生安全事故，对政府运作和形象的影响。决策局／部门须界定和实施适当的措施，以确保物联网装置和数据的信息安全与数据的保密分类相称。

4. 物联网安全介绍

4.1 物联网安全的挑战

在物联网技术相关的系统中，智能装置的数据保护面临新的挑战。与传统信息技术设备相比，物联网装置的攻击面更广、更多样化。也就是说，物联网装置的安全威胁可能来自很多方面：设备、网络、储存以及与物联网装置相关的应用/服务，如云端、网络和流动服务。所有这些都可能受到网络攻击。

简单而言，物联网所面临的主要威胁有以下几方面：

装置

装置通常是发动攻击的主要目标。装置的漏洞可来自内存、固件、实体界面、网页和网络服务。攻击者也可以利用不安全的默认设定、过时的组件和不安全的更新机制所产生的漏洞来攻击装置。缺乏设备管理和实体加固也是装置的常见威胁。以下是装置常见的威胁：

- 缺乏设备管理
  物联网装置可能缺乏妥善管理，包括资产管理、修补程序管理、安全退役和系统监控等。这种情况通常发生在低成本设计的传感器中。

- 不安全的默认设定
  由于一些物联网装置体积非常小和应用数量大，管理员可能通过使用装置的默认设置来简化操作。但是，默认设定一般容易受到外部攻击，很容易被第三方利用，导致未经授权的系统访问。

- 缺乏实体强化
  对于物联网装置，特别是安装在政府场地以外的物联网装置，并不足够或有效落实端口限制或实体访问限制等强化措施。这使得攻击者可以入侵实体设备以获得控制权。

- 使用不安全或不支持的组件

  由于物联网装置可能会应用在广泛的范畴，而很多设备都是以低成本为前提下设计的，因此，无论是硬件还是软件，其组件都可能支持不足或存有不安全的设定。这令装置很容易被入侵。

- 容易被修改的装置

  由于装置制造商可能未有采用设计层面的安全方式，物联网装置可能会无意中留下后门。

- 容易遭破壞的装置

  由于物联网装置可能会安装在公共区域，若装置被盗或被破坏，可能会损坏装置或相关系统并导致系统未能正常运作。

数据

物联网装置可能需要收集数据，并与对应装置交换这些数据。用户可能会低估收集的数据量，并收集不必要的数据。数据外泄是物联网装置常见的威胁之一，原因如下：

- 弱密码或不可更改的密码

  有些物联网装置可能不支持严谨的密码设置，甚至不允许更改密码。此外，如果用户缺乏安全认知，他们可能会选择一些容易被暴力攻击破解的密码。攻击者就可能很容易进入这类系统。

- 缺乏安全更新机制

  一些物联网装置制造商可能缺乏资源为其设备（包括固件和软件模块）提供安全更新，或可能无法及时提供安全更新。此外，物联网装置可能由没有安全更新的第三方软件/代码组成。

- 不安全的数据储存

  物联网装置或会储存数据，但可能没有安全措施或没有加密功能来保护敏感数据。因此可能不足以防止未经授权的访问。

- 信息外泄

  由于物联网装置可能安装在限制区内，因此可能存在向未经授权方泄漏敏感环境数据的风险。此外，如果物联网装置与互联网互连，攻击者可能会通过恶意软件感染、未经授权的访问或中间人攻击等手段来获取资料。

网络

攻击者可以透过信道攻击物联网组件。此外，物联网系统中使用的通讯规约可能存在会影响物联网系统的安全漏洞。以下是一些常见的威胁：

- 不安全的网络服务

  装置本身运行不安全的网络服务，特别是暴露在互联网上的网络服务，可能会危害物联网的安全或允许未经授权的远程控制。

- 不安全的数据传输

  一些物联网装置由于其效能有限，可能无法提供足够的加密强度或敏感数据的访问控制。

- 通过网络收集资料作恶意用途

  虽然互联功能是物联网装置的优势之一，但这也带来了攻击面。中间人或者会话劫持等攻击可能让攻击者获得敏感数据。

- 恶意攻击

  与上述情况一样，恶意攻击者可能会通过网络获取物联网装置的访问权限，并在装置上安装恶意软件。这将导致分布式拒绝服务攻击，甚至将物联网装置变成僵尸网络。

私隐

物联网装置可能安装在办公环境或公共区域。管理员可能没有意识到物联网装置可能会收集过多的个人资料。如果不妥善管理，攻击者可能会收集这些个人资料危及私隐。

应用系统

物联网装置的云端服务、流动应用程序、网上应用系统和相关软件的漏洞都可能导致系统受破坏。以下是一些常见的威胁：

- 不安全的应用程序界面
  物联网生态系统中不安全的网址、后端应用程序界面、云端或流动界面可能会让物联网装置受破坏。常见的问题包括缺乏认证/授权，缺乏或弱加密，或缺乏输入和输出认证。

- 软件漏洞
  软件漏洞和配置错误是物联网装置的常见威胁。这些漏洞通常被攻击者使用的攻击工具入侵，例如，网上应用系统被利用作窃取用户凭证或安装恶意的固件更新。

4.2 物联网部署中的组件

下图说明建基于物联网的部署中常见的组件。它由物联网装置、通讯、后台服务器和储存设备以及应用系统组成。这有助于我们识别威胁和推行相应的安全措施。部署模式将在第 7 节--物联网装置的案例中描述。取决于部署的可扩展性，有些组件是非必要的。例如，并非所有的物联网部署都需要应用服务器或数据库。

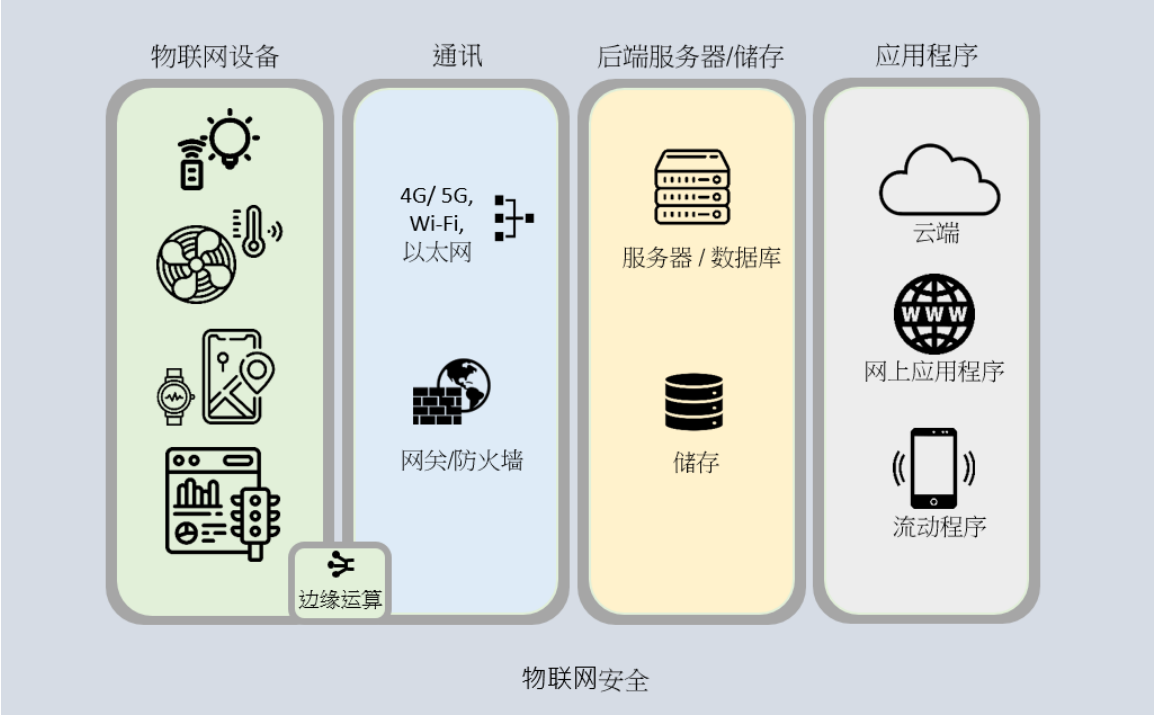

图 4.1 建基于物联网的部署中的常见组件

物联网装置

装置层又称端点，是物联网技术系统的实体界面。物联网装置可以有各种操作系统、中央处理器类型、内存等。这些装置可能位于办公环境或公共区域，有些可能位于偏远地区，这便需要远程控制来保持正常操作。

边缘运算是保护物联网安全基础架构的重要组成部分。由于物联网装置通常在提供安全功能方面有所局限，因此边缘运算可充当抵御潜在攻击的角色。在这种情况下，边缘装置就是掌控那些物联网装置的看门人。

通讯

连接是物联网装置的关键。物联网装置可以相互连接，也可以直接连接到互联网。网络基础设施包括传输数据数据、语音、图像和视频影片的局域网、广域网络或流动/无线连接（4G/5G、Wi-Fi 等）。

一些连接的例子包括：

- 4G/5G
- LTE
- Wi-Fi
- 以太网络
- 近距离无线通信
- 低功耗蓝牙
- 射频识别

在技术方面，物联网装置支持多种通讯识别，如互联网规约地址、媒体访问控制地址、电话号码等，其中互联网规约地址是比较常用的。互联网规约地址可以通过无线连接(Wi-Fi、4G、5G、LTE 等)以及有线(以太网等)通讯方式进行通讯。

后端服务器和储存设备

一些物联网系统需要应用后端服务器或数据库。在一些大规模的物联网应用中，需要后端服务器或数据库来支持计算功能或数据储存。后端服务器或数据库可以由数据中心或通过云端平台来提供。

应用系统

物联网可以与云端、网络或流动应用程序相结合。在某些情况下，云端平台负责对收集的数据进行有效处理和管理。它还托管应用系统，以提供服务和管理整个物联网架构。

5. 物联网的安全考虑因素和控制措施

信息安全是任何数据和通讯技术系统的主要关注点，物联网系统也不例外。因此，信息安全管理原则适用于物联网安全。然而，物联网系统为信息安全带来特殊的挑战，因为物联网装置可以高度分散，亦可涉及大量不同的单位。使用物联网装置须全面检视端对端安全，采取风险为本的方法为物联网装置识别安全风险、订定风险的缓急次序和应对有关风险，包括但不限于资产管理、认证和授权、通讯网络、软件和应用系统、后端基础设施、装置安全、实体安全等。由于物联网装置和流动装置的某些相似性，例如连接性，流动性和体积小，因此，在政府安全文件列出的流动装置安全要求和原则应该同样应用于物联网装置。

以下章节将介绍物联网特定安全领域的挑战和建议，重点介绍以下安全领域：

- 信息技术安全政策
- 资产管理
- 访问控制
- 加密方法
- 实体及环境安全
- 操作安全
- 通讯安全
- 系统购置、发展及维护
- 遵行要求

5.1 信息技术安全政策

决策局 / 部门须订定并确实执行其信息技术安全政策，根据业务和安全要求，就保护信息系统和资产的工作提供管理方向和支持。当物联网装置部署或引入信息系统时，决策局 / 部门须覆检其部门的安全政策，以配合物联网装置的安全要求。此外，须设有正式的使用政策及程序，并采取适当的安全措施以防范针对物联网装置的风险。以下是一些对决策局 / 部门的建议：

- 覆检信息技术安全政策

  决策局／部门信息技术安全政策应根据业务需要和安全要求，在必要时确实执行、定期覆检和更新，以保护信息系统和资产。特别是在信息技术环境中引入物联网时(如物联网装置、后端服务器/储存等)，更新各安全领域，引入新的或强化的安全要求，如访问控制、实体安全、通讯安全、资产管理等。

- 制定正式的物联网装置使用政策及程序

  须制订正式的使用政策及程序，并采取适当的安全措施，以防范针对物联网装置的风险。使用政策及程序应包括但不限于以下要求：a.)实体保护，防范物联网装置和数据被盗或遗失；b.)访问控制，防范未经授权操纵设备和修改数据；c.)通讯保护，防范拦截数据或嗅探攻击；d.)加密要求，提出基本和有效保护的最低标准；e.)日志管理，跟踪异常活动并识别其责任；f.) 安全漏洞管理，防止恶意软件针对已知的安全漏洞，发起的恶意代码和病毒的攻击。

  使用政策及程序还应包括有关保护物联网装置之间连接以及连接到政府网络的物联网装置的规则和建议，保护物联网端点免受安全威胁，例如成为攻击者操纵的僵尸网络的一部分、恶意软件传播、分布式拒绝服务攻击等。

5.2 资产管理

决策局／部门应确保和维持物联网装置和数据受到适当的保护。决策局／部门应备存和覆检存有敏感数据或连接内部/外部网络的物联网装置列表，并作出适当安排以确保按照政府的安全要求处理数据，以期减少对物联网装置、政府数据以及对信息系统可能产生的影响的安全风险。

- 妥善记录和管理物联网装置

  决策局／部门应从资产中识别出物联网装置，并在列表中标明、备存和定期覆检列表，以确保列表是最新和准确的。应拟订物联网装置列表，提供装置资产数据，包括型号、独有标识符、固件、序号、拥有权等，并订明会否处理、储存或传送任何敏感数据。决策局／部门应考虑使用计算机系统管理资产记录，以有效促进资产管理和信息技术安全。

- 对物联网装置处理的数据进行评估和分类

  应根据数据的敏感程度对其进行分类。在处理、储存或传输数据过程中，应根据其类别予以相对应地保护。应明确界定和记录数据所有权和处理程序。

- 当不再需要时，删除储存在物联网装置中的敏感数据

  为防止数据外泄、遗失或未经授权的访问，在处理或重用所有敏感数据前，须参照 G3 第 10.3(b)节的规定，以彻底清除或销毁敏感数据。

5.3 访问控制

决策局 / 部门须界定和实施适当的安全措施，以确保物联网装置和数据的安全与数据类别相称。这些措施应能有效防止物联网装置和数据在未经授权的情况下被入侵和操控。应考虑以下访问和管理物联网装置的常用安全措施、控制和作业模式，但并非详尽无遗：

- 选择设计上提供了安全功能（如识别、认证和授权）的物联网装置。
- 限制和控制对物联网装置和数据的访问，根据最小权限和职务分工的原则，向用户授予访问权限。当不再需要这些权限时，撤销这些权限。
- 确保充分的认证，使用严谨的密码，定期更换密码。
- 启用双重认证（如有）。
- 更改默认配置和设置，如用户名称和密码。
- 启用帐户锁定机制，防止过多的无效登入尝试和暴力攻击。
- 停用或删除不必要的用户帐户（如访客、演示户口）。
- 只允许受信任的互联网规约地址或/和获授权的设备访问物联网装置或后台系统（如建基于云端的服务器）。
- 只允许经授权的人员实际访问物联网装置。
- 在传递和储存过程中保护使用者凭证（如加密）。
- 在可行的情况下，禁用不必要的服务或逻辑端口（如远程登入）和实体端口（如通用串行总线）。
- 在传输层安全和其他规约协商过程中，尽可能使用证书进行设备认证和保密，并在集成其他访问控制机制时，支持各种身份绑定。
- 确保支持公开密码匙基础建设的标准服务，如撤销检查、信任管理、程序注册和登记，以及事故复原。

5.4 加密方法

在物联网环境中，加密技术是不可或缺的，如果实施得宜，加密技术可以为认证性、机密性、完整性和不可否定性提供安全保证。加密技术被广泛用于保护储存或传输数据的机密性。如果敏感数据需要存储在物联网装置中，必须进行加密。数字签名或讯息认证码则用以核实储存或传送敏感或保密数据的真确性或完整性。决策局 / 部门应利用加密技术，以保护物联网环境中的数据、系统、设备及它们之间的通讯。应考虑以下常见的安全措施、控制和做法，但并非详尽无遗：

- 选择在设计上已支持加密功能（如加密、公开密码匙基础建设等）的物联网装置。
- 使用加密规约来加密对等装置、智能流动装置应用程序、云端服务和应用程序界面之间的任何通讯。
- 加密在不受信任的网络上储存和传输中的敏感数据。
- 使用标准的、可信任的、加密算法以及严谨的密码匙长度（如 AES - 256）进行数据数据加密。
- 正确管理和使用加密密码匙；避免在多个端点使用同一加密密码匙。

5.5 实体和环境安全

对于物联网装置，须根据物联网装置储存、处理和传递的信息的保密分类实施安全控制，防止装置遗失、被盗和损坏。

物联网装置和相关网络设备应得到妥善管理、选择适当的地址和保护，以降低不利环境和未经授权的实体访问的风险。攻击者可能会利用物联网装置的实体漏洞对在同一网络上的其他端点进行破坏。

对于使用中的物联网装置，决策局 / 部门应避免在这些物联网装置收集和储存保密数据。如因为业务需要处理保密数据，应将数据加密并传递至安全控制措施符合相关政府安全要求的安全后端储存。如因业务需要而无可避免地将保密数据储存在没有人员看管的物联网装置，则在侦测到并确认实体保护遭到尝试入侵时，须实施适当的实体保护和辅助措施（如删除数据、中断网络连接）。

应考虑以下与物联网装置实体安全相关的常见安全措施、控制措施和作业模式，但并非详尽无遗：

- 为物联网装置和相关设备提供足够的实体保护和检测措施和控制（如钥匙锁、入侵检测系统、警报或监控系统等），当特别安装在公共区域或无人看管的位置时，可以检测到实体窜改。
- 正确选址和妥善安装物联网装置，并采取足够的实体措施和控制措施，可以有效地保护物联网装置免受遗失、被盗、服务中断、数据拦截或被实体攻击或破坏。
- 保护电力和电讯导线不被拦截、干扰或损坏。
- 确保物联网装置和设备不容易被拆解。
- 限制通过实体界面或端口直接访问物联网装置。
- 启用任何实体访问的详细日志，如通用串行总线端口。
- 禁用所有不必要的实体界面和端口，包括那些用于调试的界面和端口。

5.6 操作安全

决策局 / 部门须确保物联网组件及其环境的操作安全。下列措施是必要和有效的安全措施，包括防范恶意软件、记录信息技术流程和事件、监察可疑活动、防止技术性安全漏洞被利用等。以下为一些与物联网操作有关的常见安全措施、控制措施和作业模式。这些措施和做法都应予以考虑，但并非详尽无遗：

操作程序和责任

- 订立和备存物联网装置、相关系统和网络的操作程序。该程序是逐步的操作指令（如物联网装置和系统的安装和配置、数据的演算和处理等）。
- 应用最少功能原则来管理物联网装置、相关系统和网络。删除和限制所有不必要的功能、服务或组件。

防范恶意软件

- 启用促使对所有物联网端点的反恶意软件保护，包括物联网装置、后端系统、流动装置等。
- 须定期更新恶意软件定义和侦测及修复保护引擎。

漏洞管理

- 及时在物联网端点上安装由产品供货商所提供最新的安全修补程序和更新固件，或实施其他补偿安全措施。
- 在应用物联网装置之前，认证完整性和真实性，并测试制造商提供的安全修补程序和固件。
- 界定并维持一份授权软件或应用程序的列表。
- 在使用开源软件或代码(如库、数据库和应用程序界面等)之前，核实和评估风险(如程序错误、安全性漏洞或后门)和影响。

云端数据和通讯安全

- 加密储存在云端中的数据以及云端与其他端点之间的通讯。
- 正确管理和保护加密密码匙的整个生命周期。当储存的数据被认为是敏感时，考虑使用硬件安全模块来保护加密密码匙操作。

记录和监察

- 根据其业务需要和保密类别，定义和覆检与物联网装置和相关信息系统活动记录相关的政策。
- 保存活动记录的时间应与其作为审计工具的时效相称。
- 保护活动记录，防止未经授权的访问和篡改。
- 定期检查活动记录的完整性。
- 持续不断并实时监控物联网端点和相关网络通讯。这可以帮助及时检测和跟进异常或可疑活动。

物联网装置安全

- 当需要高安全级别的物联网装置，安全芯片是首选组件。这能强制执行安全启动，以防止未经授权的固件、引导加载器或引导映射更新。
- 使用包含安全功能的硬件，以加强对设备的保护和完整性。

5.7 通讯安全

由于物联网装置能够通过有线或无线连接与其他设备和系统进行通讯，因此应采取充分有效的安全措施和控制措施来应对相关的安全威胁和攻击。

对于连接到政府内部网络的物联网装置，如果没有采取适当的防御措施，就能成为一个安全漏洞点，如泄露保密资料、向政府内部网络传播恶意软件、或当被攻击者感染时，发起分布式拒绝服务攻击。

除非得到决策局 / 部门的适当批准，否则用户不得将已连接到政府内部网络的物联网装置连接到外部网络。

应考虑以下与物联网装置通讯安全相关的常见控制措施和作业模式，但并非详尽无遗：

- 网络应尽量简单和可靠（即把「安全」网络与其他网络的网络界面点减至最低）。
- 设立物联网装置及相关网络设备的网络图、逻辑位址和实体位址、配置等网络信息，以反映最新、全面的网络环境，以便进行有效的安全控制措施和事故应急。
- 通过实体或逻辑手段将网络划分为独立的网络域，当安全性漏洞发生时，将影响降到最低。
- 确保组件/层级（即物联网装置、网络设备、后端系统/储存和应用）之间的通讯安全。
- 限制和控制所有的网络通讯和连接（如通过防火墙规则、媒体访问控制地址过滤等），只允许获授权的出入通讯以及连接到适当的网络设备。
- 停用所有不必要和不安全的网络服务（如远程登入、档案传送规约等），并使用安全规约（如保密外壳、保密档案传送规约等）。
- 在有线和无线通信中启用加密功能。
- 在网络传输前，用标准的、可信的加密算法对数据进行加密。
- 在接達网络服务和装置到装置的连接时，确实执行严谨的认证。
- 对于装置与装置之间的连接，在初始配对过程中需要使用者互动，以避免意外配对给未经授权的远程方。在初始配对过程中，在提供正常服务之前，应将默认的无线密码从出厂默认值更改，或重新设置密码。

- 建立零信任网络1和/或安全访问服务边缘2的框架，以控制对物联网系统的授权和安全访问。
- 考虑实施入侵检测系统，以检测异常活动、虚假设备和潜在的信息安全事件，以及实施入侵防御系统通过阻止可疑通讯来防止恶意攻击。数据分析和深度数据报检测有助从物联网装置产生的数据中识别威胁和异常情况。

5.8 系统购置、发展及维护

现今的信息技术环境中，安全是不可或缺的。如果安全意识和措施不足，会严重影响信息技术基础设施、业务营运和声誉。对于物联网相关的应用、系统和装置，安全应该是整个系统开发生命周期中不可或缺的一部分。在系统开发生命周期的早期阶段就应该考虑安全问题，以便更好地管理安全风险和相关问题。设计层面的安全是实现这目标的一种方法。物联网安全应有自己的需求，并纳入系统需求中。应根据政府、法律和规管以及业务要求，正确和明确地定义这些要求，以确保系统、设备和数据的机密性、完整性和可用性。

政府信息技术安全政策及指南所载的安全规定适用于与物联网有关的系统和装置。决策局 / 部门应遵守《基准信息技术安全政策》和《信息技术安全指南》第 16 节 - 系统购置、发展及维护的规定。

此外，安全覆检应在设计时间进行，可以确保系统已分辨及纳入必要的安全要求，评估和处理相关的安全风险和影响，以有效促进系统发展生命周期的后续阶段。

对于物联网相关的应用程序、系统和设备，须进行安全风险评估和审计，对安全审计中发现的风险进行核实，确保生产前采取适当、充分的安全措施。

应考虑以下与购置和发展物联网应用相关的常见安全措施、控制和作业模式，但并非详尽无遗：

[1] 零信任网络所指的保安概念是指不会基于实体或网络位置（即局部区域网络或互联网）就给予用户、资产或服务的信任。 在授予访问权限之前必须严格执行授权和验证。评估访问请求后，仅根据用户身份和职务授予最小特权访问。在授予访问权限之前，必须严格执行授权和身份验证。 评估访问请求后仅根据用户身份和角色授予最小权限访问。

[2] 安全访问服务边缘是指结合了广域网络功能和网络保安功能的网络体系结构以提供服务，例如保安网页网关，云端访问保安代理，防火墙即服务和零信任网络访问。

- 根据安全政策和指南，以及部门的信息技术政策，界定和覆检安全要求，例如数据和系统访问控制(例如认证方法)、密码管理(例如加密算法、密码匙保护)、安全漏洞管理(例如固件的可用性、服务供货商／制造商提供的安全修补程序)、通讯规约(例如保密外壳、TLS、HTTPS)、备份策略。
- 识别持份者(如数据拥有人、系统拥有人)，确定并记录他们的角色和责任。
- 应实行更改控制。对系统配置或程序代码的更改应遵循规定的程序，以保持完整性和可靠性。
- 在规定的时间段(如在提供正式服务前，以及在进行大规模升级和变更前)对系统和应用程序进行安全风险评估。测试、覆检和执行适当的安全措施，并确保其有效性。

物联网相关系统和装置购置

- 应开展调查研究，评估适合并满足规定的安全要求的安全机制和功能。
- 选择已设计、内置或已实现实体和逻辑安全功能的物联网装置或系统，如访问控制（如身份认证）、漏洞管理（如固件、安全修补程序）、反恶意软件保护机制（如防火墙）、加密控制（如加密、可信平台模块），能有效加强对设备、系统和数据的保护。

应用系统设计和开发安全

- 考虑从收集/生成到弃置的整个资料生命周期的安全性。
- 确保并保持应用程序的完整性（如通过版本控制机制，分离开发、系统测试、验收测试和实际运行的环境）。
- 避免收集和储存不需要的敏感数据。
- 避免在物联网装置中收集和储存保密数据。
- 在所有设计文件中记录数据项、保密类别级别及其保护机制。
- 根据全球认可的安全标准（如 OWASP）检查网上应用系统和应用程序界面服务。
- 通过网上应用系统防火墙保护网上应用系统和应用程序界面服务。
- 认证网上应用系统和应用程序界面服务的数据输入。
- 在网上应用系统和应用程序界面服务中使用加密技术来保护传输中的数据。
- 在网上应用系统中认证身份，并启用会话超时的应用程序界面服务。
- 加密在流动应用程序与后台云端应用系统或物联网装置的通讯。

- 当储存的数据被认为是敏感数据时，加密数据并考虑双重认证。

5.9 遵行要求

决策局／部门须避免违反与安全要求相关的法律、法定、规管或合约责任。决策局／部门除了考虑本地的法律及法定外，亦应考虑其他国家或地区的相关法律或法令的适用性，特别是在个人资料及私隐方面。如有需要，建议决策局／部门寻求专业或法律意见。安全措施须根据相关安全要求推行及操作。

就物联网装置部署而言，决策局／部门可考虑采用现成的云端服务，以用于物联网后端系统/储存或应用。决策局／部门购置云端服务前，应仔细研究和了解云端服务的范围、内容、合约条款和条件、责任和限制、使用政策等。决策局／部门在选择解决方案时，应评估相应的安全措施和控制措施是否符合政府的安全要求，特别是处理保密/敏感的数据。此外，决策局／部门应注意云端服务的信息系统和储存的数据可能位于香港以外的地区，亦因此受海外法律所规管。

关于云端服务及相关安全考虑，请参考 ITG InfoStation 上的《云端安全实务指南》
https：//itginfo.ccgo.hksarg/content/itsecure/docs/Guidelines/DocRoadmap.shtml。

关于外包服务的安全性，请参考《基准信息技术安全政策》和《信息技术安全指南》第 17 节--外包信息系统的安全。

文件数据

决策局／部门须保存记录，以证明遵守安全要求的情况，并支持对有效执行相应安全措施的审计。安全风险评估和安全审计的报告或记录结果，可视为适当和可接受的证明。由于安全风险评估和安全审计是持续进行的程序，有关记录可作为参考，以便进行下一次评估或审计，以及采取进一步的跟进行动。

应检查遵守安全的条例和政策的情况，并将其明确纳入服务合同的规格和规约中。审计员为检查遵守要求而提供的审计报告，应确保对信息技术安全政策、资产管理、访问控制、密码学、实体安全、操作安全、通讯安全、系统发展和遵守情况，已有适当控制。

数据保护、个人资料和私隐

决策局／部门须在数据资产的整个生命周期内，从产生或收集、储存、处理、传输到销毁，对其进行保护。

决策局／部门须根据保密类别对数据进行评估、分类和保护。应明确定义和记录所有相关持分者的数据拥有权、角色和责任。物联网的采用通常是由业务需要带动的。因此，涉及物联网装置的信息技术系统拥有者有责任管理相关的安全事宜。参考《基准信息技术安全政策》 第 5.3.3 节 有关部门信息技术安全组织，信息技术系统的系统管理员可负责涉及物联网装置信息技术系统的日常管理、运作和配置，包括安全监察，以防范安全威胁。另外，决策局／部门在实施物联网之前，系统拥有人应该已经获得部门信息技术安全主任的批准。此外，如涉及物联网装置的信息技术系统将连接到部门网络，系统管理员可指定由负责监察决策局／部门网络整体安全的网络或局部区域网管理员负责监控物联网装置。

在处理保密数据方面，决策局／部门须遵守政府的安全规定（例如《实务守则》、《基准信息技术安全政策》、《信息技术安全指南》及部门的信息技术安全政策）。在处理个人资料方面，除政府的安全规定外，决策局／部门亦须遵守本地的法律规定(例如《个人资料(私隐)条例》)及海外的数据保障法令或规例(例如《一般数据保护规范》)(如适用)。

为了保护物联网运作或环境中的数据，决策局／部门应考虑采取全面的方法，根据其使用情况和业务环境，透过行政（例如部门的信息技术安全政策及程序）、逻辑（例如加密、访问控制）或／及实体（例如位于上锁的房间）的措施或控制，以及遵守政府的安全规定，保护数据免遭未经授权或有意图的逻辑及实体访问、遗失或盗用。

有关个人资料和私隐的法例或问题，请参考本文件第 6 节--个人资料保护的考虑。

安全覆检

物联网相关信息系统(如后端服务器/储存)或应用系统(如流动应用程序、网上应用系统)的安全风险评估和安全审计须按照政府的安全要求，每隔一段时间进行一次。

- 安全风险评估

  安全风险评估是一个识别、分析和评估安全风险的过程，并确定将风险降低到可接受水平的缓解措施。

  与传统信息系统和应用系统类似，与物联网相关的信息系统和生产应用系统至少须每两年进行一次风险评估，并须在提供正式服务前，以及在进行大规模升级和变更前。决策局／部门应确保妥善评估和处理在风险评估期间发现的物联网系统和应用系统的风险。

  对于处理敏感数据并安装在公共区域的物联网装置，须进行安全风险评估，评估信息系统和数据资产的安全风险，并须采取足够的安全控制措施，特别是实体安全措施，以保护数据。

  除信息系统及应用系统的安全评估外，其他安全范畴(例如物联网基础设施、物联网组件／层之间的连接等)也应采用安全评估，以覆检和评估潜在的安全风险。因此，决策局／部门应考虑善用安全评估来发现和处理其业务环境和运作中的安全问题。此外，为物联网组件进行安全评估的专业人士，应具备丰富的物联网运作及安全实务经验。

- 安全审计

  安全审计是认证过程或事件中遵守安全性原则或标准的程度，作为确定现有保护的整体状态和认证现有保护是否正确执行的依据。

  应由足够具备相关的物联网安全运作、管治及合规方面的知识、技能及经验的审计师定期进行安全评估。决策局／部门应确保其物联网组件受到妥善保护，并符合政府和部门的信息技术安全政策。

有关安全风险评估和审计的详情，请参阅 ITG InfoStation 上的《安全风险评估与审计实务指南》

https：//itginfo.ccgo.hksarg/itcontent/itsecure/docs/Guidelines/DocRoadmap.shtml。

6. 个人资料保护的考虑因素

物联网装置可能会收集、监察或分析与个人有关的各种数据。建议决策局／部门在系统设计时间采用「设计层面的私隐」，以避免过度收集个人资料。决策局／部门应清楚通知用户将会收集的个人资料的种类、收集的目的、个人资料的潜在受让人，以及为保护个人资料而采取的安全措施。

决策局／部门在处理个人资料时，须确保遵守《个人资料(私隐)条例》，特别是保障资料原则 4(个人资料的安全)。决策局／部门亦应留意其他经济体系的规管架构（例如欧盟公布的《一般数据保护规范》）可能造成的影响。防止个人资料外泄及滥用的考虑因素包括但不限于：

- 尽量减少收集个人资料。
- 对物联网装置采用「设计层面的私隐」。
- 实施适当的安全措施，如加密个人资料并将其传输到安全的后端储存，并执行严谨的密码以防止帐户被劫持。
- 对个人资料进行去身份识别或匿名化处理(如适用)。
- 当不再需要时，安全地销毁个人资料。

7. 物联网装置的应用案例

物联网装置可以放置在广阔而多样化的领域。物联网装置收集和处理数据的位置是其安全性的关键，因为在办公环境和在公共区域的安全控制措施是完全不同的，特别是在实体安全控制措施这范畴。 另外一个关键是涉及数据的保密分类。在购置前，决策局 / 部门应研究潜在供货商的物联网装置所具备的安全功能，以期得到最高安全水平的物联网装置。物联网装置应避免在设备本身储存数据，尤其是敏感数据。应该有适当的安全保护数据收集和传输到后端储存。为保护物联网装置中收集/处理/储存的资料，应遵循相关政府安全规例、政策和指南，这些规例、政策和准则对保护保密资料有具体要求。

本章节将讨论以下两个部署物联网装置的例子，以提供一些有关物联网安全的一般指南，供决策局 / 部门在不同的情况下作参考。

I. 在公共场所安装的物联网装置（案例一）
II. 办公环境中安装的物联网装置（案例二）

7.1 宏观物联网参考模型

下图展示了一个宏观的物联网参考模型，其中包括上述两个部署案例。下文各节将对每个部署案例进行详细说明。

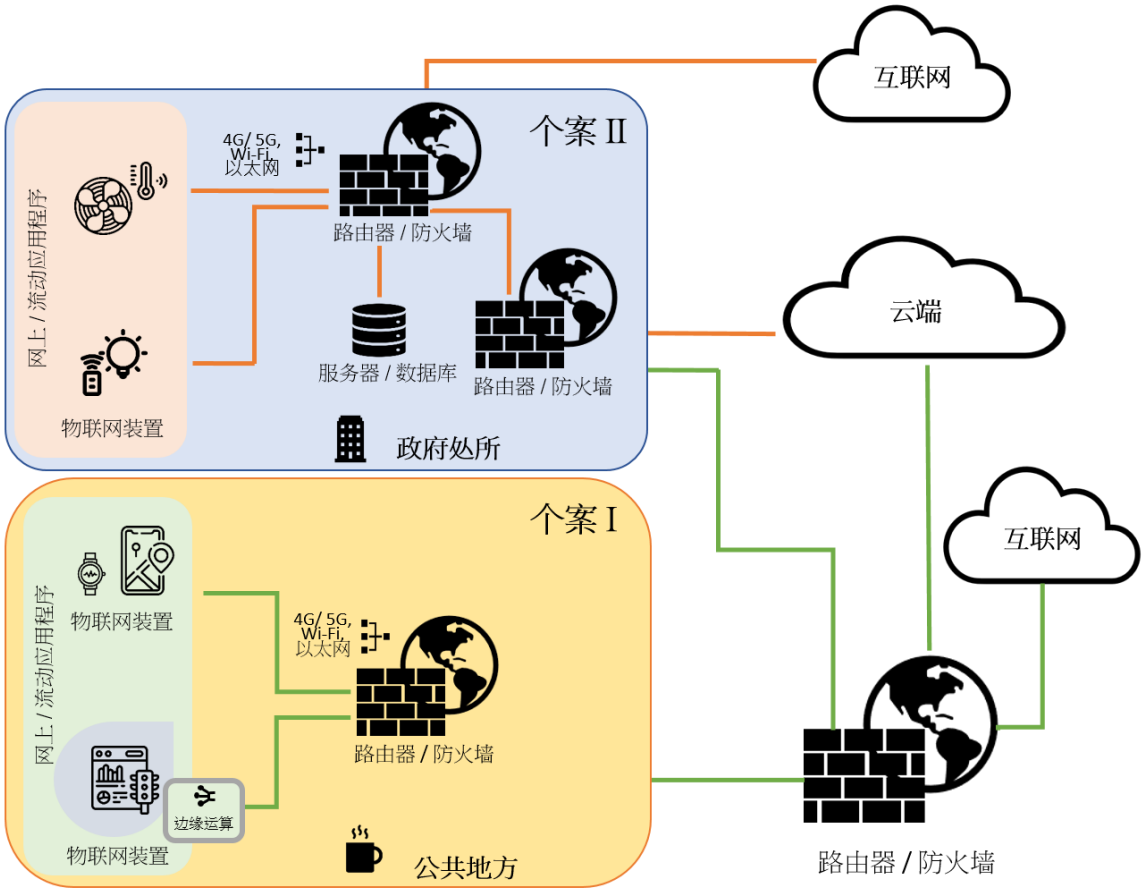

图 7.1 宏观物联网参考模型

7.2 公共区域安装的物联网装置（案例一）

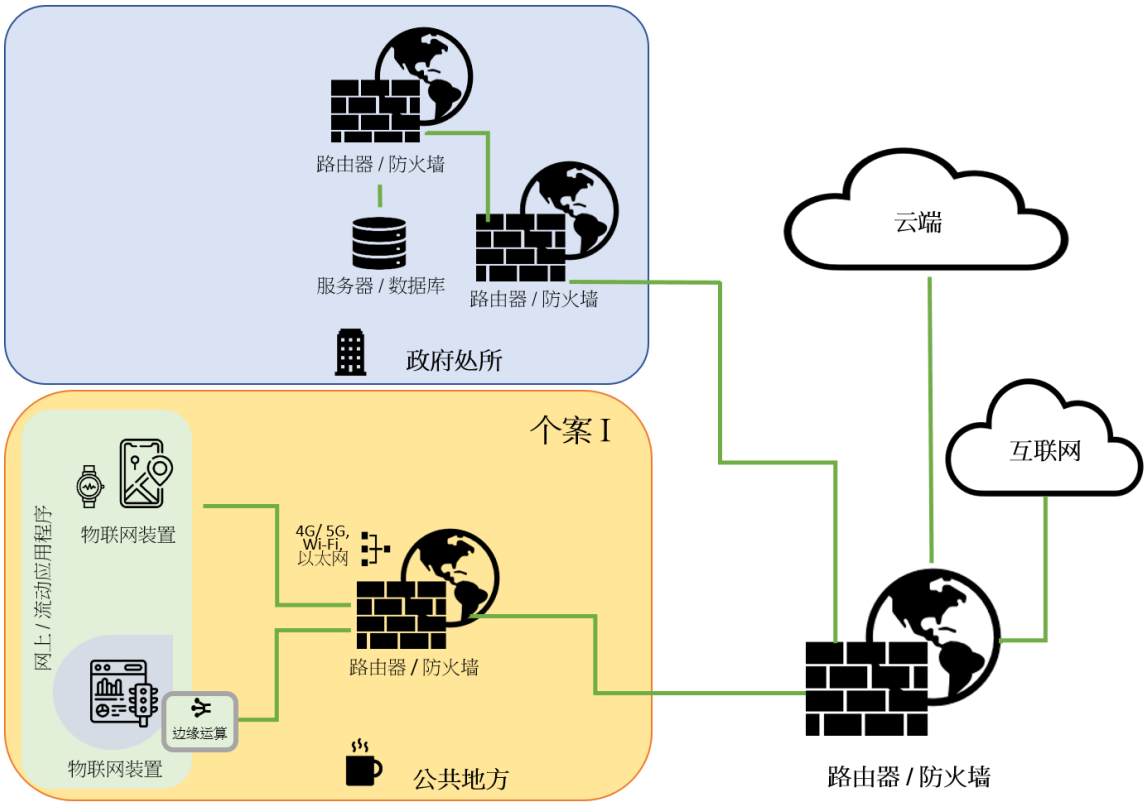

图 7.2 物联网部署案例一 – 公共区域

对于案例一，物联网装置安装在公共区域。 它们相互连接或连接到路由器，以访问云端或互联网获取服务或储存数据。物联网装置也可能通过路由器、防火墙或云端间接连接到政府内部网络。

由于这类装置，尤其是物联网装置产生的数据量增长得非常快，实时数据可能会出现延迟问题，影响应用的性能。在某些情况下，引入边缘运算以提供对行动/数据的实时响应。边缘运算的部署是为了使计算和储存更接近设备和创建数据的位置，以提供高效的数据处理从而降低延迟。用于物联网应用的边缘运算在业界越来越受欢迎。数据处理，如聚合、复制和去识别化，以及一般的物联网功能，如传感和安全管理，都可能受益于边缘运算，以提高物联网系统的服务水平。

边缘运算在物联网系统中起着安全保护的重要作用。在边缘设备上实施入侵检测系统或入侵防御系统可以抵御分布式阻断服务、暴力攻击等可能的攻击，方法是进一步提高攻击的检测率并增强对物联网基础设施的恶意企图的防御能力。应全面保障物联网系统的安全，在边缘结点施行数据认证、访问控制、修补程序更新、防止网络攻击等安全控制措施，并确保数据保护得到备存。必须遵守边缘设备上的安全要求。

由于在这个部署个案中，物联网装置既没有员工看管，也没有安装在有实体安全的地方，因此无法保证有效的实体安全保护。在这情况下，决策局／部门应避免收集敏感资料。如因业务需要无法避免，则决策局／部门不应把敏感数据储存在物联网装置内，以减低数据外泄的风险。如需要储存数据，则应将数据加密，并传输至安全的后端储存库，而该储存库的安全控制措施应符合政府的相关安全要求。如因业务需要而无可避免地在没有员工在场的情况下把保密数据储存在物联网装置中，决策局／部门须采取适当的实体保护措施，并在发现和确定有人试图入侵实体保护时，采取辅助控制措施，例如远程或自动删除数据、中断网络连接等。

另外，设计良好的网络对于保障物联网的系统安全至关重要。一组物联网装置应该由一个具有适当访问控制的网关进行分组和分段。物联网装置绝不应直接连接到内部网络。应配置非军事区，将内部网络与外部网络分开，藉此隐藏内部网络的数据。应实施网络分段，以降低来自物联网装置的违反安全事项的风险。

7.2.1 应用系统界面的安全建议

支持物联网的解决方案通常建立在常见的应用系统界面上，如云端、流动或网络平台。这些常见的应用系统形成了一个物联网生态系统。对物联网生态系统的任何威胁都可能导致物联网装置或其相关组件受损。常见的问题包括缺乏认证/授权、缺乏或使用较弱加密等。下面的章节列出一些与这些应用系统界面有关的注意事项。

云端界面

这类系统通常会用云端数据库、云端储存平台和云端服务来构建物联网解决方案。在采用物联网技术的过程中，采用云端服务会增加安全风险，如缺乏可视性和控制、共有的技术漏洞以及不安全的界面等。以下是保护云端环境中物联网装置的安全控制措施，包括但不限于：

- 确保对所有云端界面进行安全漏洞覆检。
- 尽可能启用 HTTPS。
- 加密储存在云端中的数据以及与其他端点之间的通讯。
- 妥善管理和保护密码匙的整个生命周期。当储存的数据被认为是敏感时，考虑使用硬件安全模块来保护加密密码匙。
- 尽可能采用双重认证方案。
- 尽可能启用网上应用系统防火墙。
- 如果系统有本地或云端的网上应用系统，将默认密码改为严谨的密码，默认用户名称也改为严谨用户名称。
- 启用帐户锁定功能。
- 启用严谨的密码（如果提供）。
- 执行定期更改密码，例如每九十天。

流动界面

物联网应用系统负责提供应用服务。 在大多数情况下，使用者主要通过网上应用系统和流动应用程序与该应用系统进行互动，安排应用系统数据的收集、处理、分析和储存。物联网系统的流动界面需要有针对性的安全防御，如：

- 使用个人辨认号码或密码来提供额外安全（在客户端和服务器上）。
- 尽可能使用双重认证。
- 启用帐户锁定功能。
- 启用严谨的密码（如果提供）。
- 强制定期更改密码，例如每 90 天更改。
- 加密与后台云端应用系统或物联网装置的通讯。
- 不要在流动应用程序中输入非绝对需要的敏感数据，如地址、出生日期、信用卡等。
- 将敏感数据(如个人资料、用户凭证、加密密码匙等)存放在安全的储存场所，并采取符合相关政府安全要求的安全控制措施。

网页界面

与流动应用程序界面一样，网页界面是使用者与物联网互动的另一个主要界面。网页应用系统界面被认为是主要的攻击面之一，需要实施有效的安全措施，如：

- 尽可能启用 HTTPS。
- 尽可能使用双重认证。
- 如果可能的话，启用网上应用系统防火墙。
- 更改默认的用户名称和密码。
- 启用严谨的密码（如果提供）。
- 启用帐户锁定功能。
- 进行完善的网络安全标准检查，以降低风险。
- 如果系统有内部或云端的网上应用系统，确保将默认密码更改为严谨的密码，如果可能，也更改默认用户名称。
- 如果系统具有帐户锁定功能，确保启用该功能。
- 考虑采用防火墙等网络分段技术，隔离物联网系统与关键信息技术系统
- 启用会话超时。

7.3 办公环境中安装的物联网装置（案例二）

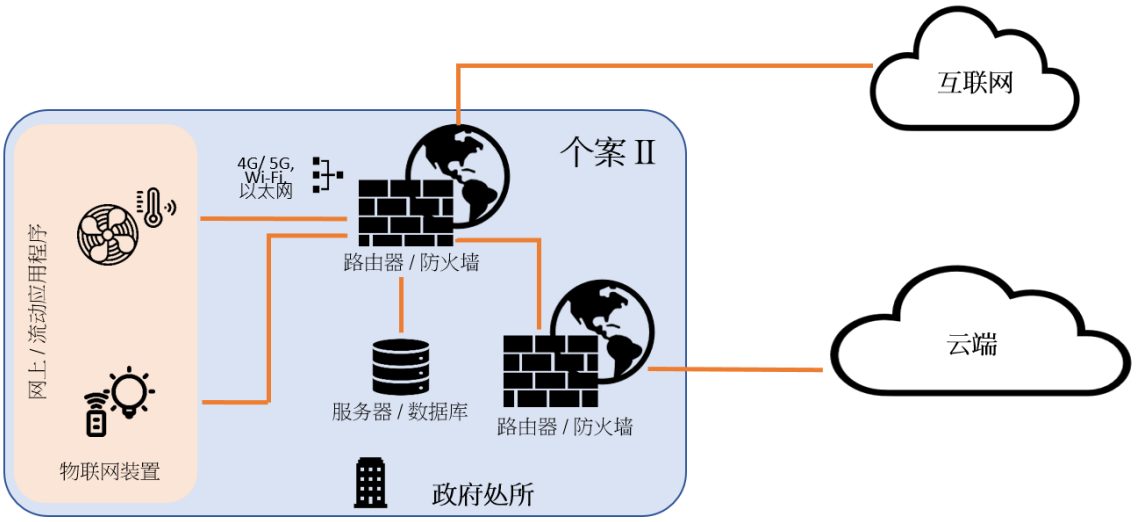

图 7.3 物联网部署案例二 – 办公环境

对于案例二，物联网装置部署在办公环境中，用于支持业务营运。物联网装置可以连接到部门网络。物联网装置可以通过防火墙连接到云端进行数据处理或储存。由于物联网装置安装在办公环境中，须加以保护，避免收集敏感数据或被入侵成为攻击内部网络的跳板。办公环境中的工作站和端

点应考虑的因素包括但不限于实体保护、访问控制、网络分段、加密保护、记录管理、装置管理（例如使用安全修补程序和固件升级、恶意软件侦测和预防），以及数据保护（尤其是个人资料）方面的要求。

从安全的角度来看，应尽可能采用最少功能和最少权限的原则，并设有防范恶意软件的保护机制。决策局 / 部门需要评估所需的功能，并停用任何不必要的功能和端口，以避免收集敏感数据和连接未经授权的设备或网络。如果可能的话，应将允许的服务 / 连接列为白名单。由于物联网装置与流动装置有某些相似之处，例如连接性、流动性和体积细小，政府安全文件中对流动装置的安全要求和原则，应同样适用于物联网装置。

此外，由于物联网装置即使在办公环境中也可能无人看守，因此应实施实体安全控制措施，防止遗失、盗窃和损坏。使用者应该明白，他们的设备只允许连接到批准的网络和设备。应确保连接宽带或 Wi-Fi 的网络是安全的。

与个案一相似，决策局 / 部门应避免收集敏感资料。如因业务需要而无可避免，决策局 / 部门不应把敏感数据储存物联网装置内，以减低数据外泄的风险。如需要储存数据，则应将数据加密，并传输至安全的后端储存库，而后台储存库的安全控制措施应符合政府的相关安全要求。

7.3.1 部署物联网装置的示例

以下是在不涉及敏感信息的情况下通过 Wi-Fi 网络连接到互联网来安装物联网装置的示例。首先，应采取整体和深层防御的方法。一般来说，应考虑以下三个部分：

- 宽带路由器
- Wi-Fi 路由器
- 智能装置

宽带路由器

宽带路由器位于本地网络和互联网之间，是抵御黑客、恶意软件和病毒的第一道防线。在网络层面上，决策局 / 部门应确保物联网装置不会连接到办公室网络，并应考虑在互联网网关(例如宽带路由器)限制所有对本地网络(例如 Wi-Fi 网络)的存取。除了将宽带路由器放置在安全区域外，建议正确配置和利用宽带路由器的安全功能，包括但不限于：

- 改变出厂默认设置（如用户名称、密码、服务设定标识符等），使用严谨的密码进行认证。
- 保持固件的更新，并从制造商网站下载更新的固件。
- 启用防火墙功能。
- 启用媒体访问控制地址过滤功能，限制可以加入网络的设备。
- 启用划一资源定地址过滤，防止用户访问特定网站。
- 停用已知安全问题的服务/功能，如

    - WPS (Wi-Fi Protected Setup)，允许在没有密码的情况下连接网络。
    - 远程管理。
    - 通用即插即用，允许自动连接未经授权的设备。
    - 不安全的规约（远程登入、档案传送规约等）。
    - 网络服务。

- 关闭服务设定标识符广播。
- 启用拒绝服务保护功能，停用支持端口扫描服务。
- 启用记录，并进行定期检查。

Wi-Fi 路由器

决策局 / 部门应注意，Wi-Fi 网络会被其他端点共享，以访问宽带。一旦端点或智能设备受到感染，便会有安全风险。恶意代码会在同一网络内传播，而其他端点亦会受到感染。因此，建议将智能设备与其他端点设备隔离在一个与部门网络隔离的网络（例如访客 Wi-Fi 网络）中，该网络可配置不同的服务设定标识符、认证方法，并只允许访问互联网，但不允许连接至内部网络。隔离的网络可以有效防止或减低感染的影响。可以的话，这个分离智能设备的 Wi-Fi 网络以及服务设定标识符不应广播，以减少对智能设备以及 Wi-Fi 网络的攻击面。 此外，我们亦建议使用最新的 Wi-Fi 标准/规约(例如 Wi-Fi 保护接入 3 (WPA3))及适当的访问控制(例如认证、严谨的密码等)进行 Wi-Fi 通讯，因为据知 WPA2 容易受到 KRACK(Key Reinstallation Attack)的攻击。

智能设备

为保护端点（如智能设备），应采用最少功能和权限原则，并实施防止恶意软件的保护机制和防止遗失、被盗和损坏的实体安全控制措施。如果可行，建议：

- 停用未使用或不需要的功能 。
- 停用实体和逻辑端口或服务（如通用串行总线端口、局部区域网络端口、蓝牙、从互联网远程访问智能设备等）。
- 为智能设备提供固件和操作系统，及安装应用程序的安全修补程序，使其保持在最新的安全状态。
- 从可信的程序商店下载并安装授权的流动应用程序 。
- 只连接已授权的设备到智能设备。
- 不使用时关闭电源。
- 在不需要的情况下，停止互联网的连接。

最后，建议决策局 / 部门进行安全风险评估，以识别和评估潜在的安全风险（例如未经授权进入 Wi-Fi 网络或智能装置、传播恶意软件、 显示非预期的内容）和影响，然后根据业务需要，决定和实施适当的安全措施和配置，以符合相应的政府安全要求。

完