数字政策办公室

信息安全

信息技术安全指南

[G3]

第 10.1 版

2024 年 7 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	修改报告可于政府资讯科技情报网查阅		4.0	2003 年 4 月
2	将「资讯科技署」更改为「政府资讯科技总监办公室」		4.1	2004 年 7 月
3	丰富 / 加强本文件，以提供更多有关： – 应用系统安全的详尽指南（载于第 10.1.1 节「应用系统设计及发展的安全考虑事项」及第 10.7 节「网上应用系统安全」） – 适当处理 / 限制数据披露的详尽指南（载于第 10.4 节「程序 / 系统测试」及第 11.3 节「电邮安全」） – 网络通讯 / 端口及系统服务的适当限制的详尽指南（载于第 11.2 节「互联网安全」） 将英文版中香港电脑保安事故协调中心的简称由“HKCERT/CC”更新为“HKCERT”	10-2 10-6 10-7 10-4 11-4 11-3 无	4.2	2004 年 9 月
4	作出相应更新，以符合经修订的政府安全要求	9-3, 9-10, 11-2	4.3	2004 年 11 月
5	修改报告可于政府内联网「资讯科技情报网」查阅		5.0	2006 年 5 月
6	根据经修订的政府安全要求对附录 B 作出相应更新 对附录 C 作出相应更新并摘录全部六项保障数据原则	B-2 C-1	5.1	2008 年 11 月
7	修改报告可于政府内联网「资讯科技情报网」查阅		6.0	2009 年 12 月
8	修改报告可于政府内联网「资讯科技情报网」查阅		7.0	2012 年 9 月
9	修改报告可于政府内联网「资讯科技情报网」查阅		8.0	2016 年 12 月

10	修改报告可于政府内联网「资讯科技情报网」查阅 (https://itginfo.ccgo.hksarg/content/itsecure/review2021/documents.shtml)		9.0	2021 年 3 月
11	根据公务员学院成立对第 9.1(c)节作出相应更新 关于消磁产品配置灵活性对第 10.3(b)节作出更新 关于严谨密码政策对第 11.4(b)和 11.4(c)节作出更新 根据新版本的文件对第 16.1(b)节作出相应更新	24 30, 31 36-38 80	9.1	2022 年 8 月
12	修改报告可于政府内联网「资讯科技情报网」查阅		10.0	2024 年 4 月
13	将「政府资讯科技总监办公室」更改为「数字政策办公室」 将「香港电脑保安事故协调中心」更改为「香港网络安全事故协调中心」 关于威胁情报平台及来源的例子对第 9.1(c)和 14.7(b)节作出更新		10.1	2024 年 7 月

目录

1. 目的

本文件就《基准信息技术安全政策》所列明的安全要求诠释当中的政策要求，以及订定相关实施标准，同时为有效推行相应的安全措施提供一套指南。

本文件所载的数据不是为任何特定的计算机平台而编制。决策局／部门须遵从本文件所载的指南推行安全控制措施，以符合相关的安全要求。在不影响安全标准的情况下，决策局／部门宜按需要制订适合本身情况的安全措施。

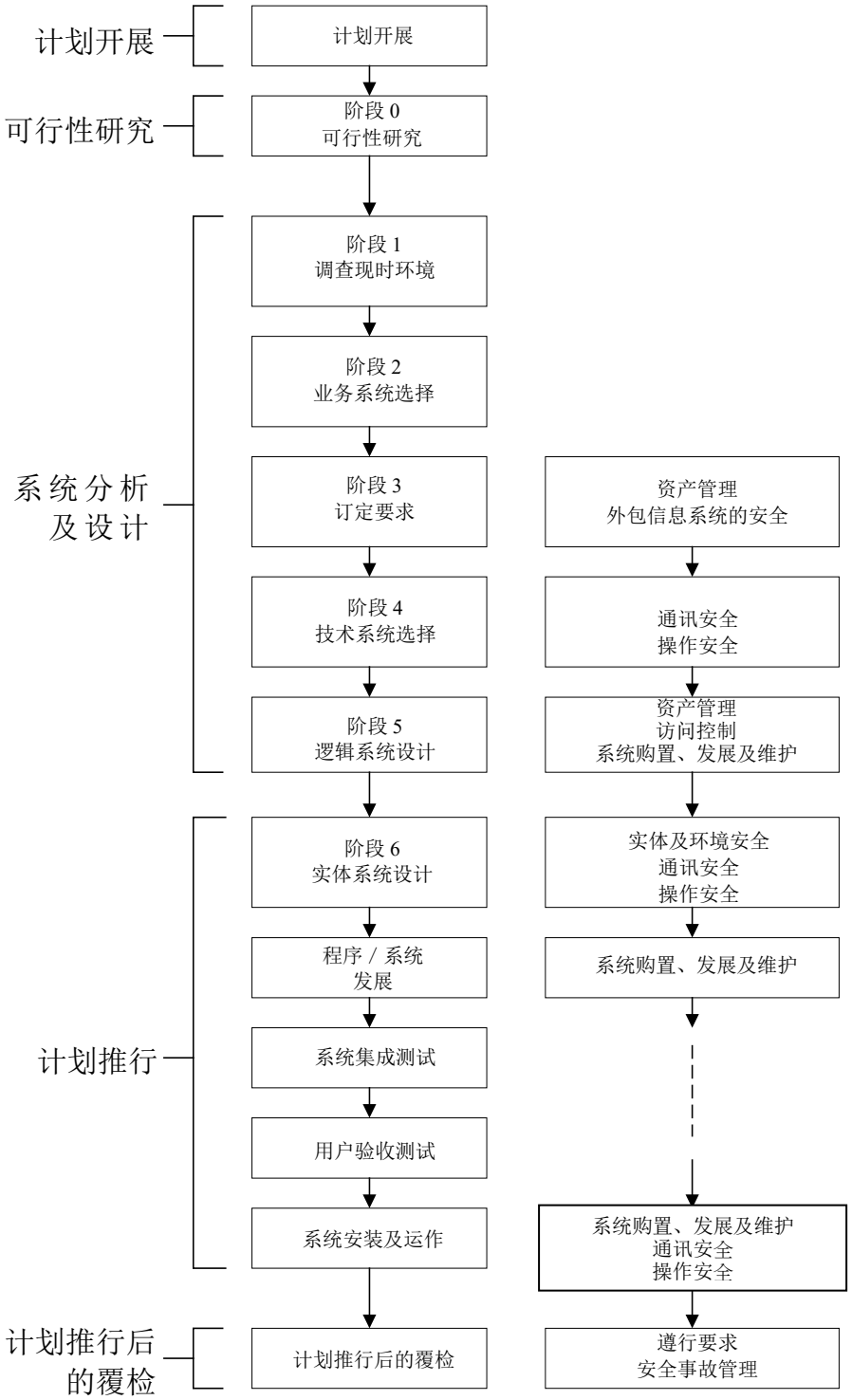
2. 范围

2.1 适用性

本文件采用国际标准化组织（ISO）及国际电工委员会（IEC）所订立的信息安全、网络安全和隐私保护—信息安全管理体系—要求（ISO/IEC 27001:2022）及信息安全、网络安全和隐私保护—信息安全控制（ISO/IEC 27002:2022），并在有关安全范畴及控制措施的部分作调整。本文件就下列 14 个范畴阐述相关指南：

- 管理职责（见第 7 节）；
- 信息技术安全政策（见第 8 节）；
- 人力资源安全（见第 9 节）；
- 资产管理（见第 10 节）；
- 访问控制（见第 11 节）；
- 加密方法（见第 12 节）；
- 实体及环境安全（见第 13 节）；
- 操作安全（见第 14 节）；
- 通讯安全（见第 15 节）；
- 系统购置、发展及维护（见第 16 节）
- 外包信息系统的安全（见第 17 节）
- 安全事故管理（见第 18 节）；
- 信息技术安全方面的业务持续运作管理（见第 19 节）；以及
- 遵行要求（见第 20 节）

基本上，上述范畴在系统发展周期的各个阶段均应予考虑，但若干阶段亦各有需注意的范畴。下页的图示列出这些范畴。



系统发展周期各个阶段涉及的安全范畴

2.2 对象

本文件是为各决策局／部门内担当不同职务的各级人员制订，当中包括管理人员、信息技术管理员和一般的信息技术终端用户。全体人员均有责任通篇阅读整份文件，并了解及遵行，以有效实施相关安全要求。

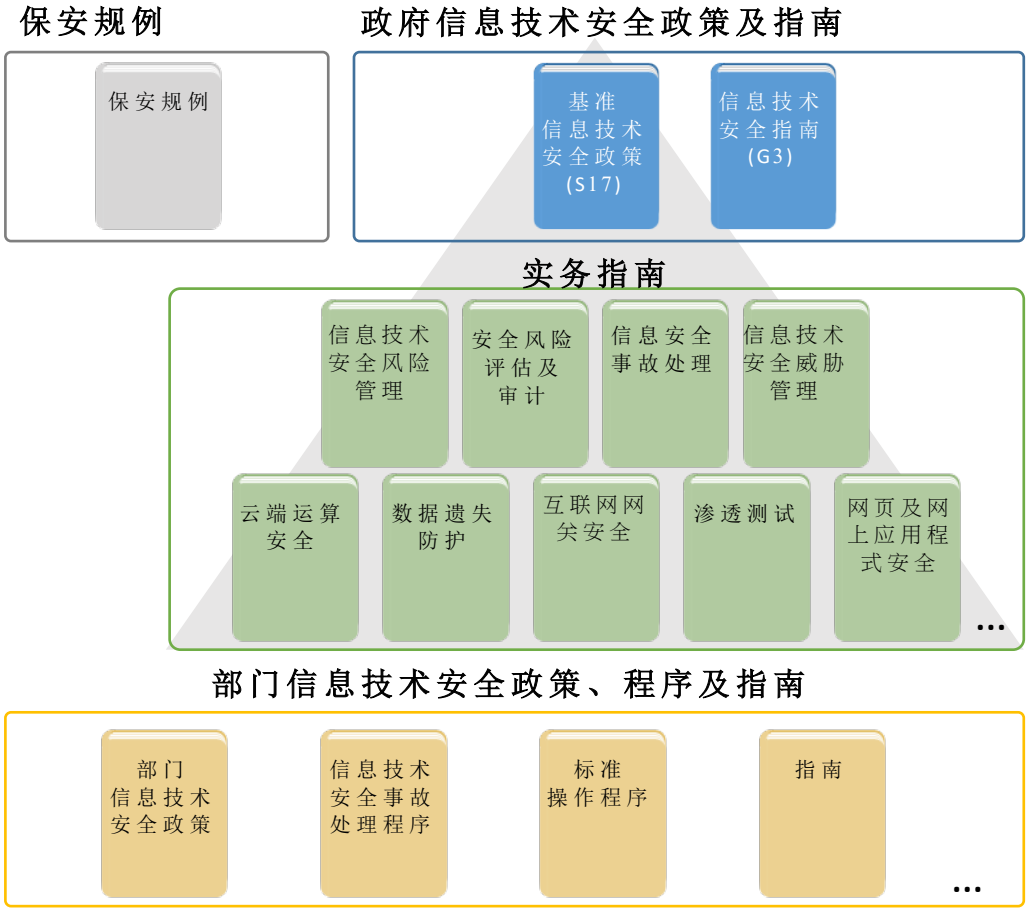
另外，本文件亦供为政府提供信息技术服务的供货商、承包商及顾问使用。

2.3 政府信息技术安全文件

政府已发布一系列保安规例、政府信息技术安全政策及指南，协助决策局／部门制订及推行保障政府信息安全的信息技术政策及控制措施。决策局／部门须遵行《保安规例》、《基准信息技术安全政策》[S17]及《信息技术安全指南》[G3]内的政策要求，以及遵从相关实务指南内的实施指南。这些安全文件是信息安全管理不可或缺的参考资料。

决策局／部门须对第 1 级信息系统采取本文件所载的所有强制性安全要求，并对第 2 级及第 3 级信息系统额外采取附录 C 所载的更严格安全要求，以达致信息技术安全等级保护，从而确保所有政府信息系统均受到与信息系统风险等级相称的安全控制措施所适当保护。

下图显示政府内部多份信息技术安全文件之间的关系：



2.3.1 《保安规例》

由保安局授权的《保安规例》订明哪些文件、材料及信息需列作保密资料，并确保这些文件、材料及信息在政府业务运作过程中得到充分保护。

2.3.2 政府信息技术安全政策及指南

由数字政策办公室制订的政府信息技术安全政策及指南旨在提供相关参考，方便推行信息安全措施，以保障信息资产。这些文件参考了 ISO 及 IEC 所出版的信息安全、网络安全和隐私保护—信息安全管理系统—要求（ISO/IEC 27001:2022）及信息安全、网络安全和隐私保护—信息安全控制（ISO/IEC 27002:2022）。

政府信息技术安全政策及指南订明安全要求的最低标准，并提供有关推行适当安全措施以保护信息资产和信息系统的指导。

《基准信息技术安全政策》 [S17]	最高层次的指令文件，为所有决策局／部门制订安全规格必须达到的最低标准。这份文件列明了对决策局／部门至关重要的安全工作领域。《基准信息技术安全政策》可视为必须遵守的强制性基准规例，各决策局／部门亦可采取其他合适的措施加强安全。
《信息技术安全指南》 [G3]	就《基准信息技术安全政策》所列明的安全要求阐述当中的政策要求，以及订定相关实施标准。决策局／部门必须遵行《信息技术安全指南》，以有效实施相关安全要求。

此外，尚有数份补充《信息技术安全指南》的实务指南，就特定安全范畴提供指导说明，协助决策局／部门应对及减低新兴科技及安全威胁所带来的风险。这些实务指南包括《互联网通讯闸安全实务指南》、《信息技术安全风险管理实务指南》、《信息技术安全威胁管理实务指南》、《安全风险评估及审计实务指南》和《信息安全事故处理实务指南》等。

这些实务指南已载于政府资讯科技情报网的信息技术安全专题网页 (https://itginfo.ccgo.hksarg/content/itsecure/techcorner/practices.shtml)。

2.3.3 部门信息技术安全政策、程序及指南

决策局／部门须根据上文第 2.3.1 及 2.3.2 节所述《保安规例》及政府信息技术安全政策及指南内列明的所有政府安全要求及实施指南，制订本身的部门信息技术安全政策、程序及指南。

3. 参考标准

a) 香港特别行政区政府《保安规例》

b) 《基准信息技术安全政策》[S17]

c) Information security, cybersecurity and privacy protection – Information security management systems – Requirements, ISO/IEC 27001:2022, dated 25 October 2022

d) Information security, cybersecurity and privacy protection – Information security controls, ISO/IEC 27002:2022, dated 15 February 2022

e) 信息安全技术网络安全等级保护基本要求，GB/T 22239-2019，发布于 2019 年 5 月 10 日

f) 《电子政府互用架构》[S18]

4. 定义及惯用词

4.1 定义

a) 第 1 级信息系统	由硬件及软件组成的系统，用作收集、处理、储存、传递或弃置资料，不论其资金来源及项目类型。
b) 第 2 级信息系统	对政府或社会运作重要的第 1 级信息系统，其故障或中断会对政府运作带来严重影响，或可能引致公众混乱及灾难性后果。
c) 必要服务	对社会及其经济的运作和安全必要的服务。
d) 第 3 级信息系统	与提供有关的必要服务直接相关且其中断或破坏可能对经济、民生、公共安全等造成严重损害的第 2 级信息系统。
e) 机密性	在任何方面只有获授权人士及信息系统能够知悉或访问信息系统所储存或处理的数据。
f) 完整性	在任何方面只有获授权人士及信息系统能够修改信息系统所储存或处理的数据。
g) 可用性	信息系统在获授权人士及信息系统提出要求时，可供该人士及信息系统访问及使用。
h) 信息技术安全政策	明文规定的管理指示，详细阐述如何妥善使用和管理计算机及网络资源，以保护有关资源和信息系统所储存或处理的数据免在未获授权的情况下被披露、窜改或破坏。
i) 保密资料	按《保安规例》划分的各类保密资料。
j) 人员	受聘为政府工作的人士，或其服务是用以为政府工作的人士的统称，包括不论雇用期及雇用条件的所有公职人员、通过中介公司聘用的非政府借调人员，以及其他提供定期合约服务的人士等。此等人士在访问保密数据方面可能有不同权限，亦受到不同的安全审查规定规管。有关人力资源安全的具体规定载于《基准信息技术安全政策》第 9 节。

k)	数据中心	放置信息系统及相关设备的中央数据处理设施。
l)	计算机室	放置计算机设备的专用房间。
m)	恶意软件	蓄意进行未获授权的程序以破坏信息系统的机密性、完整性或可用性的程序。恶意软件的例子包括计算机病毒、蠕虫、特洛依木马及间谍软件。
n)	流动装置	可储存及处理数据的便携式计算机及通讯装置。例子包括便携式计算机、流动电话、平板计算机、数码相机、录音或录像装置。
o)	抽取式媒体	可插入计算机装置及从计算机装置移除的便携式电子储存媒体，例如磁性、光学和闪存记忆装置。例子包括外置硬盘或固态硬盘、软磁盘、压缩盘、光盘、磁带、记忆卡、闪存盘和类似的通用串行总线储存装置。
p)	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。

4.2 惯用词

本文件的惯用词载列如下：

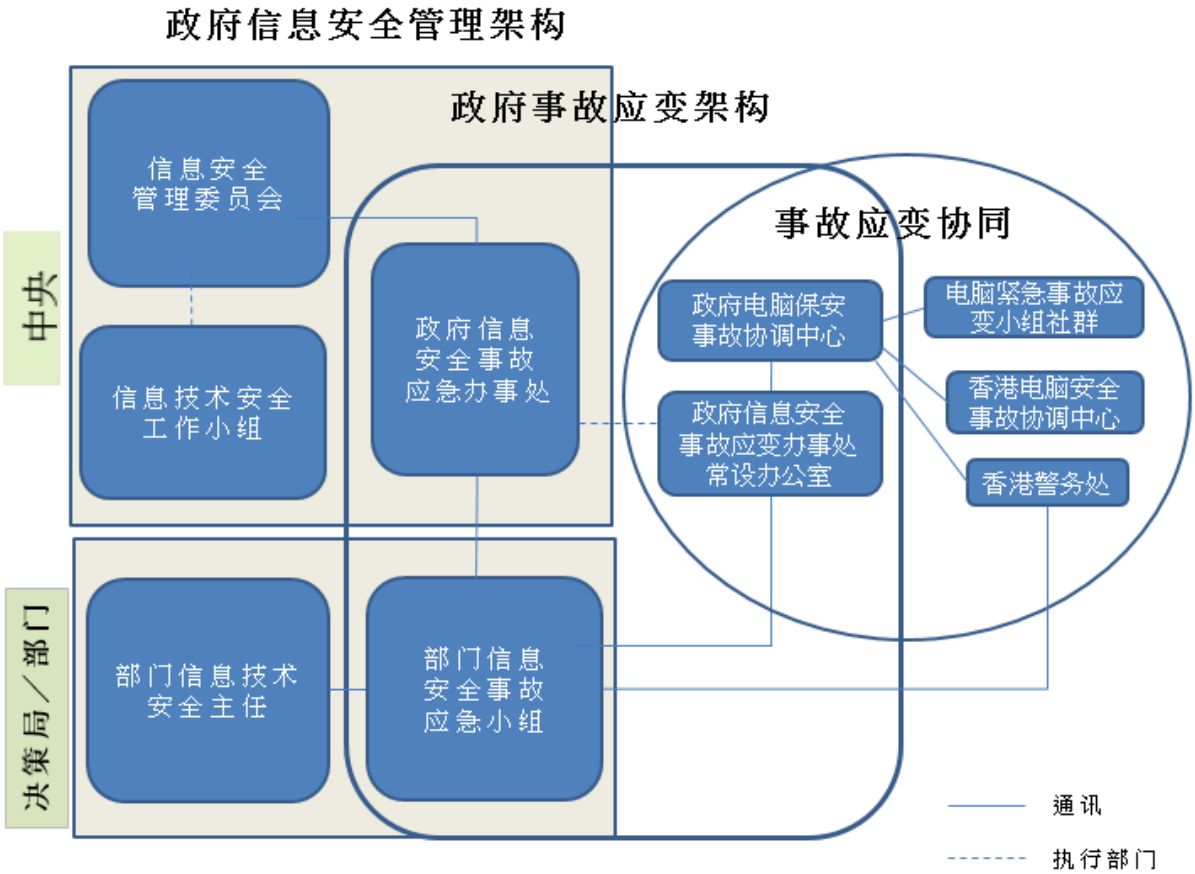
须	「须」表示强制性规定。
应	「应」表示良好作业模式，应尽可能贯彻执行。
宜	「宜」表示期望达到的良好作业模式。

5. 政府信息安全组织架构

5.1 政府信息安全管理架构

为协调及推动政府内部的信息技术安全工作，政府设立了由以下五方组成的信息安全管理架构：

- 信息安全管理委员会
- 信息技术安全工作小组
- 政府信息安全事故应急办事处
- 政府电脑保安事故协调中心
- 决策局 / 部门



政府信息安全管理架构

以下几节将详细介绍有关各方所担当的职务和职责。

5.1.1 信息安全管理委员会

信息安全管理委员会为中央组织，成立于 2000 年 4 月，以监督整个政府内部的信息技术安全工作。委员会定期举行会议，以：

- 覆检与政府信息技术安全有关规例、政策及指南，并批准有关修订；
- 界定与信息技术安全相关的具体职务和职责；以及
- 通过信息技术安全工作小组就实施与信息技术安全有关规例、政策及指南，向决策局／部门提供指导及协助。

信息安全管理委员会的核心成员包括下列决策局／部门的代表：

- 数字政策办公室
- 保安局

委员会将按需要就特定事宜从其他决策局／部门增选代表。数字政策办公室会依照本文件的要求，协助覆检并厘清各决策局／部门提交的文件。

5.1.2 信息技术安全工作小组

信息技术安全工作小组作为信息安全管理委员会的执行部门，负责发布与政府信息技术安全有关的规例、政策及指南，并监督其遵行情况。信息技术安全工作小组于 2000 年 5 月成立，其职责如下：

- 协调各项工作，以期就实施与信息技术安全有关规例、政策及指南向决策局／部门提供指导及协助；
- 监督决策局／部门对《基准信息技术安全政策》的遵行情况；
- 订定及覆检与信息技术安全有关规例、政策及指南；以及
- 提高政府内部对信息技术安全的意识。

信息技术安全工作小组的核心成员包括下列决策局／部门的代表：

- 数字政策办公室
- 保安局
- 香港警务处
- 政务司司长办公室

工作小组将按需要就特定事宜从其他决策局／部门增选代表。

5.1.3 政府信息安全事故应急办事处

为处理决策局 / 部门内部的信息安全事故，各决策局 / 部门须成立信息安全事故应变小组。同时，政府信息安全事故应急办事处将集中协调并支持各决策局 / 部门信息安全事故应变小组的运作。政府信息安全事故应急办事处常设办公室是该办事处的执行部门。

政府信息安全事故应急办事处的主要功能如下：

- 设立中央数据库，并监督政府内部处理所有信息安全事故的工作；
- 定期编制政府信息安全事故统计报告；
- 充当中央协调办事处，以协调处理多点安全攻击（即不同的政府信息系统同时受到攻击）的工作；以及
- 促使各决策局 / 部门的信息安全事故应变小组之间互相分享和交流信息安全事故处理的经验和数据。

政府信息安全事故应急办事处的核心成员包括下列决策局／部门的代表：

- 数字政策办公室
- 保安局
- 香港警务处

5.1.4 政府电脑保安事故协调中心

政府电脑保安事故协调中心于 2015 年 4 月成立。除与政府信息安全事故应急办事处常设办公室合作，协调政府内部的信息及网络安全事故外，政府电脑保安事故协调中心亦会与电脑紧急事故应变小组社群分享事故信息及威胁情报，并就良好作业模式进行交流，借此加强地区内的信息和网络安全能力。政府电脑保安事故协调中心的主要功能如下：

- 就即将及已经发生的威胁向决策局 / 部门发出安全警报；以及
- 在处理网络安全事故时，充当香港网络安全事故协调中心与其他电脑安全事故紧急应急小组之间的桥梁。

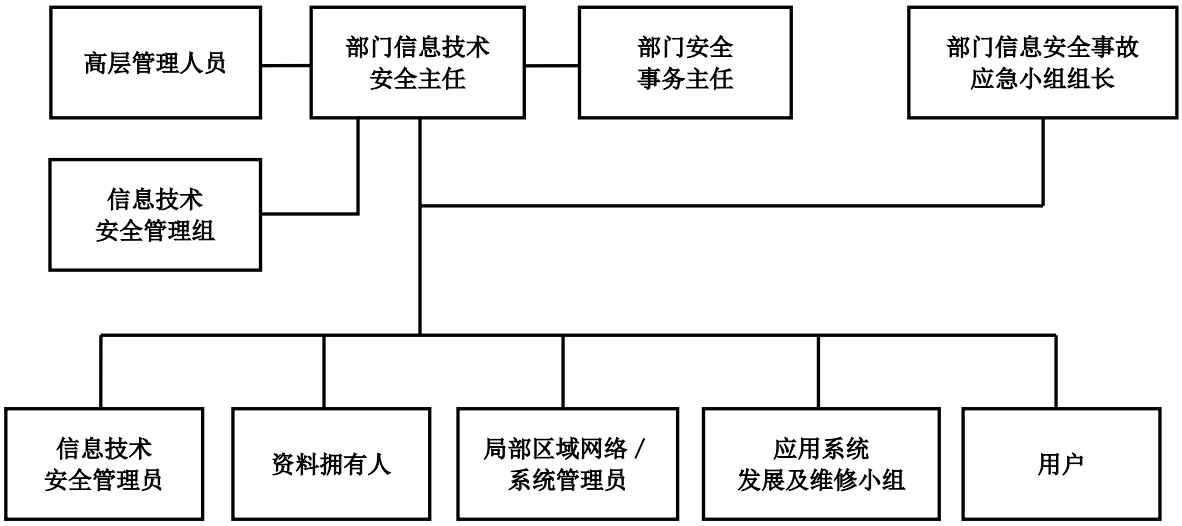
5.1.5 决策局 / 部门

决策局 / 部门须负责确保其信息资产和信息系统的安全。有关决策局 / 部门内部信息技术安全人员的职务和职责详情，载于第 5.2 节—部门信息技术安全组织。

5.2 部门信息技术安全组织

本章节阐述部门信息技术安全组织中个别人员的职务和职责。为确保职务分工恰当，除非受到资源限制，否则不应指派一名人员担当多项职务。

下图为部门信息技术安全管理架构的示例：



部门信息技术安全管理组织架构图标例 [1]

5.2.1 高层管理人员

决策局／部门的高层管理人员须正确认识信息技术安全、安全问题和解决方法。高层管理人员的职责包括：

- 在决策局／部门内发挥领导才能，推动和优先考虑信息技术安全；
- 指挥及落实制订安全措施；
- 提供推行安全措施所需的资源；
- 确保各级管理、行政、技术及操作人员对信息技术安全工作的参与及问责，并向他们提供一切支援；
- 在决策局／部门上下推动安全意识和问责文化；以及
- 确保决策局／部门的信息技术安全策略配合业务目标。

高层管理人员应考虑成立信息安全督导委员会，或将信息安全列作管理层会议定期讨论项目之一。

[1] 实际的信息技术安全管理架构可能会因应各部门的情况而有所不同。

5.2.2 部门信息技术安全主任

决策局局长 / 部门首长须从高层管理人员中委任一名人员，担任部门信息技术安全主任，负责信息技术安全工作。负责决策局 / 部门信息技术管理工作的首长级人员可视作适合担当部门信息技术安全主任的职务。视乎部门规模，首长级的部门职系人员如了解有关决策局 / 部门的缓急需要、该决策局 / 部门信息系统及数据资产的重要性，以及保障该决策局／部门所须达到的安全级别，亦可视作合适人选。

如决策局 / 部门最终不能委任一名首长级人员为部门信息技术安全主任，有关决策局局长 / 部门首长则应委任一名高层人员，并授予足够的权力在处理严重威胁事件或安全事故时调动资源和作出决定，该项委任亦应向决策局 / 部门的所有相关工作人员发布。

为了让获指派担任部门信息技术安全主任的人员具备更多安全管理和相关科技的知识或技术，保安局和数字政策办公室会为部门信息技术安全主任提供培训，以便他们执行职务。部门信息技术安全主任须出席指定的培训。部门信息技术安全主任的职务和职责须清晰界定，包括但不限于：

- 制订和维持信息保护计划，以协助全体人员保护所使用的信息及信息系统；
- 制订适当的安全监管程序，以评估、指导、监察及传达决策局 / 部门内有关信息技术安全的工作；
- 推动高层管理人员定期讨论信息技术安全问题，以获得足够的支援和资源；
- 带领有关制订、维持及推行信息技术安全政策、标准、程序及指南的工作；
- 在信息技术操作的各阶段监督、监察、覆检和改善信息技术安全管理工作的效益和效率；
- 监察并确保遵行政府信息技术的安全要求；
- 监督决策局 / 部门内的整体信息技术安全意识及培训计划；
- 在信息技术安全事务上与其他决策局 / 部门协调；
- 监督决策局 / 部门内的整体信息技术风险管理程序，包括确保进行必要的信息安全风险评估和审计，并应对不断变化的风险形势、监管变化、技术改良和系统关键性；
- 向决策局 / 部门的负责人传达政府信息安全事故应急办事处就即将及已经发生的威胁所发出的安全警报；以及
- 就违反安全事故主动展开调查并作出修正。

5.2.3 部门安全事务主任

决策局局长 / 部门首长会指派一名部门安全事务主任负责部门内的安全相关工作。部门安全事务主任将担当执行人员的职务，以：

- 履行决策局 / 部门内的所有安全职责；以及
- 就安全政策的制订及覆检提出建议。

部门安全事务主任可兼任部门信息技术安全主任。如决策局 / 部门委任他人为部门信息技术安全主任，部门信息技术安全主任须与部门安全事务主任合作，共同监督决策局 / 部门的信息技术安全工作。

5.2.4 部门信息安全事故应变小组组长

部门信息安全事故应变小组是协调处理决策局 / 部门内信息安全事故的中央联络点。决策局局长 / 部门首长应从高层管理人员中挑选一名人员，担任信息安全事故应变小组组长。信息安全事故应变小组组长应有权委任信息安全事故应变小组的核心成员。信息安全事故应变小组组长的职责包括：

- 全面监督及协调处理决策局／部门内所有信息系统的信息安全事故；
- 就控制损毁、系统复原、外部机构委聘及其所参与工作的程度，以及复原后恢复正常服务的后勤工作等关键事项作出决策；
- 因应事故对决策局 / 部门业务运作的影响，在适当情况下启动部门的运作复原程序；
- 代表管理层批核为事故处理程序投放的资源；
- 代表管理层批核就事故的立场所作的公众发布；
- 与政府信息安全事故应急办事处合作，报告信息安全事故，以便作中央记录及采取必要的跟进行动；以及
- 促进决策局 / 部门内部互相交流和分享信息安全事故处理及相关事宜的经验和数据。

5.2.5 信息技术安全管理组

决策局／部门须设立信息技术安全管理组，向部门信息技术安全主任报告并协助部门信息技术安全主任履行职责。各决策局／部门的信息技术安全管理组的规模及组成可能有所不同，视乎各决策局／部门的业务及运作需求而定。信息技术安全管理组的职责包括：

- 协助部门信息技术安全主任制订、建立和备存决策局／部门的整体信息安全策略和路线图，包括制订信息技术安全政策、基准、标准、指令等；
- 协调决策局／部门内的安全意识及培训计划；
- 协调信息技术安全措施的推行并监察信息技术安全流程的进度，以确保信息技术安全管理的成效并符合政府安全要求；
- 推动信息技术安全威胁和风险管理活动，并支援与信息技术安全相关的运作复原和业务持续运作计划职能；以及
- 履行部门信息技术安全主任指示的任何其他职责。

5.3 其他职务

5.3.1 信息技术安全管理员

信息技术安全管理员须负责提供有关安全及风险管理方面的支持服务。信息技术安全管理员的职责还包括：

- 协助找出并缓解系统的安全漏洞；
- 协助进行修补程序管理流程；
- 执行安全管理工作，例如推行访问控制和管理用户权限；
- 备存和覆检审计记录；
- 监察威胁情报来源并适时了解新兴安全威胁；以及
- 操作和维护安全工具和系统，例如入侵侦测和防御系统。

信息技术安全管理员不应由系统管理员兼任。信息技术安全管理员与系统管理员两者的职务应有清晰的分工。

信息技术安全管理员虽然负责管理审计记录，但不应窜改或更改任何审计记录。

决策局／部门可委任一名信息技术安全审计师，负责审计信息技术安全管理员的工作，以确保其尽忠职守。

5.3.2 资料拥有人

资料拥有人须为整理和拥有信息系统内所储存资料的人士。资料拥有人的主要职责是：

- 决定数据的保密类别、授权数据的用途，以及保护数据的相应安全要求。

5.3.3 局部区域网络 / 系统管理员

局部区域网络 / 系统管理员须负责决策局 / 部门内部计算机系统和网络的日常管理、运作及配置工作，而互联网系统管理员则负责处理与连接互联网的信息系统相关的工作。局部区域网络 / 系统管理员及互联网系统管理员的职责包括：

- 根据部门信息技术安全主任制订的程序 / 指南，推行安全机制和控制措施。

5.3.4 应用系统发展及维修小组

应用系统发展及维修小组须负责通过使用优良的程序、技术和工具，以发展优良的信息系统。该小组的职责包括：

- 联络资料拥有人，以便在应用程序开发和维护过程中订定和执行系统安全要求；以及
- 确保使用优良的程序、技术和工具开发安全的系统。

5.3.5 用户

信息系统的用户必须是获授权访问和使用数据的人员。用户须为自己的一切活动负责。用户的责任包括：

- 参与决策局 / 部门指示的安全意识及培训计划；
- 尽量了解、认识、遵从及运用一切可行及可用的安全机制；
- 防止其所保管的数据外泄和遭他人在未获授权的情况下访问；以及
- 尽力安全地保管计算机和储存装置，防止他人在未获授权的情况下访问或恶意攻击该等装置。

6. 核心安全原则

本章节阐述一些广为接纳并从宏观角度应对信息安全事宜的原则。这些原则属基本原则，甚少改变。决策局 / 部门须遵守这些原则，以制订、推行和了解安全政策。下列信息安全原则并非详尽无遗：

- **信息系统安全目标**

  信息系统安全的目标或宗旨可通过下述三项整体目标说明：机密性、完整性和可用性。安全政策和措施须按这三项目标制订及推行。

  这些安全目标可作为指南，以制订标准、程序和控制措施，供安全设计及安全方案各个范畴使用。简单来说，就信息系统而言，只有获授权用户才可知悉、访问、更改或删除信息系统所储存或处理的数据。此外，信息系统须在获授权用户提出要求时，可供该用户访问及使用。

- **风险为本的方法**

  须采用风险为本的方法，以一致及有效的方式为信息系统识别安全风险、订定应对风险的缓急次序和应对有关风险。须依照第7.2 (b)节所述的信息技术安全等级保护推行适当的安全措施，以保护信息资产及系统，并把安全风险减至可接受的水平。

  风险为本的方法一般包括风险评估和风险处理两个程序，这些程序可以加入到不同的程序中，例如项目管理、漏洞管理、事故管理、问题管理，甚至临时就某特定主题进行的程序。风险评估程序包括：

  (a) 制订及持续覆检接受风险准则，以及信息安全风险评估的启动准则；
  (b) 找出风险拥有者和在失去信息机密性、完整性和可用性情况下相关的风险；
  (c) 根据潜在的影响和发生的可能性来确定风险水平以分析风险；
  (d) 通过比较风险分析的结果与既定准则作出评估，并订定处理经分析的风险的缓急次序。

  风险处理程序须用作选择合适的风险处理方案，并决定所需的控制措施，以落实执行选定的方案。这个风险为本程序须确保已包括一切所需的控制措施，以及订立一套风险处理计划，并由风险拥有者批准有关计划和接受余下的安全风险。

  风险拥有者须负责评估、管理及监察已被确认的风险和选定的风险控制措施的推行情况。

- **设计层面的安全**

  须采用设计层面的安全概念，将安全要求纳入系统发展周期，确保信息系统和应用程式采取适当的安全和资料保护措施。在开发过程的所有阶段均须考虑和引入安全元素，以尽量减少重做系统所需的工作。

  设计层面的安全是一种软件及硬件开发方法，目的是在系统发展周期的每个阶段中透过设计和建立安全性来减少系统漏洞和攻击面。这包括在设计中纳入安全规格、在每个阶段持续进行安全评估，以及遵循良好作业模式。针对信息技术安全，设计层面的安全解决了系统生命周期中的信息技术保护问题。这包括专门用于增强系统的信息技术复原能力的安全设计。因此，决策局／部门须尽可能采用设计层面的安全方法。

- **预防、侦测、应变和复原**

  信息安全涵盖预防、侦测、应变和复原措施。预防措施用于避免或制止不利情况发生。侦测措施用于识别已出现的不利情况。应变措施是指在不利情况（或事故）发生时所作出的协调行动，以控制损毁。复原措施则是令信息系统的机密性、完整性和可用性回复至预定状态。

  防御是第一道防线。采取适当的安全保护措施，有助减低发生安全事故的风险。然而，如安全措施遭攻破，决策局／部门亦须有能力迅速侦测安全事故及快速应变以控制损毁，并须及时令信息系统和有关数据复原。因此，决策局／部门须指派适当人员管理信息技术安全事宜，以及制订信息安全事故处理计划。

- **处理、传输和储存数据时的保护措施**

  处理、传输和储存数据时，须视乎情况考虑及推行安全措施，以维持数据的机密性、完整性和可用性。例如欠缺保护的无线通信容易遭受攻击，因此传输保密数据时须采取安全措施。

  决策局／部门制订安全措施时，须审慎考虑及评估有关风险，包括资料被他人在未获授权的情况下窜改、破坏或披露，以及在不同情况下查阅数据的要求被拒等。

- **外部系统假定为不安全**

  一般来说，外部系统须假定为不安全。决策局／部门在把其信息资产或信息系统连接至外部系统时，须根据业务要求及相关的风险水平，以实体或逻辑方式推行安全措施。

  外部系统未必根据政府安全要求设计、开发及维护，因此决策局／部门须考虑在其信息资产或信息系统连接至外部系统时，采取多重防御措施。来自外部系统的任何数据，包括用户输入的数据，均可能是潜在的攻击来源，信息系统须因此进行分隔或隔离，并应按系统所需的安全水平推行不同程度的访问控制和保护措施。

- **重要信息系统的复原能力**

  所有重要信息系统须具备复原能力，以应付严重的服务中断情况。决策局 / 部门亦须采取措施，以侦测服务中断情况、尽量减低破坏，以及迅速应变和使系统迅速复原。于复原计划中，须考虑并适当地推行损害控制措施，以限制事故范围、强度及影响，令系统能有效复原。

  损害控制是指推行安全控制措施，以限制安全事故所带来的影响。信息系统的复原能力是指信息系统在不利或压力情况下，甚至在效率下降或几近不能操作的状态下，仍可继续操作并维持基本功能。复原能力亦包括可因应业务需要，在所定时间内令系统恢复有效运作的能力。

- **审计和问责**

  信息安全须加入审计和问责元素。审计是指通过审计追踪、系统记录、警报或其他提示信息等证据，核实信息系统内的活动。问责是指审核所有曾与信息系统互动的人士 / 机构的活动和所涉的程序。须根据资料的敏感度，明确制订和定出有关各方所担当的职务和职责，并据此授予权限。

  审计有助重组完整的系统行为记录，故可于安全事故发生时，有助找出和调查有关系统所出现的问题。问责则往往能确定涉事的单一个别人士，让有关方面能追查其在信息系统上的活动。

- **持续改进**

  为了因应不断转变的环境和技术而作出更新，须推行一套持续改进程序，以监察、覆检及改善信息技术安全管理工作的效益和效率。安全措施的效能须定期予以评估，以确定是否达到信息技术安全目标。

  决策局 / 部门须找出将予监察和测量的信息安全程序和控制措施，并决定监察、测量及评估结果的方法。须定期覆检安全措施，以确保措施维持足够、适当及有效。安全覆检的结果须包括对可予持续改善之处作出的决定，以及视乎情况对安全措施作出任何变更的需要。

7 管理职责

决策局局长／部门首长须落实执行有效的安全安排，以确保政府的信息系统和资产得到保障，以及信息技术服务能安全运作。

7.1 一般管理

(a) 职务和职责

决策局／部门须应用信息安全管理中有关制衡的核心安全原则和良好作业模式。不论项目种类为何，在项目管理的每个阶段均须考虑信息安全。

无论信息系统的资金来源为何，决策局／部门须确保其所有信息系统，包括基础设施及部门共享的信息技术服务，均按其风险程度得到妥善保护。须采取第 7.2(b)节所提及的信息技术安全等级保护，以便对信息系统进行有效的信息技术安全风险管理。此外，决策局／部门须确保安全保护措施能够迅速应对并配合不断变化的环境和技术。

决策局／部门须参照第 5.2 节—部门信息技术安全组织，订定其部门信息技术安全管理架构。决策局／部门应委派一名高层要员，负责监督制订和实施合适的安全政策和程序，并确保在行政及操作过程中有足够的制衡机制。决策局／部门在分派职责时，应参照部门信息技术安全管理架构、政策及程序。

获分派职责的人员可将安全工作委托予其他人员，惟他们仍须有最终责任确保已推行足够的安全措施。同时，获分派职责的人员应确保受委托人员无论在能力、知识、经验及资历上均适合处理该工作。有关人员应检查所有委托工作是否已妥当处理，而委托内容亦须详细记录并定期覆检。

(b) 职务分工

职务分工是指将一项工作的各个步骤分别交由不同人员处理，以杜绝程序被一人破坏的可能性。有关安排须充分利用职务分工，并明确区分职务和职责，以尽量减少由一人独揽执行和控制整个信息系统所有安全工作和／或重要操作的权限。

如因受人手或其他技术问题所限而无法推行职务分工，则应采取辅助控制措施，以提供相同的保障，例如适当地备存有关人员在系统上所作的关键操作记录，并由适当授权级别的人员突击抽查和／或定期审阅记录档案。

(c) 预算

决策局／部门须控制预算，以确保有足够拨款推行所需的安全保护措施。管理层应根据短期及长期目标或目的，制订信息安全的预算方案、预测及资源分配计划。应根据风险等级分配资源來保护信息系统。

(d) 查阅数据的权利

在符合《个人资料（私隐）条例》的情况下，决策局／部门须保留权利查阅政府信息系统所储存或传递的各项数据，包括电邮、文件目录，以及讨论区、新闻组和网站的访问记录。这些检查有助确保内部政策的遵行情况、配合内部调查，以及促进政府信息系统的安全管理。

7.2 安全风险管理

(a) 风险为本的方法

为应对不断转变的环境和技术，决策局／部门须采用风险为本的方法处理信息安全，以确保信息资产的机密性、完整性及可用性，以及信息系统符合其他所有安全要求。决策局／部门只须采取一些简单的措施，便应能够有效减低及控制由人为及／或操作问题所导致的信息安全潜在风险，使风险降至可接受的水平。决策局／部门须根据个别业务及实际操作环境，考虑采用良好作业模式。

(b) 信息技术安全等级保护

为确保所有政府信息系统均受到与信息系统风险等级相称的安全控制措施所适当保护，决策局／部门须采取信息技术安全等级保护，为其所有信息系统（包括基础设施及部门共享信息技术服务）评级，无论其资金来源为何，并依系统等级，包括第 1 级、第 2 级和第 3 级信息系统，推行分级的安全控制措施。决策局／部门须对一般信息系统采取本文件所载的所有强制性安全要求，并对第 2 级和第 3 级信息系统额外采取附录 C 所载的更严格安全要求。决策局／部门须确保信息系统等级在信息系统的整个生命周期内与其业务目标保持一致。

第 2 级信息系统是指对政府或社会运作重要的第 1 级信息系统，其故障或中断会对政府运作带来严重影响，或可能引致公众混乱及灾难性后果。决策局／部门应考虑数据的保密级别及服务中断的后果，以决定其关键性。关键性的评估应包括以下各方面：

- 防御／安全风险（例如对人命、财产或个人隐私造成伤害、无法执行法定责任及维持治安）。
- 经济影响（例如可能减慢经济增长或导致政府经济损失）。
- 政府形象（例如对政府声誉、公众信心的影响）。
- 相互影响（例如一个系统的服务质素下降可能导致另一个信息系统的服务中断）。

此外，决策局／部门在为系统评级时，应包括适用于其信息系统的其他考虑层面，并根据在信息系统发生故障或中断时影响的范围（即受影响用户人数）、严重性（即中断或损毁引致的后果）、停止运作的容忍程度（即服务中断可造成严重影响的临界点），以及可能对业务造成的最大影响作出评估。

此外，有很多必要服务对社会及其经济的运作和安全是关键的。第 3 级信息系统是指与提供有关的必要服务直接相关且其中断或破坏可能对经济、民生、公共安全等造成严重损害的第 2 级信息系统。

决策局／部门在为信息系统评级时，须参考附录 B 的考虑因素。所有信息系统的评级详情均须妥善记录。信息系统等级须经决策局局长／部门首长或他们明确授权的首长级人员批准。

(c) 信息技术安全风险管理架构

为确保决策局／部门以有条理的方法进行及监察安全风险评估，决策局／部门应采用以下信息技术安全风险管理架构，当中包括一系列风险管理程序，并利用风险记录册，以达致有效的信息技术安全风险管理及沟通。以下是该架构的重点以供参考。

- 部门背景建立－建立决策局／部门的信息技术安全风险管理背景，其中包括决策局／部门的风险偏好和承受能力。
- 风险评估－对决策局／部门的所有信息系统进行第 20.2(a)节规定的安全风险评估，即根据风险源头（例如漏洞、威胁）和事件（例如事故场景）识别信息系统的信息技术安全风险，根据风险的影响和可能性决定已识别风险的级别，对已分析的风险进行缓急排序以作风险处理，并将已排序的风险记录在信息系统的风险记录册中。
- 风险处理－就信息系统的每项风险决定适当的风险处理方法（例如风险降低、规避、转移和接受），将其级别降低至决策局／部门的风险偏好范围内，并将其处理方法记录在信息系统的风险记录册中。
- 风险关联、汇总和规格化－透过在部门背景中进行风险关联、汇总和规格化，将信息系统的各个风险记录册整合到部门的信息技术安全风险记录册中，以便决策局／部门进行信息技术安全风险监控和沟通。
- 风险监控和报告－监控部门的信息技术安全风险和相应的风险处理，并向部门信息技术安全主任和其他有关各方报告。

如欲获取更多有关信息技术安全风险管理架构的资料，可参考以下文件：

- **《信息技术安全风险管理实务指南》**
  可在政府资讯科技情报网下载
  （https://itginfo.ccgo.hksarg/content/itsecure/techcorner/practices.shtml）

8. 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，以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援。

8.1 信息技术安全的管理方向

(a) 部门信息技术安全政策

信息技术安全政策须订定安全规格的最低标准及列明哪些方面对机构至关重要。因此，尽管仍有其他可加强信息安全的可取措施，但信息技术安全政策必须视为强制性基本规则。

决策局 / 部门须以《基准信息技术安全政策》文件为基础，制订部门信息技术安全政策。

部门信息技术安全政策须涵盖妥善使用信息系统、数据资产、网络资源、信息技术服务及设施，以及安全事故预防及应变程序等范畴。拟订政策时须考虑以下内容：

- 决策局 / 部门本身对安全的要求
- 第 2.3 节所列明的现行政府信息技术安全要求
- 《个人资料（私隐）条例》
- 《公开资料守则》
- 《办公实务手册》的档案管理数据

在拟订有关政策时须额外考虑以下内容：

- 香港特别行政区政府的施政目标和方向
- 香港特别行政区政府现行的政策、规则、规例和法律
- 决策局 / 部门本身的要求和需要
- 推行、分配及执行方面的问题

决策局 / 部门应制订程序，迅速为调查违反安全事故的相关工作和政策推行问题提供协助。成立部门信息安全事故应变小组和制订安全事故应变计划可加强政策的成效。

(b) 评估及定期覆检

信息安全政策、标准、指南和程序须定期覆检。覆检的结果和建议的变更须由有关各方评估和批准，以确保已纳入所需的要求。决策局／部门宜考虑外聘合资格的信息技术安全审计师或顾问覆检或协助制订信息安全文件，以提高文件的质素和全面性。

在得不到持续支持的情况下制订的信息安全文件，最终会无人理会甚至过时。事实上，随着时间的流转，有些问题可能不复重要，而新的问题又会不断涌现。因此，经常覆检信息安全文件有助确保相关政策符合部门的最新要求，并能随着科技发展与时并进。

(c) 与用户沟通

决策局／部门须发布本身的信息技术安全政策，并须建立一套政策发布机制，以确保所有人员、功能组别及管理层均能轻易得知有关政策。决策局／部门须确保他们充分认识信息技术安全政策，以便履行职务及切合政府的安全要求。

除非用户或有关各方均作出承担和进行沟通，否则不得将政策视为已落实推行。因此，决策局／部门应确保用户和有关各方：

- 在新加入时已通过简介或入职培训获悉相关政策。
- 获邀参与制订政策建议。
- 已接受遵行政策所需的技能培训。
- 定期获知会及认识安全威胁或问题。
- 已获发分为小篇幅单元的政策指南。

为协助计算机终端用户了解其信息技术安全职责，决策局／部门应以简单易明的实际操作指示形式，制订部门终端用户信息技术安全操作指示文件，概述有关终端用户的安全要求。附录 A 载有一份终端用户信息技术安全操作指示样本，以供参考。

9. 人力资源安全

积极培养深厚的安全文化，对于提升决策局 / 部门的安全态势、降低风险、遵行法规，以及在整个政府内建立一个具复原能力和可信赖的环境，是至关重要的。决策局 / 部门须确保参与政府工作的人员适合担当有关职务，了解他们的职责，并对信息安全风险有所警觉。决策局 / 部门须在新聘、更改或终止雇用过程中维护政府利益。

9.1 新聘、雇用期间或终止雇用

(a) 信息技术安全职责

须在所有人员获派任新职位时，告知他们其信息技术安全职务和职责，并须在他们受雇期内，定期提醒他们有关职务和职责。决策局 / 部门须确保所有人员：

- 在新加入时已通过简介或入职培训获悉部门信息技术安全政策；以及
- 了解他们的信息技术安全职责及政府安全要求，并定期获提醒有关职责及要求。

(b) 信息发布

须设立有效的信息发布机制，以确保全体有关人员充分了解规管其在信息系统使用权限和应用范围方面的相关政策和程序。

(c) 培训

决策局 / 部门须定期向所有人员（包括参与政府工作的用户、开发人员、系统管理员及安全管理员）提供适当安全培训，以及有关信息安全政策的最新数据，加强他们的信息安全意识。培训可以任何形式进行，例如课堂讲授、计算机授课或自学形式（按自己步伐学习）。应提醒用户留意公务员学院公务员易学网（「易学网」）向参加者提供的培训资源，包括与一般信息技术安全有关的教材和自我评核套件。决策局 / 部门根据其业务及运作需要为辖下人员或承包商提供特定的培训计划及教材时宜参考这些培训资源。有关「易学网」的详情，可浏览 https://www.clcplus.csc.gov.hk。

人员亦可以通过参与安全演习和参加研讨会、展示会或浏览载有安全情报信息和一般安全信息（例如网络安全资讯站、资讯安全网）的专页来提高安全意识。决策局 / 部门须参与数字政策办公室指定的信息技术安全意识活动。

应为系统管理员提供有关推行信息技术安全程序的适当指导和培训。系统管理员应懂得如何保护系统免受攻击及被未获授权人士擅用。系统管理员须有一套汇报安全问题的既定程序。

决策局 / 部门应考虑制订信息技术安全培训计划，以便为其员工提供适切和有系统的信息技术安全意识活动。

信息技术安全培训计划应包括但不限于以下内容：

(i) 计划目标

决策局 / 部门应就信息技术安全意识计划制订目标。这些目标应与决策局 / 部门的整体信息技术安全策略一致。

(ii) 对象

决策局 / 部门应识别需要参与培训活动的对象或角色。决策局 / 部门应根据不同的技术专业水平、工作职能和需求来制订培训内容。

(iii) 培训方式

培训材料和内容的设计应配合目标和对象。培训主题的例子包括网络钓鱼意识、事故应变、监管遵行、数据隐私、社交媒体平台意识等。此外，应根据决策局 / 部门的规模、风险、资源和对象的需要，采用适当的培训方法。培训方式可包括演示、影片、互动模组、实践练习和案例研究。

(iv) 评估培训活动成效

决策局 / 部门应检视培训活动的成效。可进行评估以确保人员了解信息安全要求和责任，例如透过培训后测试、意见调查、模拟练习、观察行为变化或安全事故数目等方法，来评估知识增长、行为变化和参与者满意度。

(v) 定期覆检及更新

决策局 / 部门应持续覆检及更新培训计划，以反映不断变化的威胁形势、新技术，以及法规和遵行要求的改变。此外，决策局 / 部门应参考意见调查结果，找出需要改善的地方，并调整或微调培训计划。

(d) 人事安全

保密资料须受到保护，以免在未获授权的情况下被访问或披露。任何人员不得发布、私自复制或向未获授权人士传递其因公职身分而取得的保密文件或资料，除非有关人员基于政府利益而须这样做，则作别论。「有需要知道」原则适用于所有保密数据，这类数据只可提供给有需要和获授权访问数据的人员，以便他们有效执行工作。如对某人员是否获授权访问某份文件、某数据类别或某些数据有疑问，应向部门安全事务主任查询。

决策局／部门须确保人事安全风险已获妥善管理。决策局／部门须评估准许个别人员访问保密资料所涉及的风险。

只限曾接受适当操守审查的公务员才可访问限阅类别以上的保密资料。决策局／部门应就《操守审查训令》咨询部门的人事部。至于非公务员的人员，决策局／部门应根据业务要求、有关人员所处理资料的类别及表面所知的风险，对该等人员进行适当的背景审查。在顾及个人隐私的情况下，背景审查宜包括以下事项：

- 独立查核身分（香港身份证或护照）
- 确认所申报的学历及专业资格
- 检查履历表所载数据是否完整和准确
- 是否有提供工作证明
- 如有需要，详细检查信用或犯罪记录等数据

(e) 清晰的政策及程序

管理人员须就信息系统的使用制订清晰的政策和配套程序，清楚订明信息系统所容许及禁止的用户行为。这些行为一般应在部门的信息技术安全政策订明。部门信息技术安全政策须规定，任何人员如违反政策的任何条文规定，可能受到不同程度的纪律处分或惩罚，但须视乎违反安全事故的严重性而定。决策局／部门须正式通知有关人员他们已获授权访问信息系统，以及其在信息系统方面的职责和职务。

(f) 终止或更改雇用后的信息技术安全职责

须于雇用条款及条件中制订离职后的职责和职务。向人员发出有关终止雇用后职责的通讯须包括延续的信息安全要求和法律责任，以及任何保密协议和雇用条款及条件中所订明离职后特定时间内的职责。职责或职位上的变动，须作为终止现有职责或雇用，然后开展新职责或雇用的安排。

10 资产管理

决策局 / 部门须给予所有硬件、软件及信息资产适当保护，并确保有关数据得到适当程度的保护。

10.1 对资产的责任

(a) 资产清单

资产清单有助作出有效的保护及识别遗失的资产。无论信息系统的资金来源为何，均须为所有信息系统包括基础设施和部门共享信息技术服务（及其系统等级）、硬件资产、软件资产、有效保用证、服务协议和法律 / 合约文件（例如公共域名注册和相关互联网规约地址、数据储存的实体位置等）制订一份列表。清单须定期予以覆检，以确保能妥善持有、保管及维护有关资产。为了更好地管理软件供应链，决策局 / 部门应尽可能收集有关软件资产相关组件的信息（例如供应商、组件名称、版本、依赖关系等）。

部门信息技术安全主任尤其须备存其决策局 / 部门所有与互联网连接的服务的最新清单。清单必须详尽，且至少包括各项服务在互联网上公开的描述、互联网规约地址、域名及开放的网络埠。

在设立资产或从其他各方转移资产时，须编配资产拥有权。资产拥有人须妥善管理资产，以确保：

- 资产被列入清单。
- 资产得到适当分类及保护。
- 资产的访问限制有清楚订明，并获定期覆检。
- 资产的弃置或重用事宜获妥善处理。

(b) 政府信息系统的数据保护

所有人员不得向任何未获授权人士披露信息系统的性质和位置，以及所采取的信息系统控制措施，或执行有关措施的方式。除非按「有需要知道」原则，以及在获部门信息技术安全主任授权的情况下，否则不得披露可能损害信息系统安全的信息系统数据，例如写有互联网规约地址的网络图和安全审计报告。此类数据亦须按保密级别分类及得到保护。

此类数据可能因外聘服务供货商的信息安全管理不足而受到威胁。如需向外聘服务供货商披露此类数据，则须通过不可向外披露数据的协议或同等的措施保护有关资料。不可向外披露数据的协议须制訂不能披露的数据，以及有关各方处理此类数据的方

法。如决策局 / 部门与外聘服务供应机构签订不可向外披露数据的协议，该协议应规定有关外聘服务供货商约束其雇员、董事、代理人、相联者或承包商等负上相同的保密责任。

(c) 交还资产

任何人员如被调职或停止向政府提供服务，该调职或离职人员或外聘服务供货商雇员须将计算机资源和有关数据移交及交还政府。决策局 / 部门须制订一套终止程序，确保之前发出并属其所有的全部资产均已交还。

如离职人员或外聘机构人员拥有关于决策局 / 部门运作的重要知识，该等知识应予以记录并移交有关决策局 / 部门。

10.2 资料分类

(a) 数据分类及卷标

在订立安全措施前，首先应确定需要保护的数据并进行分类，例如有金钱价值的数据，或一旦遗失可导致日常操作受阻的数据。数据的保密级别应按其敏感度划分。

决策局 / 部门应按照数据的保密类别制订保密数据标签及数据处理的程序。决策局 / 部门须遵守及遵从有关数据分类和卷标的要求，例如保密类别的标记、重新划分文件的保密等级及降低文件的级别。此外，决策局 / 部门须遵守以下有关信息系统处理保密数据的要求：

- 信息系统的用户在使用或准备使用信息系统内提供的保密数据时，须获得提示所使用数据的保密类别。
- 保密电邮文件的主题栏必须包括文件的保密类别。
- 存有保密数据的抽取式媒体和盛载媒体的保护盒必须稳固地贴上标签，展示清晰可读的识别记号和显而易见的保密类别标记。
- 存有密码匙的抽取式媒体，若不是用作备份用途，则无须贴上附有保密类别标记的卷标。

(b) 整体数据机密性

不论使用何种储存媒体，所有限阅或以上类别的数据必须加密储存。关于加密方法，决策局 / 部门应采用风险为本的方法评估安全风险，并根据本身的业务需要为信息系统决定合适的安全措施和配置。如系统内有限阅及非保密数据，则不论是以应用系统或其他方式在字段、数据库、档案或硬盘层次为限阅数据加密，亦能符合有关要求。

部分系统，如网络设备（例如防火墙、路由器）及专属设备未必能为其配置、规则集和日志记录此类可能被列为保密数据的数据加密。如没有可行的解决方法，决策局／部门应采取辅助措施，例如加强访问控制，并考虑以此项限制作为理据，取得决策局局长／部门首长批准。

没有列入任何保密类别的数据亦应予以保护，以维持数据的机密性及完整性。向外界公开数据事宜，应由与数据相关的指定工作范畴的负责人员按照《公开数据守则》的原则加以管制。决策局／部门应紧记须确保数据的机密性、完整性和可用性，并应在适当时考虑和推行安全措施，以保障数据在处理、传输和储存时的机密性、完整性和可用性。

类似的保护亦适用于中介数据和在处理过程中产生的数据。在不再使用计算机设备时，必须移除所有政府数据和系统磁盘。

根据数据处理的一般原则，任何形式的保密信息／数据／文件，其保密级别须与书面文件相同，并须按照政府安全要求要求获得相应的保护。

决策局／部门须建议其业务伙伴、承包商或外包人员在储存、处理及传递政府拥有的数据时，必须遵守政府安全要求，并设立机制以检查他们的遵行情况。

10.3 储存媒体的处理

(a) 设备及媒体控制

决策局／部门须管理使用和运送存有保密数据的储存媒体的事宜。为确保数据在运送时得到保护，决策局／部门应：

- 提供足够包装，以免储存媒体在运送途中受到实体损坏。
- 备存记录，以识别储存媒体的内容、所采取的保护措施、送交运输托管人和在目的地接收媒体的时间。

由于流动装置及抽取式媒体体积细小及容易遗失或被窃，如用作储存数据，将存在风险，故应避免把保密数据储存在这些装置内。有关人员应有充分的理据才可使用这类装置储存保密数据，并必须使用由决策局／部门提供的流动装置及抽取式媒体。有关人员应事先得到正式授权，方可把最少所需的保密数据储存在流动装置及抽取式媒体内。为尽量减低数据外泄的风险，应只使用具备适合保护保密数据的加密功能的装置。当无须使用流动装置及抽取式媒体储存保密数据时，所有人员须尽快删除该等装置所储存的保密数据，以尽量减低数据曝光的机会。所有人员亦须确保在弃置或重用该等流动装置及抽取式媒体前，其内所有保密数据均已彻底清除或销毁。

用户未必清楚知悉，一些电子办公室设备（包括多功能打印机及复印机）可能内置储存媒体作为辅助装置。决策局／部门应覆检装置列表，并作出适当安排，确保根据《保安规例》的要求及相关政策、程序与作业模式处理数据。这些设备如有可能用作储存或处理保密数据，使用及管理时须加倍小心。如有需要，应关掉这些设备的档案储存功能，以避免储存任何保密数据。

必须严格按照《保安规例》所订的程序，处理储存保密数据的所有储存媒体。遇有问题，可向部门安全事务主任或政府安全事务主任寻求意见。

(b) 删除数据

在弃置或重用媒体前，须通过(a)净化程序或 (b)实体销毁，把媒体内的所有保密数据彻底清除或销毁，以确保该等数据无法复原：

(a) 净化程序：指彻底删除媒体上的数据，以确保无法读取原有数据的程序。净化程序可通过盖写或消磁完成：

(i) 盖写

对于曾用作储存保密数据的媒体，在弃置或重用前，须通过盖写以删除媒体上的数据。有关程序涉及先以一个字符及其补码盖写所有可寻地址，然后再以一个随机字符盖写和加以核实。删除数据时，媒体储存空间的每一个数元均须进行盖写，这点是至为重要的。就闪存记忆装置（例如固态硬盘或闪存盘）而言，生产商一般会提供内置指令[2]，以有效净化装置，销毁整个磁盘的数据，而非仅盖写或删除加密密码匙。决策局／部门应使用该等功能。尽管如此，如未能核实媒体已获有效净化，以及确保不能再读取原有数据，则须使用其他净化或实体销毁方法。这些方法须能核实媒体已获净化和原有数据不能再被读取。

(ii) 消磁

消磁如使用得宜，不失为销毁硬磁盘、软磁盘及磁带等磁性媒体上的保密数据的有效技术解决方案。为硬磁盘进行消磁时，必须先移除硬磁盘上所有可能干预消磁器磁场的保护物料（例如铸件、机壳及托架）。在消磁过程中，硬盘盘必须保持消磁器指定的某位置或方向。

须实施足够的制衡机制，例如要求进行消磁的个别人士证明消磁工作已完成。此外，须由另一人抽样检查已消磁的媒体，确保消磁工作已办妥。

[2] 建议决策局／部门在采购闪存记忆装置（尤其是固态硬碟）时，考虑是否已具备数据净化功能。

(b) 实体销毁：不能净化的储存媒体须以切碎、解体或研磨等方法作实体销毁。

对于闪存记忆装置，媒体须被切碎或解体成标称边缘尺寸不超逾 2 毫米的碎片／颗粒。

至于光学储存媒体（光盘、数码影像光盘、蓝光光盘和磁光盘），则须切碎或解体成碎片／颗粒：

- 如媒体曾用作储存机密类别以上的保密资料，则碎片／颗粒的标称边缘尺寸不得超逾 0.5 毫米，表面面积不得超逾 0.25 平方毫米；或
- 如媒体曾用作储存机密或限阅数据，则碎片／颗粒的标称边缘尺寸不得超逾 2 毫米。

光盘媒体亦可以通过研磨销毁，以磨掉存有数据的光盘表面。

对于曾用作储存机密类别以上保密资料的媒体，除采用上述程序进行净化外，亦应在弃置有关媒体前作实体销毁。

为遵行有关要求，须使用适当的工具盖写媒体上原本储存了保密数据的储存区。市面上有具备安全删除数据功能的商业软件，这些软件符合在储存区多次盖写的业界良好作业模式，包括以不同形式盖写，以确保彻底删除数据。由于将闪存式固态硬盘或通用串行总线闪存盘内的个别档案完全盖写未必可行，因此应净化整只硬盘而非个别档案，以确保完全删除数据。

可考虑进行加密删除，作为数据净化以外的另一种方法。这种方法会盖写用作加密数据的加密密码匙，但这种方法也容易带来风险，例如加密算法被破解、备份匙未被删除和不能保证数据已被净化。决策局／部门在进行加密删除前，须评估有关风险及潜在影响。在销毁保密数据时，加密删除可与其他净化和实体销毁方法同时使用，而不可只单独以加密删除方式净化数据。

须实施制衡机制，以核实是否已顺利完成安全删除程序。储存媒体应由其他人员抽样检查，以确保所有保密数据已妥为清除或销毁。

用户如认为将要弃置或重用的计算机或储存媒体上存有会引致数据隐私问题的数据，则应采取与删除限阅数据类似的步骤。

如欲获取更多有关销毁及弃置储存媒体的数据，可参考以下文件：

- **销毁及弃置储存媒体实务指南**
  可在政府资讯科技情报网下载
  (https://itginfo.ccgo.hksarg/content/itsecure/techcorner/practices.shtml)

11. 访问控制

决策局 / 部门须防止信息系统被未获授权用户访问及破解，并只容许获授权的计算机资源连接至政府内部网络。

11.1 访问控制的业务要求

(a) 最小权限原则

决策局 / 部门在向用户及技术支持人员分配信息系统的资源及权限时，须确保能遵从最小权限原则。这项原则将用户可访问的信息系统资源（例如数据档案、信息技术服务及设施或计算机设备）或访问的种类（例如读、写、执行、删除），限制在履行其职责所需的最低限度。

(b) 资料访问

决策局 / 部门须确保除非获相关资料拥有人授权，否则不得授予资料访问权限。数据拥有人应订立适当的访问控制规则，以及个别用户职务需要的数据访问权限。访问控制的详细程度和限制应能反映有关信息安全风险。

(c) 保密数据访问控制

任何人士在未经适当认证前，不得访问保密资料。可使用的认证方法有多种，包括密码、智能卡、权标、生物特征和一次性密码。访问储存机密类别或以上保密资料的信息系统，须使用多重认证。

逻辑访问控制是指除实体访问控制（例如限制出入放置系统的地方）以外对信息技术资源的控制。一般来说，逻辑访问控制包括四大元素：用户 / 用户群组、资源、认证和授权。

- 用户 / 用户群组是指已登记及经确定可访问信息技术资源的人员。
- 人员将获授权访问系统资源，例如网络、档案、目录、程序和数据库。
- 认证是指核实用户身分。认证通常基于三个要素进行：用户所知的数据（例如个人辨认号码或用户名称 / 密码）、用户拥有的凭证（例如权标或智能卡）或用户的特征或行为的数据（例如指纹、面部特征、视网膜和声音等生物特征），如采用至少其中两个要素（一般称为多重认证），可加强认证控制。
- 用户 / 用户群组经过认证后，便会获授权访问系统资源。

11.2 用户访问管理

(a) 数据访问控制

须按照「有需要知道」原则授予数据访问权限，并须明确界定、记录和定期覆检。所有行政权限和数据访问权限（包括暂时的访问）均须定期覆检（例如至少每年一次，最好每年两次），以识别和注销不需要或过度的权限。对于部分高权限系统帐户使用情况的定期检查／审计应由独立方进行，以确保这些帐户是为合法目的而使用。此外，亦须备存有关批准和覆检访问权限的记录，以确保各方遵守适当的审批程序，并确保能因应人事变动更新有关人员的访问权限。

数据处理设施（例如放置信息系统的实际场地）的使用权，亦应根据相同的原则管理。

须设立正式的程序，以管制分配信息系统及服务访问权限的事宜。该等程序须涵盖用户访问周期所涉及的各个阶段，由最初的新用户登记、密码提供和密码重设，以至最后的用户取消登记（用户不需再访问有关信息系统及服务）。

(b) 控制特别权限的使用

对于拥有特别访问权限的帐户或用户（例如管理员或系统帐户），以下为限制及控制使用有关权限的规定：

- 须确定每个系统或应用系统所涉及的特别权限和数据访问权限，以及需获分配有关权限的用户。
- 须根据最小权限原则及职务分工向用户授予特别权限和数据访问权限。
- 须将特别权限和数据访问权限授予有别于常规业务活动所使用的用户名称。
- 不得以高权限帐户进行常规业务活动，包括但不限于阅读电邮、浏览互联网和下载档案。
- 应制订特定程序，以防默认的管理员用户名称被未获授权人士擅用。
- 高风险访问应采用多重认证。

(c) 移除访问权限

所有用户权限和数据访问权限（包括暂时及紧急的访问）如在一段预定时间内无任何操作，必须注销。这项要求须由决策局／部门通过系统／应用系统的自动安全检查，或定期的人手覆检（例如检查对上一次登入的时间），确实执行。

此外，须注销不再需要的用户权限和数据访问权限，例如在终止或更改雇用某人员后。确定用户权限和数据访问权限的文件须予以更新，以反映访问权限已被移除或调整。

如离职人员知悉用户名称的密码，而这些名称将需继续使用，则须在终止或更改雇用该人员时更改这些密码。

用户权限和数据访问权限宜授予群组而非个人，例如群组访问清单。在此情况下，决策局／部门须从相关群组访问清单中移除离职人员，并通知各方不要与离职人员分享任何资料。

(d) 用户识别

应建立个人问责制，使相关人员为其行动承担责任。就信息系统而言，可通过使用能识别个别人士的用户名称，当发生事故或发现违反信息技术安全政策事件时，便能够追踪用户在系统的活动，藉此识别及鉴定系统用户，以达到问责的目的。

除非因业务需要（例如示范系统）而无可避免，或无法在信息系统实行，否则不得使用共享或群组用户名称。任何关于这项要求的豁免必须有充分的理据，并须得到部门信息技术安全主任明确的批准。决策局／部门须权衡系统可能遭受的安全风险，提出支持使用共享账户的理据。决策局／部门须定期覆检共享或组帐户的需要，并于理据不复存在时移除账户。

11.3 用户责任

(a) 用户问责制

用户须为以其用户名称进行的一切操作承担责任。用户只可使用其用户名称执行获授权的工作和功能。须禁止未经批准的共享用户名称。有关用户名称的详情，请参阅第11.2(d)节—用户识别。

(b) 共享密码的风险

共享密码会有违用户问责制及访问控制的不容否认原则。除非有一套能确认用户身分以确实执行用户问责制的措施，否则密码不得共享或外泄。如有需要共享密码（例如需要求助台提供协助、与他人共享个人计算机及共享档案），不能确实执行用户问责制，则须给予充分的理由以事先得到部门信息技术安全主任明确的批准。决策局／部门须就系统可能遭受的安全风险说明使用共享密码的理据。共享密码无需使用时应立即重设，需长期共享的密码则应经常更改，以尽量减低违反安全事项的风险。

(c) 密码保护

须时刻妥善保护密码。当储存密码时，须采用访问控制及加密等安全控制措施以保护密码。由于密码是登入系统的关键凭证，因此在不可信任的通讯网络传输时，必须加

密处理。如无法进行密码加密，决策局 / 部门须推行辅助控制措施，例如经常更改密码。

11.4 系统及应用系统访问控制

(a) 数据访问限制

决策局 / 部门须确保信息系统采取适当及与其安全要求和所访问数据的敏感度相称的认证机制和措施。政府已发布《电子认证风险评估参考架构》，旨在提供一致的方式，作为决策局 / 部门就电子政府服务制订合适的认证方法时的参考。该架构务求令市民 / 有关人员在使用有类似认证要求的电子政府服务时有一致的体验及界面。决策局 / 部门在制订和推行其电子政府服务的电子认证要求时，应尽可能遵从该架构。有关该架构的详情，请参阅：

- **「电子认证架构」专页：**
  可在政府资讯科技情报网下载
  (https://itginfo.ccgo.hksarg/content/eauth/index.html)

视乎所需的安全控制程度，使用密码是一个简单的认证方法。应考虑在认证系统使用密码检查程序，以确实执行密码组合准则，并协助用户拣选较可靠的密码，例如避免选取低强度密码或怀疑已外泄的密码。另一种认证方法是使用多重认证（例如智能卡或权标），充当安全容器以识别用户及储存其他安全相关数据（例如加密匙），或一次性密码以提供额外的认证。举例来说，除非用户出示权标（已拥有）及有效密码（已知），否则不能启动受保护的系统。高风险访问（例如远程访问内部网络）应采用多重认证，并应考虑以此作为所有新推行或升级的系统须遵守的标准。对于部分应用系统，可选用质疑 / 应答方案向用户发出一些数据或问题，要求用户准确应答后才能成功登入。

为减低密码因受到如暴力攻击等密码猜测活动而外泄的可能性，须控制连续尝试登入失败的情况，亦须订立及执行尝试登入次数、封锁账户时限及封锁定时器重设时限。在达到尝试登入次数的上限后，账户便会自动失效。此外，亦可考虑采用增长每次连续登入尝试的间隔时间的机制，以防范密码猜测活动。可同时使用用户访问记录分析工具及中央记录服务器，以维持记录的完整性，亦能监察用户访问活动及协助事故调查。

(b) 密码政策

密码即保密的字符串或符号，是用作防止在未获授权的情况下访问数据的安全措施。信息系统可能设有不同类别的计算机帐户，包括为决策局 / 部门用户或使用政府服务的市民而设的服务帐户或用户帐户。决策局 / 部门须审慎地为各类帐户制订密码政策，并记录有关政策，务求在安全要求和运作效率之间取得平衡。密码政策须于所有信息系统上确实执行。

密码政策须至少订明最短密码长度、初次密码设定、受限制字词及格式、密码更改周期的要求，以及一套良好的拣选密码规则，并混合采用其他控制措施，如密码记录、帐户封锁，以及定期更改密码。除非技术上不可行或有真正的实施操作局限，否则最短密码长度须规定为至少八个字元。这些控制措施可减低密码因受到如暴力攻击等密码猜测活动而外泄的风险，并应尽可能推行。密码政策应定期进行审计。

所有载有保密数据的信息系统均须执行以下的严谨密码政策。此外，如任何信息系统被入侵时可能会影响上述系统的安全（例如信息系统与载有保密数据的信息系统共用同一个网络分段、或能够对载有保密数据的信息系统进行管理功能的特定设备），亦须执行以下的严谨密码政策。如以下严谨密码政策的任何控制措施因技术或操作局限而无法推行，须得到部门信息技术安全主任明确的批准，而相关的密码政策调整和理据须予记录。所有其他信息系统亦应尽可能采用以下严谨密码政策。

严谨密码政策：

控制措施	**设定**
复杂度和长度	• 由至少八个字元组成，包括大写字母、小写字母、数字及特殊字符，或 • 由至少十个字元组成，包括至少三個類別的字符 [3]
密码记录	至少记录八个之前使用过的密码
帐户锁定	五次或更少尝试登入失败后
定期更改密码	每六个月或更频繁

(c) 拣选密码

决策局 / 部门应制订一套良好的拣选密码规则，并分发予所有用户。在可行的情况下，应修改设定用户密码的软件，使其能根据部门信息技术安全政策确实执行密码规则。

以下是拣选密码的一些指南：

<u>不应</u>

- 不应使用任何形式的登入名称（原形、倒写、大写、重复等）。
- 不应使用任何形式的本人姓氏或名字。
- 不应使用配偶或子女的姓名。
- 不应使用他人容易取得的其他个人资料，包括身份证号码、车牌号码、电话号码、出生年月日、居所街道名称等。
- 不应使用由相同字母组成的密码，例如“aaaaaa”。

[3] 类别包括 1) 大写字母、2) 小写字母、3) 数字、4) 特殊字符（例如键盘上显示的符号）和 5) (1)至(4)未涵盖的其他字符（例如非英语语言的 Unicode 字符）。

- 不应使用连贯的字母或数字，例如“abcdefgh”或“23456789”。
- 不应使用在键盘上相邻键码组成的密码，例如“qwertyui”。
- 不应使用能够在英语或其他外语词典中查到的单字。
- 不应使用能够在英语或其他外语词典中查到的单字的倒写。
- 不应使用广为人知的缩写，包括决策局 / 部门名称、工程名称等的缩写。
- 不应使用稍为修改以上第 1 至 10 项所述例子后组成的密码。稍为修改的形式包括附加或加插数字或符号，或使用替代字符，例如以 3 替代 E、以$替代 S，以及以 0 替代 O。
- 不应使用少于八个字符组成的密码。
- 不应重用近期使用过的密码。

应

- 应使用由一组冗长且易于记忆的单字组成的密码短句，例如 1Apple&2orange&3banana，以大大增加透过暴力破解密码的难度。
- 应根据不同的安全要求及所需保护的信息资产的价值，于不同的系统使用不同的密码。
- 应使用不容易猜到但方便用户本人记忆的密码，这样便无须将密码写下。
- 应使用无须眼看键盘即能快速输入的密码，以避免行经的人看到所输入的内容。

不当密码示例：

“password”	最容易猜到的密码
“administrator”	用户登入名称
“cisco”	供货商名称
“peter chan”	个人姓名
“aaaaaaaa”	重复同一个字母
“abcdefgh”	连贯字母
“23456789”	连贯数字
“111111”	重复同一个数字
“1q2w3e4r5t”	键盘上相邻键码组成的密码
“qwertyui”	键盘上相邻键码组成的密码
“computer”	在词典中查到的单字
“computer12”	稍为修改过在词典中查到的单字
“c0mput3r”	稍为修改过在词典中查到的单字，例如以“0”替代“o”，以及以“3”替代“e”
“superman”	虚构人物的名字

(d) 密码外泄

决策局 / 部门应提醒有关人员禁止下列可导致在未获授权的情况下访问信息系统或削弱信息系统安全的活动：

- 交互式登录尝试，包括猜测密码及以暴力攻击。
- 通过社交工程或仿冒诈骗获得密码。
- 经监看、观察及使用相机等途径得知密码。
- 以窃听网络通讯破解密码。

(e) 系统 / 安全管理员对密码的处理

不应

- 除非可验证用户的身分，否则不应代用户透露或重设密码。
- 不应将密码储存在可供公开阅读的档案内。
- 不应在未经加密的情况下传输密码予用户，尤其是经电邮寄出密码。

应

- 应根据部门密码政策，拣选适当的帐户初始密码。
- 不同的账户应选用不同的初始密码。
- 在用户收到新密码后，应在技术上强制或要求他们立即更改初始密码。
- 应更改所有系统或由供货商提供的默认密码，包括安装新系统后的服务帐户密码。
- 应在技术上强制或要求用户定期更改密码，或在密码外泄的情况下立即更改密码。
- 在不可信任的网络传递信息时应加密密码。
- 应使用单向功能拼凑密码。在可行的情况下，以「加盐」方式拼凑密码，使同一密码产生不同的拼凑输出。
- 如多次连续登入失败，则应关闭用户帐户。
- 应提醒用户保护其密码的责任。

系统安全功能

以下是一些操作及应用系统所提供较理想的安全功能，这些功能有助执行以上建议的部分拣选密码准则。决策局 / 部门应尽可能启动这些功能。

- 在尝试登入失败次数达到默认上限后自动暂停用户帐户。

- 在账户操作暂停后，规定有关帐户必须经系统／安全管理员人手处置后才能重新启动。
- 禁止用户使用短于默认长度的密码，或重用先前使用的密码。
- 系统／应用系统进行自动安全检查，或信息技术安全管理员定期进行人手覆检时（例如检查对上一次登入的时间），如发现任何账户在一段预定时间内无任何操作，账户须注销或失效。

(f) 终端用户对密码的处理

密码机制与操作系统一样，也存在相同的安全漏洞，即用户拣选不当密码、密码外泄及密码猜测程序。

不应

- 除非备有足够的保护措施，否则不应写下密码。
- 即使有极为充分的理由，也不应透露或出示密码。
- 不应在显示器展示密码。
- 不应（尤其是通过互联网电邮系统）寄出未加密的密码。
- 如网站储存了用户的个人资料（例如身份证号码），用户不应拣选这些网站提供的「记忆密码」功能，而应取消浏览器软件的有关功能，因为可实体访问用户系统的人可访问这些网站所储存的数据。
- 除非有关媒体可阻止未获授权人士访问（例如设有访问控制或加密密码以作保护），否则不应将密码储存在任何媒体。
- 不应将用作加密的访问密码（例如密码、密码短句、个人辨认号码）储存在流动装置。

应

- 应定期更改密码，例如每九十天更改密码一次。
- 在首次登入时应更改默认或初始密码。
- 如怀疑密码已外泄，应立即更改密码。更改密码后，应通知系统／安全管理员，以便进一步采取跟进行动。
- 如因维修及支持服务的需要而向供货商透露密码，则应在维修及支持工作完成后立即更改密码。

11.5 流动信息处理及远程访问

(a) 流动信息处理及通讯

须制订正式的使用政策及程序，并针对使用流动信息处理及通讯设施的风险采取适当的安全措施。有关的使用政策及程序须顾及在没有保护的环境中使用流动信息处理设备的风险。

有关的使用政策及程序应订明实体保护、访问控制、加密技术、备份和抗恶意软件等方面的要求，亦应订定把流动设施连接至网络的规则和建议，以及在公众场所使用这些设施的指南。

须制订及推行有关远程访问的政策、操作计划和程序，并只在以下情况授权用户使用远程访问：已有适当的安全安排和控制措施，以及这些安排和措施均符合安全要求。同时，须就远程访问提供适当的保护措施，例如防止设备和数据被窃的实体保护、防止未获授权人士披露数据的适当访问控制措施、对通过远程访问进入决策局 / 部门内部系统的用户进行多重认证。此外，应向用户提供有关安全威胁的信息，而该等用户亦应承担及确认知悉其安全责任。

(b) 远程访问 / 家庭办公

远程访问或家庭办公用户可随时远离办公地点工作。虽然提高了工作效率，但因用户在非政府处所工作，因此存在安全风险。

决策局／部门不应使用远程访问软件直接连接至部门服务器或用户的工作站。这样使用远程访问软件相当于为攻击者开启了信息系统的后门，让他们能够避开防火墙 / 路由器的保护。为维护政府基础设施和信息资产的安全，各决策局／部门应制订政策，建议用户如何安全地进行远程工作。如因业务需要而使用远程访问软件，须设有适当的安全控制措施，包括但不限于：

- 提供设有严谨端对端安全（例如虚拟私有网络连接、使用个人证书／密码匙作加密保护）的安全网络连接通道
- 限制网络访问控制
- 推行适当的网络管理、分段和监察
- 开启闲置超时控制功能，以避免未获授权的访问
- 开启记录功能
- 监控访问记录以进行暴力攻击分析
- 时刻应用最新的修补程式
- 为有适当认证的登记用户和端点设置白名单
- 维持第 15.1(c)节所订明与其他网络通讯的要求
- 定期检视使用者对远程访问的需求，并移除不再需要的访问权限

尽管有上述规定，决策局／部门不得允许远程访问软件（例如远程桌面软件）透過互联网直接访问政府资源。

对于通过虚拟私有网络连接远程访问决策局／部门内部网络，或经互联网远程访问决策局／部门内部电邮系统，须使用多重认证。

应妥善保护远程计算机，例如安装个人防火墙、抗恶意程式软件及恶意软件侦测及修复措施。所有这些安全功能任何时候均应处于启动状态，并具有最新的恶意软件标识符及定义。此外，亦须为这些远程计算机安装最新的安全修补程序。在这些远程计算机连接至政府内部网络前，应为系统进行全面扫描，以侦测任何恶意软件。

为避免信息外泄，用户应尽量避免在远程或便携式计算机上储存政府数据。保密信息不得在任何私人拥有的计算机、物联网装置、流动装置或抽取式媒体中储存或处理。在一般情况下，不得使用私人拥有的信息技术设备透过虚拟桌面基础设施查看或与限阅信息交互，因为这些装置并不受制于政府的要求。决策局／部门须就此类特殊访问要求评估安全风险和获得决策局局长／部门首长的批准，并定期覆检访问权限，以撤销或限制无真正需求和合法目的的访问。决策局／部门须在技术上或行政上确保对此类私人拥有的装置有效实施完善的控制措施，包括安装有效的防毒软件以防范恶意威胁、启用自动系统更新以确保及时应用最新的安全修补程式，以及实施严谨密码政策以加强访问控制。虚拟桌面基础设施须置于决策局／部门内部网络以外的不同网络分段，并透过多重认证进行访问。应限制从虚拟桌面基础设施进行荧幕撷取和贴上。可以考虑透过使用条款及条件来防止终端用户在装置上对虚拟桌面基础设施进行荧幕截图或拍照。决策局／部门应为访问虚拟桌面基础设施提供设有严谨端对端安全（例如虚拟私有网络连接、使用个人证书／密码匙作加密保护）的安全网络连接通道，并在可行的情况下采用流动装置管理工具来管理装置，以降低中间人攻击和未获授权访问装置的风险。

在公共场所工作时，用户应避免处理敏感文件，以减低把数据外泄予未获授权人士的风险。用户亦应避免使用公共打印机，如需打印，应迅速取回打印文件。此外，用户应使用已设密码的屏幕保护程序，以保护远程计算机，切勿让计算机无人看管。

如远程访问的信息系统载有保密数据，决策局／部门应记录信息系统上的访问活动，并定期覆检，以找出是否有人可能在未获授权的情况下访问系统。

用户在远程办公室使用流动装置时，应参考第 13.2 节—设备的相关指南。

有关在在家工作安排下加强个人资料保障的实用建议，可查阅个人资料私隐专员公署网站。有关实用建议亦适用于其他敏感资料。

- 机构篇
  (https://www.pcpd.org.hk//tc_chi/resources_centre/publications/files/gn_wfh_employers.pdf)

- 雇员篇
  (https://www.pcpd.org.hk//tc_chi/resources_centre/publications/files/gn_wfh_employees.pdf)

11.6 物联网装置

(a) 使用

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。决策局／部门尤其须应备存和覆检那些处理敏感数据或连接至内部／外部网络的物联网装置清单，并作出适当安排以确保按照政府安全要求处理数据。

(b) 使用政策及程序

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物联网装置的风险。有关使用政策及程序应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式和固件升级、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。使用政策及程序亦应包括如何安全地将物联网装置连接至政府网络，以及避免被恶意攻击者控制的规则和建议。

(c) 部署

除非在推行方面在技术上不可行，物联网装置应同样遵从本文件所载对流动装置的安全要求。保密资料不得在私人拥有的物联网装置上储存或处理。此外，物联网装置上不需要的功能应予关闭，以避免收集敏感信息和连接至未获授权的装置或网络。

在访问和管理物联网装置时，应考虑适当的安全控制措施，包括但不限于：

- 推行适当的逻辑访问控制机制，例如更改默认使用者名称和密码、使用严谨的密码和定期更改密码
- 关闭不需要的连接或网络埠，并按需要限制装置连接

- 启用多重认证（如有）
- 加密静止和传递中的保密数据
- 适当管理密码匙，例如避免于多个端点共用加密匙
- 按照产品供应商的建议安装最新的安全修补程式，以进行安全漏洞管理
- 根据最小权限原则和职务分工向用户授予访问权限
- 在物联网装置执行安全启动

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资料。如因为业务需要处理保密资料，须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须将保密资料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（如删除数据和中断网络连接）。

12 加密方法

决策局／部门须确保适当和有效使用加密方法，以保护数据的机密性、真确性和完整性。

12.1 加密控制措施

(a) 数据加密

在传递及储存时，使用加密技术可保护数据并加强机密性。档案加密的模式很多，例如使用程序自备的加密功能、外置硬件设备、保密匙加密和公开密码匙加密等。

应用系统的密码保护功能，主要用于保护档案，防止他人在未获授权的情况下取阅数据。在保护数据机密性时，用户应把档案妥为加密，而非单靠密码保护。使用密码时，须遵行第 11.4(b)节—密码政策及第 11.4(c)节—拣选密码所载有关选择及处理密码的作业模式。

决策局／部门须遵行有关使用加密保护保密数据的政府安全要求。

用作认证或管理的用户密码亦应在储存时进行杂凑或加密。对于杂凑函数算法，应至少使用安全杂凑函数算法 2 (SHA-2)或同级别算法。视乎操作需要，SM3 也可用作杂凑函数算法。除非是旧有系统，否则不得使用安全杂凑函数算法 1 (SHA-1)。如进行加密，用作加密（只限对称密码匙）或解密的密码匙须保密，而且不得向未获授权用户披露。

决策局／部门应进行内部研究及评估，选择最适合其业务需要的解决方案。《资讯科技保安解决方案目录》主题网页提供数个加密方案，作为决策局／部门的参考，用户寻找相关安全方案时亦可以此作为初步的参考。决策局／部门可通过以下连结连接《资讯科技保安解决方案目录》专页。

- **《资讯科技保安解决方案目录》**
  可在政府资讯科技情报网下载
  (https://itginfo.ccgo.hksarg/itsecurity/coss)

(b) 密码匙管理

「密码匙」一词是指用于保密资料认证、解密或产生数字签名的代码。该代码通常以数学算法产生。这些算法常称为「密码算法」，产生的匙称为「密码匙」。

对于机密或以上保密类别的数据，对称密码匙的长度，起码须有 AES 加密法 128 个数元，或相对应的长度。视乎操作需要，SM4 也可符合此要求。而非对称密码匙的长度，则须至少有 RSA 加密法 2048 个数元。此外，根据操作需要，亦可使用密码匙长度最少达 224 个数元或同级的椭圆曲线加密技术，以及 SM2，以符合有关要求。至于限阅资料，亦应采用上文建议的密码匙长度。决策局 / 部门应为存有限阅资料的系统制订升级计划，以符合密码匙长度要求，并定期覆检计划以确保升级过程按预定安排进行。

用作处理机密或以上数据的密码匙必须与所处理的资料分开储存。密码匙可储存在智能卡芯片、权标、磁盘等，并用作认证及 / 或为资料解密。确保密码匙得到保护和管理至为重要。此外，在分发档案时将解密匙与加密档案一并分发十分危险，因为一旦有人取得解密匙，便很容易开启档案。

应根据以下各点妥善记录和执行密码匙管理：

(i) 密码匙产生
- 产生密码匙的设备应得到实体保护。

(ii) 密码匙储存
- 应妥善存放主密码匙，例如将之存放在硬件安全模块或可信任的平台模块，不应把有效的主密码匙带离安全的储存位置。

(iii) 密码匙复原
- 评估是否需要可复原的密码匙。如需要，应只限由获授权人员为密码匙进行复原。
- 密码匙复原密码应受到至少两重独立访问控制作保护，并只限由获授权人员进行数据复原。

(iv) 密码匙备份
- 应为密码匙备份，并采取妥善的保护措施。
- 应明文订立有关访问备份密码匙的程序。

(v) 密码匙传送
- 密码匙不应与数据或载有加密数据的媒体一并传送。

(vi) 密码匙退役

- 应订定密码匙的启用及停用日期，减低因安全威胁（如暴力攻击、职位变动、开放式办公室环境等）而导致密码匙数据外泄的机会。
- 应制订注销及更换密码匙的程序。

(vii) 交易活动记录

- 应以审计追踪记录所有访问密码匙复原密码的活动。
- 应以审计追踪记录所有访问备份密码匙的活动。

在不同加密技术的推行方法中，密码匙可用作加密及解密数据（有时称为数据密码匙），并由另一条密码匙保护（亦称为密码匙加密密码匙）。在这情况下，应根据相关政府安全要求保护最终的密码匙加密密码匙。

13. 实体及环境安全

决策局 / 部门须防止资产在未获授权的情况下被实体访问、破坏、窃取和破解，以及防止对办公场地和信息系统造成阻碍。

13.1 安全区域

(a) 场地准备

由于大部分关键信息技术设备一般放置在数据中心或计算机室内，因此数据中心或计算机室的场地准备工作必须慎重进行。场地准备工作须包括以下几方面：

- 选址及场地规划
- 供电及电力需求
- 空气调节及通风
- 防火、火警探测及灭火
- 水患及水浸控制
- 实体出入控制

首先，决策局 / 部门应参考有关一般要求和良好作业模式的现行选址和场地准备工程指南。这些指南包括但不限于：

- **数据中心设计及场地准备实务指南**
  可在政府资讯科技情报网下载
  (https://itginfo.ccgo.hksarg/content/itop/itm_site_preparation.htm)

决策局 / 部门须根据放置在数据中心或计算机室内的信息系统的保密类别遵行实体安全要求[4]。如办公场地未能符合实体安全要求，决策局 / 部门须按个别情况寻求政府安全事务主任的意见。

如要设置无线通信网络，须先进行场地勘察，确保无线讯号能覆盖预期范围，并决定无线设备的适当摆放位置。

[4]对于在政府物业进行涉及建造或改建房间，以为保密数据提供安全储存的任何建筑或装修工程，决策局 / 部门须参考政府安全要求，并向建筑署说明所需的安全级别，而建筑署须按照订明指南所订的安全级别进行所需工程。决策局 / 部门无需取得指南的详细规格，而且由于安全原因，这些规格通常不会披露。

(b) 防火措施

每更当值操作人员都应组织防火小组，并明确编配各小组成员的职责。必须定期进行火警演习，以便各人员演练发生火警时的程序。

不属防火小组的操作人员须学会使用火警侦测、防火及灭火系统和手提灭火器。

危险或易燃物品应放置在远离办公室的安全位置。文具等大量采购物品不应存放在数据中心或计算机室。在数据中心或计算机室存放的文具用品不应超过一更当值工作所需的数量。

手提灭火器应放在计算机区域的当眼或适当位置，并贴上检验标签及至少每年检测一次。

应安装烟雾侦测器以辅助灭火系统，安装位置应在整个计算机区域较高的位置并处于天花板的下方及／或高架地板的下方。此外，宜安装热能探测器，安装位置应在计算机区域天花板的下方。当发生火警时，热能侦测器应发出警报声。

应优先考虑使用气体灭火系统。如使用液体灭火系统，则宜选择干喉花洒系统而非一般洒水系统。所有灭火系统应每年进行检测。灭火系统应分开处理，以免一个计算机区域内的火警会启动办公室内的所有灭火系统。

(c) 实体访问控制

凡用作进入任何信息系统及网络的密码匙、智能卡、密码等，其实体安全须得到保障，或受到清晰明确及严格执行的安全程序所规管。应教导人员避免在未获授权人士面前输入密码，并在辞职或离职时交还卡匙或访问器件。只有获授权人员才可获知密码及获发磁卡匙，而密码记录必须存放在安全的地方。不应向任何未获授权人士透露卡匙或入口处密码。

所有人员须确保其办公室的安全。如办公室可从公共地方直接进入，则在无人使用时，不论时间长短，均应锁上，以保护其内的信息系统或信息资产。

须备存、保持更新并定期覆检一份获授权进入数据中心、计算机室或其他支持关键作业地方的人士的名单。如情况许可，要求清洁承包商指定专人清洁数据中心或计算机室，并向清洁承包商索取有关员工的个人资料。在维修信息系统期间，必须由负责的人员监督外聘人士施工。

如没有获授权人员陪同，供货商支持人员、维修人员、工作小组或其他外聘人员等访客均不得进入数据中心或计算机室。获准进入数据中心或计算机室的人士须适当地展示身分证明文件，以便识别擅自闯入的人士。同时，须保存及妥善备存访客出入记录

以作审计之用。出入记录宜包括访客姓名及其所属的机构、访客签名、到访日期、进入及离开时间、到访目的等。

在计算机区域范围内的所有受监控保护及安全地带须展示清晰显眼的警告，以阻止陌生人闯入。另一方面，数据中心／计算机室与数据控制室之间的走廊（如有）不应对外开放，以免有人暗中从数据中心／计算机室擅取数据。

在计算机区域范围内的所有受监控保护及安全地带应锁上并定期检查，以免未获授权用户轻易进入计算机室。适用的锁包括（但不限于）插销锁、密码锁、电子锁及生物特征锁。

决策局／部门应考虑安装摄录机（或闭路电视）以监控放置关键／敏感系统的计算机区域并记录影像。摄录机的视线范围应覆盖整个计算机区域。摄像记录应保留至少一个月，以便日后在有需要时回放。此外，应考虑在已放置关键／敏感系统的区域安装入侵者侦测系统。

13.2 设备

(a) 设备选址及保护

所有信息系统须设于安全的环境，或由人员看管，以防止被未获授权人士访问。须定期检查设备及通讯设施，以确保其持续可用，并侦测是否有任何故障。在物联网装置方面，须根据物联网装置储存、处理和传递资料的保密类别来执行安全控制措施，以防装置遗失、被盗和遭受破坏。

应适当控制任何人士将信息技术设备带离场地。处理流动装置及抽取式媒体时，决策局／部门须备存一份获授权设备清单，并定期进行盘点，以检查这些设备的状况。另外，决策局／部门须采取出入检查程序或盘点记录措施，以识别被带走的流动装置及抽取式媒体。虽然如此，将信息技术设备带离场地的人员亦不应在公众场所随意放置这些设备，并应在无人看管时将设备锁好，以防遗失及被盗。人员须保管因业务需要而获准使用的物品（如流动装置及抽取式媒体），不应在欠缺妥善安全措施的情况下随意放置业务物品。

为慎防他人非法访问系统，任何人员如需离开工作岗位，须启动工作站的重新认证功能（例如设有密码的屏幕保护程序），或须注销系统或中断联机。工作站如长时间闲置，则须关掉，以防他人在未获授权的情况下访问系统。

须小心放置显示信息系统所载保密数据的屏幕，以防被未获授权人士窥看保密资料。人员应考虑安装屏幕防窥片，以限制屏幕可视角度。

14. 操作安全

决策局 / 部门须确保信息系统安全操作、防范恶意软件、记录事件、和监察可疑活动，以及防止技术性安全漏洞被利用。

14.1 操作程序和责任

(a) 最小功能原则

应把信息系统的配置设定为只提供所需的功能，并且明确地禁止或限制功能、端口、规约及 / 或服务的使用。同时，应审慎覆检所提供的功能及服务，以确定哪些功能及服务可删除。管理员应考虑关闭信息系统内不使用或不需要的实体及逻辑端口和规约（例如通用串行总线端口、档案传送规约、保密外壳），以防止他人在未获授权的情况下连接装置、传送数据或采用隧道技术。

当进行系统强化、分配资源和权限，以及访问网络或网络服务时，须采取最小功能和最小权限两项原则。有关最小权限原则的详情，请参阅第 11.1(a)节—最小权限原则。

(b) 变更管理

须慎重考虑会影响现行安全保护机制的变更。应控制对信息系统作出的任何变更。操作系统及应用软件应受到严格的变更管理控制，和应考虑以下各点：

- 识别及记录重大变更
- 策划及测试变更
- 评估有关变更的潜在影响，包括安全方面的影响
- 建议变更的正式审批程序
- 向有关各方传达变更的详情
- 针对变更失败和不可预知情况的复原程序，包括终止变更及系统复原的程序和责任
- 提供一套紧急更改程序，以便迅速及在监控下执行变更以应对事故

(c) 操作及行政程序

须妥善记录、遵从、维持和定期覆检操作及管理程序，并提供给有需要的用户参阅。此外，应备妥与信息处理及通讯设施有关的系统活动的文件记录，例如计算机启动及关机、备份、设备维护、媒体处理、计算机室管理等。决策局 / 部门应建立、维持及定期覆检信息系统的基本配置。

(d) 容量管理

应监察资源的运用以实行容量管理，并应就有关系统的业务需要订定容量要求。

应为信息系统制订容量管理计划，以概述决策局 / 部门监察、分析和调整信息系统容量的方法和程序。这有助于确保信息技术基础设施有足够的容量来处理目前和规划中的业务工作负载。负责预算的人员应顾及容量管理计划的需求。

14.2 防范恶意软件

(a) 用户的保护措施

为了防范恶意软件的威胁，用户应确保其工作站及流动装置已安装及采取恶意软件的侦测及修复保护措施。此外，有些产品亦可在一定程度上防范间谍软件 / 广告软件。

但是，如没有更新恶意软件定义，保护软件将无法侦测及防范最新型的恶意软件攻击。用户须定期更新恶意软件定义和侦测及修复保护引擎。更新功能应设定为自动更新，而更新频率至少须为每天一次。如无法进行自动更新（例如不常访问网络的流动装置），至少须每周以人手更新一次。用户亦应注意，一些严重的恶意软件也可能不时爆发。如发生上述情况，用户须遵从有关指示，并实时更新最新恶意软件定义，以防恶意软件爆发。

以下是防范恶意软件的安全指南：

- 启动实时侦测以扫描现行程序、执行程序及正在处理的档案是否附带恶意软件。此外，根据操作需要定期对系统进行全面扫描。
- 在使用前，检查储存媒体上的任何档案及经网络收到的档案是否附带恶意软件。
- 避免开启可疑的电子信息，不要点击来源不可信任的划一资源定地址链接，以免被引导至恶意网站。
- 在使用前，检查附件及下载文件是否附带恶意软件。
- 在安装任何软件前，先验证软件的完整性（例如比较校验和值）及确保软件并无附带恶意软件。在安装任何执行程序 / 软件（包括经电子信息收到或自互联网下载的执行程序 / 软件）前，应先得到决策局 / 部门指定人员的批准。
- 应通过主硬磁盘启动工作站。未经允许不得通过抽取式装置启动工作站。
- 切勿使用来源或源头不明的储存媒体和档案，除非已检查并清除储存媒体和档案上的恶意软件。
- 遵从第 14.3(a)节—数据备份及复原的指南，以备份数据。

用户不得蓄意编写、产生、复制、传播、执行或参与制造恶意软件，亦应采取适当的措施防范恶意软件，以保护其工作站及流动装置。

(b) 局部区域网络 / 系统管理员的保护措施

为了防范恶意软件，局部区域网络 / 系统管理员须确保服务器、工作站和流动装置均采取恶意软件侦测及修复保护措施。恶意软件定义应设定为自动更新，而更新频率至少须为每天一次。如无法进行自动更新，局部区域网络 / 系统管理员应至少每周及在有需要时以人手更新一次。

恶意软件侦测及修复保护措施应支持企业管理，从而有助进行中央管理。有关企业管理的更多详情，请参阅第 15.1(b)节—网络安全控制措施。

局部区域网络 / 系统管理员亦应推行以下技术控制措施：

- 所有局部区域网络服务器、个人计算机、流动装置及通过远程访问连接政府内部网络的计算机，都必须开启抗恶意软件保护功能。
- 启动抗恶意软件保护程序，以扫描所有经互联网输入的网络通讯。通讯闸的配置应设定为可阻截、隔离及删除含有恶意内容的网络通讯，以及建立审计记录以供日后参考。
- 就发展中或用作测试的计算机设备及软件，均应考虑信息安全事项及推行相关程序。除非已推行妥善的控制措施，否则网络环境愈不稳健，便愈容易遭受攻击。
- 有关人员、承包商或外包员工的所有计算机须进行全面扫描后，方可访问政府网络。
- 要求外聘供货商于安装新计算机、维修服务或安装软件后，以最新的恶意软件标识符为用户的硬磁盘进行恶意软件扫描。

在管理服务器时，局部区域网络 / 系统管理员应遵守以下安全指南：

- 通过主硬磁盘启动服务器。如计算机应通过抽取式媒体（例如软磁盘、通用串行总线闪存盘或硬磁盘、光盘等）启动，在启动前必须扫描抽取式媒体是否附带恶意软件，这样可防止服务器受启动扇区计算机病毒感染。
- 通过使用访问控制功能保护服务器的应用程序，例如储存应用程序的目录应设定为「只读」。此外，应按照「有需要赋予」原则赋予最小权限，尤其是「写入」及「修改」权限。
- 考虑运用文件管理解决方案共享文档，并推行适当的访问控制和保护措施。
- 在供用户使用前，应先对所有新安装的软件进行病毒扫描。
- 宜默认文件服务器在开机后自动执行一次全面病毒扫描。
- 遵从第 14.3(a)节—数据备份及复原的指南，以备份数据。

此外，局部区域网络／系统管理员应取得最新的安全警告信息，并教导用户防范恶意软件的良好作业模式：

- 登记接收安全通知／警告信息，以便尽早取得重要的恶意软件警报。
- 立即向全体终端用户转达由数字政策办公室所发出的安全警报，并采取必要的应变措施。
- 教导用户以令其明白大规模恶意软件攻击的影响和了解感染恶意软件的各种途径以免感染恶意软件，例如教导用户一些含有恶意软件的电子信息，可能是仿冒其朋友或同事发出的。

(c) 侦测及复原

以下是一些计算机感染恶意软件的征状：

- 执行程序的时间比正常情况长。
- 可供使用的系统内存或磁盘容量锐减。
- 计算机出现来历不明／新建立的档案、程序或程序。
- 弹出新窗口或浏览器广告。
- 计算机出现异常重启／关机的情况。
- 网络负担增加。

如用户怀疑计算机感染恶意软件，应终止一切活动，因为继续使用怀疑受感染的计算机可能会让恶意软件进一步传播。用户应立即向管理人员及局部区域网络／系统管理员汇报任何怀疑恶意软件事故。如有需要，应通知部门信息技术安全主任，并由信息技术安全主任决定是否安全事故。数字政策办公室中央计算机中心求助台（ccc_hd@digitalpolicy.gov.hk）可为怀疑计算机感染恶意软件事故调查工作提供技术支持。用户亦可在局部区域网络／系统管理员的协助或建议下，使用市面上抗恶意软件的软件，自行清除恶意软件。

移除恶意软件并不代表能够复原或取回受感染或被删除的档案。复原已损坏档案的最有效方法是以原来的档案取代已损坏的档案。因此，档案应定期备份，而且应备存足够备份复本，以便在有需要时复原档案。

将计算机中的恶意软件清除后，用户应对计算机及其他储存媒体进行全面扫描，以确保没有任何恶意软件。忽略重新扫描计算机这一步骤可能导致计算机再次受恶意软件感染。

(d) 使用内容过滤软件

决策局 / 部门利用科技堵截与业务无关的网站时，应权衡轻重。即使信息系统用户能够连接某个网站，也不代表他们已获准浏览该网站。决策局 / 部门应考虑使用网页内容过滤软件防止人员滥用资源，例如从互联网下载大量档案或浏览有害网站。这些活动不仅消耗带宽和浪费资源，亦会增加感染恶意软件的风险。

建立及强制执行一份网站许可名单是一种强效的内容过滤方法。只容许访问有业务需要的网站可减低系统受到攻击的机会。决策局 / 部门亦可通过建立网站黑名单，防止用户浏览那些网站。部分内容过滤工具已装有网页分类数据库，数据库会根据网站内容将网页分类及评分，决定网页是否适合阅览，供货商亦会定期覆检及更新数据库。决策局 / 部门应进行研究，根据本身业务需要决定合适的内容过滤方案。

14.3 备份

(a) 数据备份及复原

决策局 / 部门须定期进行备份工作，并须为本身的信息系统制订及推行备份和复原政策。用户应定期为储存在工作站、流动装置及抽取式储存媒体内的数据进行备份。备份频率应视乎失去数据可用性所带来的影响而定。备份复原测试亦须定期进行。须订定并记录备份审查和复原测试的频率。决策局 / 部门在制订备份及复原政策时，应遵从有关的良好作业模式：

- 应为所有操作数据备存备份复本，以便在这些数据无意中受损或遗失时可以重组。
- 须定期备份，以便将档案复原至最新状态。
- 须定期覆检备份活动。须制订完善的数据备份及复原程序，并设法彻底测试这些程序在实际操作环境的效用。
- 备份复原测试应结合测试备份媒体和相关工具，以及复原程序，并测试复原时间是否符合要求。
- 服务器备份软件应安装在服务器内，以加快数据传送速度，并避免加重网络的传送负荷。此外，软件应可编排在无人操作的情况下工作，以便在非办公时间进行备份。
- 备份复本宜存放在安全及稳妥的地方，并远离系统的所在地。即使发生灾难并摧毁了系统，仍可在其他地方将系统重组。
- 除数据的备份复本外，如还需要软件更新版本才可复原应用系统，软件更新版本（或软件更新的备份复本）及数据备份便应存放在一起。
- 应备存多代备份复本，使复原程序有更大灵活性和弹性。备存备份复本时应考虑实施一套「三代」计划，以确保两份备份复本（即上一代及再上一代的备份复本）总与最新数据及程序操作复本存放在一起。根据最新操作状态备份的更新复本，必须与备份复本一并备存及存放。

- 应至少备存三代备份。然而，如每天备份，则在行政上可能较容易保存六至七代备份。举例来说，星期一的每天备份应保留至下一个星期一，才被盖写。如有需要，档案的月底及年底备份可保留更长时间。
- 应定期测试作备份用途的磁带、磁盘 / 光盘或盒式磁带，以确保在有需要时可复原数据。
- 如使用自动换带机，应注意往返场外存放地点可能需要较长的运送时间，因为磁带不一定会立即移往别处。在操作便利与备份数据的可用性（尤其是重要信息）之间，应设法取得平衡。

在一些不能预计的情况下，如数据在进行备份前被意外删除，或数据所在的硬磁盘因破损而无法利用系统访问，则可能需要硬磁盘数据复原服务。如需要外聘数据复原服务，决策局 / 部门应遵从有关的良好作业模式，以减低数据外泄的风险：

- 尽可能即场进行数据复原服务，并确保承包商在复原过程中留意保密资料的保护要求。
- 陪同承包商人员，并小心留意，确保保密资料不会外泄。
- 净化用作数据复原的装备工具及有关媒体内剩余的用户数据。
- 与承包商签订不可向外披露数据的协议。
- 遵守政府安全要求，尤其是有关外包安全的要求。

(b) 数据备份设备及媒体

须制订适当程序储存及处理备份媒体。须保存一份并未连接信息系统的备份复本，以防止备份数据在信息系统被破解时遭到破坏。在不能实体中断连接的情况下，决策局 / 部门应考虑以逻辑方式中断连接，例如关掉网络装置的端口，或使用配备自动磁带更换装置的磁带库，以机械方式加载及卸除磁带，或备存一份无法被恶意软件（例如勒索软件）访问和更新的备份副本，以确保即使生产系统被入侵，最后一个备份副本也是安全的。

备份媒体的访问须只可通过获授权人士按既定机制进行。未获授权人士不得进入媒体储存库或场外储存室。

须适当记录移入 / 移出数据库或场外储存室的媒体。除非得到批准，否则任何人员不得将任何媒体带离数据中心或计算机室。为方便侦测遗失的媒体，储存架可在空置的槽位附上标记 / 卷标。另须定期进行盘点以侦测备份媒体是否已遗失或遭破坏。

须妥善处理将备份媒体 / 手册运出及运入场地的工作。放置媒体的运载箱应具备抗震、隔热、防水功能，而且应能抵受磁性干扰。决策局 / 部门应考虑加密储存媒体内的数据，并将媒体分成多个部分及由不同人士运送，以防止媒体被盗。

现时有许多设备，例如磁盘、光盘及数码数据储存磁带等，均具备数据备份及复原功能。

磁带是最常用的服务器备份媒体，因应容量而言，磁带的成本相对较低。如数据容量庞大，一次备份需要使用多套磁带，则可使用加载磁带机或自动加载磁带机。为了有效使用换带机，备份软件必须具备支持换带机的功能选项。

由于工作站须备份的数据量一般比服务器的为少，不少设备均可供工作站备份。如要备份的数据量庞大，磁带仍然是成本相对最低的设备。大部分工作站备份软件既支持磁带备份，亦支持抽取式光学储存媒体。

磁带机的磁头应定期清洗。清洗磁头的次数视乎操作环境及操作（备份、回复、扫描磁带等）频率等因素而定。部分磁带机设有显示器，可在使用若干次后提醒用户清洗磁头。有关详情应参阅磁带机的说明书。

应妥善储存及维护备份媒体。应为备份媒体加上适当卷标，并存放在保护盒内及把附有的写保护标签（如有）拨到写保护的位置。备份媒体应存放在远离磁场 / 电磁场及热源的地方，在选择存放地方时应依照制造商所订的存放环境规格。

14.4 记录

(a) 记录的收集及保留

审计追踪显示日常使用系统的情况。视乎审计记录系统的配置，审计记录档案或会显示一连串的尝试访问记录，以得知不正常使用系统的情况。

较复杂的应用系统应具备本身的审计或追踪功能，以便提供更多有关个人使用或滥用应用系统的数据。这种机制实际上是高度安全应用系统必不可少的，因为操作系统的追踪功能不一定有足够的敏感度记录应用系统的关键功能。

虽然审计追踪功能实际上可无限制地记录个人用户访问数据的情况和实际更新次数，但使用记录例程会浪费系统资源，而所产生的记录过多甚至会遮盖不当使用的情况。因此，自行发展的审计追踪应重点记录用户未能成功处理事项及访问未获授权项目的情况。

事项记录可包括但不限于以下数据：

- 在未获授权的情况下的更新 / 访问
- 启动 / 终止日期及操作时间
- 用户识别（非法登入）
- 登入及退出操作（非法登入）
- 连接对话或终端机
- 计算机服务，例如复制档案和搜寻

决策局／部门须根据业务需要和数据的保密类别，制订并记录与信息系统工作记录（包括保存期）有关的政策。有关政策的要求须包括但不限于记录：

- 登入的尝试
- 更改密码的尝试
- 访问关键档案（例如软件配置档案、密码和密码匙档案等）的尝试
- 特别权限的运用（例如新增和删除用户帐户）
- 用户访问权限的变更
- 对审计政策的修改
- 启用或停用保护系统，例如抗恶意软件系统和入侵侦测系统

如未能记录以上活动，须提供理据并予以记录。

已记录的数据最低限度应符合上述要求，以便在发现违反信息技术安全政策事件（例如尝试在未获授权的情况下访问资源）时，审计有关安全措施（例如逻辑访问控制）的成效。记录的详细程度应与业务需要和数据的保密类别相称。除非得到首长级人员的批准，作为审计工作或事故处理所需，否则记录不得用作剖析个别用户的操作情况。

由数字政策办公室或决策局／部门在中央所提供的核准电邮系统和互联网访问服务记录须予记录。在电邮记录方面，栏位须包括但不限于发送日期／时间、客户端的互联网规约位址、寄件者和收件者电邮地址，以及电邮大小总值。其他有用的栏位（如电邮主旨、电邮附件的名称和大小）和事件（如访问电邮包括阅读、删除、未获授权的访问）亦应予记录。在互联网访问记录方面，栏位须包括但不限于访问日期／时间、客户端的互联网规约位址、访问网站或划一资源定位址。

抽取式媒体和打印机如不妥善控制其使用，会构成数据外泄的风险。决策局／部门应防止未获授权而可以通过打印机或抽取式媒体传输保密数据。应采取安全控制措施，包括但不限于堵截未获授权的抽取式媒体（如通用串列汇流排储存装置）的连接、记录列印活动和把档案传送至抽取式媒体的活动。如果现有系统未能推行该等安全控制措施，决策局／部门须视乎系统关键程度、数据敏感度和如发生事故其后的影响，制订推行端点保护解决方案的升级计划，以加强安全保护，以及支援对伺服器、工作站和流动装置，特别是重要信息系统，在使用抽取式媒体和打印机以进行事故评估。

记录保存期须与其作为有效审计工具的日期长短相称。所记录的数据及保存期须足够支持违反安全事项的调查工作。由数字政策办公室或决策局／部门在中央所提供的核准电邮系统和互联网访问服务的记录保存期须不少于六个月。在保存期内，记录须妥为保存以防被窜改，并只可供获授权人士阅读。决策局／部门应考虑以中央记录管理方式管理有关记录。决策局／部门须定期覆检记录保存期及储存容量，以确保记录数据适当保留，并有足够的储存空间。

决策局／部门在制订和覆检内部的记录政策时，应考虑以下各点：

(i) 产生记录
- 需要产生记录的信息技术设备的类别和组件（例如应用系统和数据库等）
- 记录的事件类别
- 每类记录事件的详细数据（例如用户名称、发送的互联网规约地址和时间标示等）
- 时钟同步要求（例如可信任的时间来源、日期和时间的格式、同步方法和频率等）

(ii) 传送记录
- 需要传送记录至中央记录管理基础设施的信息技术设备的类别和组件
- 记录的传送要求（例如网络规约等）
- 传送记录的频率（例如实时、每小时等）

(iii) 储存及清除记录
- 记录的保护要求（例如访问控制等）
- 记录的储存空间
- 记录覆写的准则
- 根据信息系统风险水平订定的记录保存期

(iv) 分析记录
- 职务和职责
- 需要发出警报给负责各方的事件类别
- 需要分析的事件类别
- 记录的覆检频率
- 对可疑及异常活动的处理程序

如决策局／部门使用共享帐户，系统／安全管理员应备存及定期更新共享／组帐户的帐户清单。列表内的数据包括但不限于系统名称、可共享帐户的用户名称（个人姓名）、共享的用户名称、批准的权限、账户有效期及共享账户的理由。如有需要，在进行调查时，帐户清单可用作追踪在特定时间内个别用户利用共享帐户访问特定系统的活动。

载有机密类别或以上资料的系统须启用审计追踪所有数据共用访问。

如在独立个人计算机或工作站的硬盘机储存保密数据，则必须启动审计追踪及记录功能。须根据部门记录政策订定的记录保存期，预留足够硬盘空间保存记录。

应定期（至少每月一次）根据可信赖的时间服务器的时间校准信息系统的时钟。决策局／部门应使用政府主干网络的时钟同步服务或通过网络时间规约使用香港天文台的时间服务器。网络时间规约的认证可加强时钟同步程序的安全。所有设备的系统时间未必完全相同。视乎信息系统的类别和系统对精确度的要求，应将时间的差异控制在合理范围内。具备同步时钟，可使审计追踪能够有可信任的时间标示及更方便地记录事件之间的联系。此外，在调查事件时，审计追踪将会更加可靠。

有关政府主干网络时钟同步服务的资料，可查阅政府资讯科技情报网
(https://itginfo.ccgo.hksarg/content/gnet/servicevas.htm#ntp)

有关香港天文台时间同步服务的数据，可查阅天文台网站
(https://www.hko.gov.hk/en/nts/ntime.htm)

14.5 操作环境的控制

(a) 安装计算机设备及软件

安装计算机设备及软件前，须先得到系统拥有人或负责的管理人员的批准，然后由获授权人员执行。有关设备或软件的安装及连接工作须在不影响现行安全控制措施的情况下进行。有关设备或软件的任何变更，均应作详细记录及经过测试，并应就所有安装和提升项目备存审计追踪记录。

(b) 变更控制

如设施、信息系统，以及业务和安全程序出现会影响信息技术安全的变更，这些变更均须受到控制。须制订更改控制程序及制订相关的职务和职责，以确保变更得到适当控制，并须备存变更记录，以追踪曾作出的变更。除操作环境外，供发展、测试及运作复原的环境亦应有适当的变更控制。变更管理控制详情可参阅第 14.1(b)节—变更管理。

14.6 技术性安全漏洞管理

(a) 漏洞管理程序

决策局 / 部门须进行漏洞管理程序，包括识别、评估、缓解和追踪漏洞。将这些程序整合到常规例程中有助确保任何新漏洞在被利用前得以及时识别和修复。有效漏洞管理亦有助决策局 / 部门有效的管理信息技术安全风险。

(i) 漏洞识别

决策局 / 部门须进行漏洞识别程序，以持续找出其信息系统内的潜在漏洞。此程序应涉及不同的漏洞识别活动，包括漏洞扫描、渗透测试、程式源码扫描、手动程式码审查、配置审查、模拟攻击等，以识别潜在的安全漏洞。另一方面，漏洞识别程序还应包括监控发出安全新闻、警报、报告和其他刊物的来源（例如政府电脑保安事故协调中心），以便及时识别新的攻击方法和未修补的漏洞。此程序中使用的漏洞识别活动也可用于安全风险评估期间的风险识别程序，以识别可能导致信息科技安全风险的漏洞。

(ii) 漏洞评估

决策局 / 部门一旦发现漏洞，须进行漏洞评估程序，以评估漏洞的潜在影响和严重性。此评估应考虑不同数据或系统的敏感性、成功利用漏洞所造成的潜在损害或中断，以及利用漏洞的复杂性等因素。

(iii) 漏洞缓解

决策局 / 部门在评估漏洞后须进行漏洞缓解程序，采取行动及时解决和缓解漏洞。此程序涉及进行完善的修补程式管理程序以安装必要的更新，并调整配置设定以保护信息系统。推行额外的安全控制以防止漏洞被利用，并确保使用授权软件，也是此缓解程序的重要一环。如果无法立即采取缓解措施，决策局 / 部门应推行临时应变方案或辅助控制措施。

(iv) 漏洞追踪

决策局 / 部门须进行漏洞追踪程序，以确保持续追踪和监控已识别的漏洞及其相应的缓解工作。这包括备存漏洞清单、定期更新漏洞状态，以及向部门信息技术安全主任提供定期更新资料。

(b) 漏洞扫描

漏洞扫描是漏洞识别活动的一部分，应在漏洞管理程序中采用。漏洞扫描使用专门的工具有系统地检查信息系统是否存在已知漏洞，目的是在恶意者利用漏洞之前识别漏洞。

决策局／部门须备存漏洞扫描结果和所采取的补救措施的记录。记录有助日后进行安全审计和风险评估。此外，决策局／部门应定期审查和更新其漏洞扫描计划和工具，以确保它们能够有效应对不断变化的威胁和漏洞。

参与漏洞扫描程序的所有人员都应接受适当的培训和支援，以便有效地执行其工作。这包括了解如何配置和使用扫描工具、解释结果，以及修复已识别的漏洞。政府电脑保安事故协调中心的技术中心会为决策局／部门提供漏洞扫描设施，以协助决策局／部门对其与互联网连接的网站进行漏洞扫描。

(c) 渗透测试

渗透测试是漏洞识别活动的一部分，应在漏洞管理程序中采用。漏洞扫描试图在不利用漏洞的情况下发现漏洞，而渗透测试则使用自动和手动技术来发现漏洞并模拟网络攻击以利用漏洞。渗透测试是确保信息系统安全措施有效实施的必要方法，让决策局／部门更了解其系统的弱点，并采取积极措施来解决这些弱点。在对信息系统进行安全风险评估时，还可将渗透测试纳入相应的风险识别程序中，以发现信息系统中的漏洞。

在进行渗透测试前，决策局／部门应明确制订测试的范围和目标，其中包括与渗透测试人员就所使用的方法以及如何报告结果达成协议。渗透测试须从外部潜在攻击者的角度进行，并可涉及主动利用可能有的漏洞。渗透测试须涵盖网络安全、系统软件安全、客户端应用系统安全，以及伺服器端应用系统安全。渗透测试人员还应了解测试的范围和潜在的操作影响。决策局／部门可考虑聘请专门从事渗透测试的外聘承办商来进行这些测试。

可以使用威胁情报以提供对威胁者使用的最新策略、技术和程序的见解，从而提高渗透测试的有效性。这些信息可以指导测试的设计和执行，使测试能够更好地模拟真实世界的攻击，并识别当前和新兴的威胁可能利用的漏洞。

与漏洞扫描的做法相若，决策局／部门须记录所有渗透测试结果和跟进行动。记录对于日后进行安全审计至关重要，可以为决策局／部门的持续安全态势提供宝贵的见解。

有关渗透测试的指南，请参阅《渗透测试实务指南》。

(d) 配置审查

配置审查是漏洞识别活动的一部分，应在漏洞管理程序中采用。配置审查旨在识别可能引入漏洞并危及信息系统安全的潜在错误配置。配置审查可利用自动扫描工具或透过手动审查工作，来确保信息系统的配置正确设定并符合安全良好作業模式。

(e) 源码扫描

源码扫描是漏洞识别活动的一部分，应在漏洞管理程序中采用。源码扫描是指使用自动扫描工具或透过手动程序检查代码，以识别信息系统中的漏洞、错误和安全缺陷的程序。决策局 / 部门应利用源码扫描来识别、分类和订定修复信息系统源码中存在的错误的缓急次序。程式码修改、应用安全编码作业模式和推行安全控制是已识别源码问题的常见缓解措施。

(f) 模拟攻击

由情报驱动和威胁主导的模拟攻击演习，是技术漏洞管理的关键。模拟攻击是漏洞识别活动的一部分，可在漏洞管理程序中采用。模拟攻击演习亦称为红队演习，旨在模仿真实的攻击，以验证决策局 / 部门在安全控制上的整体实力及其抵御实际攻击的能力。演习利用各种方法来测试不同的漏洞点，从社交工程到精密的技术利用不等。渗透测试旨在尝试尽可能发现更多的漏洞，而模拟攻击则是以外部威胁者的角度进行，并有特定的议定目标（例如访问第 2 级信息系统的特定资料库）。

在进行模拟攻击演习前，应先明确界定演习的目标、范围和参与规则。应分析模拟攻击的结果，以评估决策局 / 部门侦测、应对和从攻击中恢复的能力。分析应是全面的，要同时考虑应对的技术和部门层面。应记录调查结果，并提出补救建议。最终报告应详细提供可行的见解，以协助决策局 / 部门加强安全态势。在采取补救措施后，应重新进行测试，以验证已识别的漏洞是否已有效解决。

决策局 / 部门可在模拟攻击中利用威胁情报，例如可以透过威胁情报来改善侦察阶段，因为它有助于根据潜在威胁者的已知策略、技术和程序来识别可能的攻击媒介。这使模拟攻击能够更准确地反映真实世界的威胁，测试决策局 / 部门对最有可能遇到的攻击的防御能力。

另一方面，还有另一种攻击模拟演习，即紫队演习，在模拟攻击过程中还涉及蓝（防守）队。蓝队参与演习旨在了解红队所发现的安全漏洞，并提升决策局 / 部门的整体防御能力。

(g) 修补程式管理

修补程式管理是及时安装软件更新和修复的程序，以解决信息系统中的漏洞和问题。它迅速解决已识别的漏洞，是漏洞缓解的重要一环。

为免有人对已知的安全问题或漏洞作出攻击，局部区域网络 / 系统管理员须在信息系统（包括操作系统、数据库软件、程式库）及在这些系统上运行的应用系统，安装由产品供货商提供的最新安全修补程序 / 修复程序，或采取其他辅助安全措施。决策局 / 部门应确保其局部区域网络 / 系统管理员了解最新推出的安全修补程序 / 修复程序。

有效的修补程序管理程序在维护信息系统安全方面至关重要。随着新发现的漏洞及相应提供的修补程序与日俱增，局部区域网络 / 系统管理员有必要以有系统及管制的方式管理修补程序。

成功的修补程序管理需要一套完善的程序，即修补程序管理流程，当中包括以下多个步骤：

- 取得修补程序 — 选择及下载适当的修补程序，并部署应用。
- 测试 — 进行测试以确定修补程序是否与其他修补程序、主要企业应用系统甚至整个环境「基准」相冲突。
- 风险评估 — 评估与安装修补程序相关的风险及影响，并确定将采取的措施。考虑以下问题：系统应用程序的功能是否会受影响？安装修补程序后是否需要重新启动系统（这会令服务供应受影响）？
- 安装 — 将修补程序安装于目标设备，并确保修补程序仅安装于必需的设备上。
- 遵行要求 — 核实所有设备均运作正常，并符合相关的信息技术安全政策及指南。

此外，修补程序的安装及管理应遵从以下指南：

- 建立及备存决策局 / 部门常用的硬件设备、软件（包括其修补程序管理系统）及其版本号码的列表。这列表对修补程序管理程序至关重要，可方便系统管理员监控及识别相关的漏洞及修补程序。
- 制订与修补程序管理相关的职务和职责，包括漏洞监控及修补等。
- 考虑统一信息系统的配置。统一的配置可简化修补程序测试及安装程序。
- 监控与决策局 / 部门有关的信息技术安全资源的漏洞及修补程序。
- 订定与系统技术配置有关的安全警告信息的应对时间表。
- 一旦确定出现安全漏洞，则应评估相关的风险及制订将采取的措施。
- 定期覆检修补程序管理程序，以评估其成效及效率。

- 在软件供货商的官方网站检查软件产品的终止支持日期，并事先拟备可行的迁移计划。
- 移除已终止支持的软件产品，或升级至其他有安全更新的软件产品。
- 教导用户高度重视信息技术安全及修补程序管理对日常操作的重要性。
- 定期执行漏洞识别，例如使用以主机或网络为基础的漏洞扫描工具，以找出修补程序的不足或系统的错误配置。
- 考虑购买修补程序管理系统，以支持整个修补程序管理周期，从而减轻人手管理工作及减少修补程序安装／测试的时间。应为修补程序管理系统采取适当的安全措施。

当安全修补程式发布时，决策局／部门须评估此安装相关的影响。在此安装前，须测试及评估修补程式，以确保其成效。须通过既定更改控制程序安装安全修补程式。如安装修补程式不可行，则应计划为有关产品进行升级以消除安全问题或推行其他安全控制措施并记录在案。

对于已终止支援的软件，已識別的風險将不再有安全更新可供修复安全漏洞，这样会增加成功入侵系统或网络的机会。如有需要继续使用已终止支援的软件，决策局／部门须评估使用有关已终止支援软件的安全风险，以及采取适当安全措施保护信息系统和相关数据。为了减低已终止支援的影响，应在终止支援日期前至少六个月推行迁移计划，而相关安全措施应于不迟于终止支援日期前实施。迁移计划应包括但不限于使用该等软件的风险评估、计划取代该等软件的日期、使用已终止支援软件时的安全措施（如从部门网络实体隔离、应用系统和通用串列汇流排装置白名单）。

信息系统的风险水平会因应其性质而有所不同，例如供内部使用的信息系统所面对的威胁会较供公众使用并与互联网连接的信息系统为少。决策局／部门须根据风险水平，为信息系统制订适当的修补程式管理策略，包括修补程式检测及使用修补程式的频率。决策局／部门须采用风险为本的方法，考虑每个漏洞的潜在影响和被利用的可能性，以确定每个漏洞的修补计划。所有部署在与互联网连接的信息系统的伺服器和相关装置都须受到严格的修补程式管理。所有已知的与互联网连接的信息系统的安全漏洞应在安全修补程式发布后一个月内修复。一般应优先处理高风险的信息系统。决策局／部门须遵从政府电脑保安事故协调中心发出的安全警报中所订明的建议，以缓解其信息系统的漏洞。

当评估是否使用安全修补程式时，应将漏洞所导致的风险与安装修补程式带来的风险作比较，从而评估与安装修补程式有关的风险。如决策局／部门因任何理由而决定不安装修补程式或并无修补程式可用，便应咨询部门信息技术安全主任，并须妥善记录此事。决策局／部门亦应采取其他辅助控制措施，例如：

- 关闭与漏洞相关的服务或功能
- 调整或加强访问控制
- 加强监控，以侦测或防止实际攻击活动

(h) 使用获授权软件

软件安装控制措施防止未获授权的软件出现潜在漏洞，是漏洞缓解的重要一环。决策局／部门须根据操作需要建立及备存一份获授权软件清单（包括免费软件、开放源码软件、流动应用程式、程式库和相关应用程式）。安装不在获授权软件清单上的软件前，须得到决策局／部门指定人员的适当批准。

至于从互联网下载的软件，决策局／部门必须留意，即使这些软件是合法下载的软件，仍有机会隐藏恶意软件。决策局／部门须从正式途径取得软件，并利用供货商提供的校验和核实软件的完整性。此外，决策局／部门在采用软件前，应考虑以下几点：

- 使用软件／产品的需要
- 产品的过往记录
- 修补频率及产品供货商处理产品漏洞所需的时间
- 可能对决策局／部门带来风险的产品特性（例如将数据与云端服务同步）
- 如软件／产品被入侵，对决策局／部门带来的安全风险
- 软件／产品的技术支持问题

软件资产管理工具的用途是将软件列表扫描及软件计量自动化。软件资产管理工具有助侦查未获授权软件，确保所有软件均得到特许使用权，而且还可反映未曾使用或使用率不足的软件特许使用权数目。决策局／部门应考虑配备软件资产管理工具，协助管理软件资产。

软件资产管理有不同的产品和技术。举例来说，有些桌面操作系统提供备存软件资产清单的工具，以防止未获授权软件载入。决策局／部门应选择最适合本身信息技术环境的软件资产管理工具。决策局／部门亦可委聘服务供货商推行软件资产管理措施、进行软件审计及安装软件资产管理工具。

14.7 信息技术安全威胁管理

(a) 威胁管理机制

决策局／部门须建立威胁识别、侦测和监察机制，并定期覆检机制，以确保其在信息系统性质和技术进步方面的成效。此机制至少须涵盖定期监察信息系统（例如伺服器、虚拟私有网络通讯闸、防火墙）的日志记录，以及决策局／部门相关安全装置（例如抗恶意软件系统、入侵侦测系统、端点侦测与回应解决方案等）所检测到的信息技术安全威胁的迅速应变计划。

(b) 威胁识别和情报收集

威胁情报是为了减少威胁对信息系统造成的危害而收集和分析的威胁相关信息。威胁情报可以是特定攻击的操作细节、有关攻击者策略的信息（例如方法、工具），以及有关不断变化的威胁形势的策略性信息（例如攻击和攻击者的类型）。

决策局／部门须订阅安全新闻、警报、报告和其他信息安全刊物，了解与其业务和日常操作有关的新兴安全威胁和相关风险。政府电脑保安事故协调中心是就即将及已经发生的威胁向决策局／部门发出安全警报的来源之一。决策局／部门也可在威胁情报平台取得威胁信息（例如恶意互联网规约地址和域名）。

决策局／部门应考虑建立一套获取威胁情报的机制，从不同来源（例如政府电脑保安事故协调中心）收集威胁相关信息和分析其对决策局／部门的影响，并将所获得的威胁情报传达给决策局／部门内的有关各方。

(c) 威胁监察及侦测

一旦发现潜在威胁，对信息系统的持续侦测和监控就变得至关重要。须按已订定的检查频率定期检查记录（尤其是处理／储存保密数据的系统／应用系统的记录），除检查记录是否全面外，亦须检查其完整性。所有疑因违反安全事项而引致的不当情况或系统及应用系统误差，均须予以记录和呈报。如有需要，应展开详细的调查。

不同装置内的记录应互相关联，以找出潜在安全事故，以及操作和安全问题。除了应用系统记录外，网络装置及服务器系统记录（例如防火墙记录、网页访问记录、系统事项记录）亦须定期覆检，以侦测异常的情况，包括攻击／入侵系统软件，或针对终端用户的网上应用程序。应就所有在未获授权的情况下访问信息系统的事件作出汇报，并稽查（宜每天稽查）违反安全事件报告。此外，对系统软件亦应制订严格的更改控制程序，以侦测未获授权擅用的情况。

大部分操作系统均设有记录档案。定期检查这些记录档案往往是侦测未获授权擅用系统的第一道防线。以下情况可为侦测在未获授权的情况下访问系统的事件提供线索：

- 大部分用户一般会在每天差不多相同的时间登入及退出。在「正常」时间以外登入的账户可能被入侵者擅用。
- 会计记录（如有）亦可用作判断系统的使用模式；不正常的会计记录可能表示系统被人擅用。
- 应检查系统记录设备，以找出从系统软件发出的任何不正常误差信息。举例来说，在短时间内录得大量登入失败记录可能表示有人尝试猜测密码。
- 以操作系统指令列出执行中的各个程序，有助侦测未获授权用户使用的操作程序，并可侦测入侵者所启动未获授权使用的程序。

利用标准操作系统软件结合多个不相关的程序，亦可制作其他监察工具。举例来说，可使用此方法建立和以离机形式储存档案拥有人及权限设定清单。日后，这些清单可定期重新组合与主清单作比较。如有差异，则显示系统可能已在未获授权的情况下被窜改。

主机入侵检测系统或入侵防御系统可作多方面的分析，以判断是否有滥用（网络内部的恶意或滥用活动）或入侵（外来的违反安全事件）的情况。主机入侵检测系统／入侵防御系统会参考多类记录档案（核心、系统、服务器、网络、防火墙等），与存有已知攻击的共用识别码的内部数据库作比较。入侵检测系统／入侵防御系统还可验证重要档案及可执行文件案的数据完整性。入侵检测系统／入侵防御系统可检查由用户预先选定的保密档案数据库，就每个档案以信息摘要实用程序（例如 sha2sum）制订其校验和。然后，入侵检测系统／入侵防御系统以纯文本文件格式储存校验和，并定期将档案校验和与文本档案的数值作比较。如有任何档案校验和不相符，入侵侦测系统／入侵防御系统便会以电邮、电话、短讯或传呼机通知管理员。

外聘供应商及公共软件下载网站亦有提供其他工具。决策局／部门应根据其目标及具体要求选择合适的安全监察和检测工具。

决策局／部门须在技术可行的情况下，在所有伺服器、工作站和移动装置中部署端点侦测与回应解决方案，以即时识别异常或可疑活动，并就潜在安全事故发出预警。端点侦测与回应解决方案有助即时侦测和应对威胁，减少安全事故的潜在影响。此外，端点侦测与回应解决方案针对网络内的个别装置（例如端点），可供深入了解所采取的每项操作，同时监察流量以识别可疑模式和异常情况。决策局／部门亦可考虑网络侦测与回应解决方案，该解决方案可以持续监察网络流量，以发现安全事故的迹象。

(d) 持续改善和适应

决策局／部门应根据安全事故的经验教训和风险形势变化，定期评估和更新其威胁侦测和监察程序。决策局／部门亦应利用漏洞管理程序中常用的漏洞识别活动，包括漏洞扫描、渗透测试和模拟攻击，以验证决策局／部门检测和应对真实攻击的能力，并将其纳入为持续改善和适应策略的一部分。有关漏洞识别活动的更多资料，请参阅第 14.6 节。

如欲获取更多有关信息技术威胁管理的资料，可参考以下文件：

- **信息技术安全威胁管理实务指南**
  可在政府资讯科技情报网下载
  (https://itginfo.ccgo.hksarg/content/itsecure/techcorner/practices.shtml）

15 通讯安全

决策局 / 部门须确保在政府内部及与任何外部机构之间传送的数据的安全。

15.1 网络安全管理

(a) 一般网络保护

对于网络式或分布式应用系统，多重系统的安全与互连网络的安全同样重要，尤其有关应用系统使用公众人士可访问的宽广区域网络。

在与外部网络连接时，必须权衡有关利弊风险，并宜施加限制，只容许没有储存敏感数据的主机与外部网络连接，并隔离主要计算机。

以下是一些网络保护指南：

- 网络应尽量简单（即把「安全」网络与其他网络的网络界面点减至最低）。
- 只容许获授权的通讯进入「安全」网络。
- 利用多重机制鉴定用户身分（例如密码系统加上预先注册的互联网规约地址及 / 或预先注册的媒体访问控制地址）。
- 在网络传递数据前，使用经证明有效的加密算法为数据加密。

须备存最新的系统或网络数据，特别是网络图、内部网址和配置，显示最新的网络环境，以有效推行安全控制措施。这些数据须适当地分类及稳妥地储存。如把这些数据外泄予未获授权各方，可能会导致违反安全事项，所以须按照「有需要知道」原则只向用户或有关各方披露，并备存适当记录。决策局 / 部门须确保未经事先批准不会公开这些数据。

(b) 网络安全控制措施

除非有运作上的需要并得到部门信息技术安全主任的批准，否则用户不得把未获授权的计算机资源（包括私人拥有及外聘服务供货商拥有的计算机资源）连接至政府内部网络。即使得到部门信息技术安全主任的批准，决策局／部门亦须确保该等计算机资源的使用同样符合相关的信息技术安全要求。

如有需要连接宽广区域网络，可考虑限制所有局部网络的访问都要通过指定的通讯闸，即所有进入或来自局部网络的访问均必须经过指定的通讯闸，这个通讯闸可作为局部网络与外界之间的防火墙。这个系统必须受到严格控制和以密码作保护，其配置应只容许来自外部用户的合法网络通讯访问受其保护的网络。防火墙受到损害可能导致受其保护的网络也受到损害。

此外，应考虑设立双重防火墙，以进一步保护信息系统。此结构使用两道防火墙，包括外部及内部防火墙。外部防火墙保护非军事区不受来自互联网的入侵，而内部防火墙则进一步保护内部网络。就此设计而言，即使外部用户损害非军事区的服务器，内部防火墙仍可保护内部网络的服务器／工作站。

除防火墙系统外，还应考虑为经网络传送的密码引入加密算法，并推行安全程序识别系统，以便分布在网络的应用系统可识别对话的「对象」。

为侦测网络异常活动，决策局／部门须推行入侵检测策略，在网络关键节点安装网络入侵检测系统或网络入侵防御系统。网络入侵检测系统监察网络线路的小包，旨在揭发意图入侵系统（或发动拒绝服务攻击）的黑客／计算机破坏者。一旦入侵检测系统发现系统遭到攻击，便会向信息技术管理员发出警报，从而将系统停机时间及对服务的潜在影响减至最低。入侵防御系统的功能与入侵检测系统相若，然而该系统会采取额外措施主动阻止攻击来源或将攻击的影响减至最低。入侵检测系统及入侵防御系统的配置须调校标识符及识别方式，以减少虚假警报。

决策局／部门须全面承担保护数据、信息系统及网络的责任。决策局／部门须确保信息／通讯系统已妥善配置及稳妥管理，包括关掉所有无须使用的服务和适当地设定安全配置。配置须定期覆检，并在有需要时更新。决策局／部门亦应购置安全软件（如防火墙、恶意软件侦测及修复软件等），以便推行企业管理。企业管理是指有关软件运用中央管理控制台管理机构内所有安全软件，通常具备远程更新、政策实施、状态查询、报告编制、安全功能等特点，可节省政策／标识符／更新所需的调配时间、实施统一标准的机构安全政策、协助进行遵行要求评估，以及减轻局部区域网络／系统管理员及信息技术安全管理员的工作负担。

决策局／部门须将其网络划分为分隔的网域。可以按可信任的程度选择网域（例如公众可访问的网域、桌面网域、服务器网域），并可采用实体或逻辑（例如使用虚拟私有网络）的方式分隔网域。此外，跨网络连接应仅按需要而提供。

每个网域的边界须清晰界定。网域之间可容许互相访问，但应使用通讯闸（例如防火墙和过滤路由器）在网域边界作出控制。把网络分隔为网域和容许通过通讯闸访问的准则，应根据对各网域安全要求的评估制订。有关评估应根据第 11 节—访问控制内有关访问要求及所处理数据的价值和保密类别进行，亦应考虑采用合适通讯闸技术所需的相对成本及对效能的影响。

流动装置通常具备网络连接功能。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，可能导致违反安全事项，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。除非得到部门信息技术安全主任的批准，否则用户不得将其已连接政府内部网络的工作站或流动装置同时连接至外部网络。

在技术可行的情况下，信息系统的管理控制台和管理界面不得直接访问互联网。

在通过无线通信访问保密数据时，应考虑把所有无线访问视为不可信任的连接。因此，使用无线通信访问内部系统须通过指定通讯闸（例如虚拟私有网络通讯闸）进行，并应推行适当的认证、加密、用户层网络访问控制和备存记录。

(c) 与其他网络的通讯

与另一个网络的连接不得导致被连接的一方网络处理的数据安全受到损害，反之亦然。决策局 / 部门须在建立网络连接前，与另一方的决策局 / 部门或外部机构就安全要求进行沟通。决策局 / 部门须制订及推行适当的安全措施，以确保部门信息系统连接至其他决策局 / 部门或外部机构辖下的信息系统时，其安全标准不会有所降低。有关安全要求应依据的原则是，如双方的安全保护级别不同，则双方均采用较严格的安全保护。

一些决策局／部门所实施的安全要求可能较其他决策局／部门的严格（例如客户端程序配置／设置、网络传递要求、用户身分识别及鉴定、对话管理、事项完整性等方面）。有时会出现两个决策局／部门的安全要求不同，但需要互相通讯的情况。如部门间通讯的安全要求存在差异，应遵守以下原则：

- 信息系统提供者的安全要求较其他决策局／部门用户的安全要求严格：

  在此情况下，应以信息系统提供者的安全要求为准，因为作为信息系统提供者的决策局／部门有合理的业务上考虑因素提高其安全要求，其他决策局／部门的用户需要遵从。

- 信息系统提供者的安全要求较其他决策局／部门用户的安全要求宽松：

  在此情况下，信息系统提供者应进行安全风险评估，以厘定是否需要调整其安全要求。如评估结果显示没有需要更改其安全要求，作为信息系统提供者的决策局／部门应与安全要求较高的其他决策局／部门用户协调，为其设置其他访问渠道，或要求这些用户容纳较宽松的安全要求。

  如评估结果显示作为信息系统提供者的决策局／部门需要加强其安全要求，便应相应推行额外的安全控制措施。如在加强安全要求后，仍有其他决策局／部门用户采用比其更高的安全要求，作为信息系统提供者的决策局／部门应与这些用户协调，为其设置其他访问渠道，或者要求这些用户容纳较宽松的安全要求。

当决策局／部门推行信息系统供其他决策局／部门的用户使用时，该决策局／部门应把有关接入要求视作来自不可信任的网络，并根据应用系统的特定要求推行足够的安全控制措施，同时推行额外措施确保用户的行为恰当（例如自动对话超时），而不应假设其他决策局／部门的用户会遵从其信息技术安全政策行事。

(d) 无线通信

无线通信是指在没有连接电线、导线或任何其他形式的电导体的情况下在一段距离上传递数据。无线电话、流动电话、全球定位系统装置及无线计算机等装置，均使用无线通信。无线局部区域网络是政府常用的无线通信技术，是一种利用高频无线电波（而非经线路）在装置之间进行通讯的局部区域网络。无线局部区域网络是一种灵活的数据通讯系统，用以作为有线局部区域网络的替代或延伸。无线信息通讯使人们可以更容易及自由地互动。随着科技日新及价格／性能提高，办公室或公共场所愈来愈广泛应用无线连接。

无线局部区域网络是以电机电子工程师学会订定的 IEEE 802.11 标准为基准。该标准已演化为 802.11a、802.11b、802.11g 及 802.11n 等不同标准，以支持不同频谱及带宽。

IEEE 标准 802.1X 及 802.11i 是互相关连的。802.1X 标准是以埠为基础的网络访问控制规约，为 IEEE 网络（包括以太网及无线网络）提供安全架构。802.11i 标准则针对无线安全功能而制订，与 IEEE 802.1X 共同运作。

使用无线通信接驳政府内部网络时，须采取充分认证及传递加密措施，并辅以适当的安全管理程序及作业模式。

(e) 无线局部区域网络面对的威胁及安全漏洞

无线信号的特点是有关信号普遍在无线局部区域网络的覆盖范围内通过空气传输，并可穿越建筑物的墙壁及窗户。因此，除非已采取安全措施保护无线传递不被「窃听」，否则会带来任何人也可截取及阅读这些信号的潜在安全风险。事实上，无线局部区域网络面对的风险，相等于运作有线网络的风险，加上无线规约的漏洞所引致的新风险。以下是与无线局部区域网络相关的一些风险：

- 怀有恶意的人士可通过无线连接，并有可能避开防火墙，在未获授权的情况下访问政府内部网络及发动攻击。
- 计算机恶意软件可破坏无线装置内的数据，继而影响有线网络的运作。
- 怀有恶意的人士可利用未获授权设备（例如客户装置及无线接驳点）暗中访问或窜改数据。
- 未经加密（或采用较弱的加密技术加密）的保密数据在无线装置之间传递时或会被截取及外泄。
- 拒绝服务攻击可能会针对无线连接或装置发动。
- 可能有虚假的无线接驳点被建立，以获取无线局部区域网络内传送的数据。

无线局部区域网络技术日新月异。决策局／部门须定期覆检其 Wi-Fi 基础设施，以评估在 Wi-Fi 通讯标准和规约所发现之安全漏洞的影响。政府应考虑采用较强的无线安全规约如「无线保护访问 3」，以保护无线局部区域网络。由于日后可能在这些规约发现新的漏洞，故不能只依赖这些无线安全规约作为保护调制解调器密性及完整性的唯一措施。决策局／部门如需通过无线局部区域网络传输保密数据，应在无线局部区域网络之上设置虚拟私有网络。

(f) 保护无线局部区域网络的安全控制措施

决策局／部门应注意，除使用技术安全措施保护其无线局部区域网络外，还须采取适当的管理控制措施以有效保护其无线局部区域网络。以下是一些管理及技术安全控制措施，以供参考：

管理控制措施

- 就无线局部区域网络的使用及可经无线局部区域网络传递的数据类别制订无线安全政策。
- 制订及妥善备存无线局部区域网络的覆盖图，涵盖相关无线接驳点的位置及服务设定标识符数据，避免无线信号的覆盖范围过大。
- 确保硬件及软件得到妥善修补及更新。
- 定期搜寻虚假或未获授权的无线接驳点。
- 定期进行信息技术安全风险评估及审计，以找出安全漏洞。
- 妥善备存所有配置无线界面的装置的记录。某装置一旦被报失，应考虑更改密码匙及服务设定标识符。
- 推行严格的实体安全控制措施及鉴定用户身分，以弥补无线装置实体安全的不足。
- 在远离门窗的位置安装无线接驳点，以防止网络在可公开进入的地方被窃听。

技术控制措施

- 在安装时更改网络默认名称。服务设定标识符不应包含任何决策局／部门的名称、系统名称或产品名称／型号。
- 更改产品默认的无线接驳点配置设定。为方便设置，有关默认配置设定在大部分情况下视为不安全。
- 关闭无线接驳点上所有不安全及未使用的管理规约，并以最小权限配置所需的管理规约。
- 确保所有无线接驳点均有严谨而独立的管理密码，并定期更改密码。
- 开启及配置安全设定，包括服务设定标识符、密码匙和简单网络管理规约的社群字符串。
- 关闭服务设定标识符广播功能，以免无线接驳点广播服务设定标识符，只有配置与无线接驳点服务设定标识符相符的获授权用户才可与网络连接。

- 关闭动态主机配置协议服务器，并向所有无线用户指派固定的互联网规约地址，从而将未获授权用户取得有效互联网规约地址的机会减至最低。
- 配置无线接驳点时使用媒体访问控制地址过滤功能，使只有具有特定媒体访问控制地址的客户才可访问网络，或只容许访问一系列设定的媒体访问控制地址。
- 切勿直接连接无线局部区域网络和有线网络。在无线接驳点与决策局／部门网络之间安装防火墙或路由器，并使用访问控制名单，以过滤连接。
- 启动基本参数，例如静止暂停。
- 启动记录功能，并在可行的情况下把所有记录转移至远程记录服务器。有关记录应定期检查。
- 安装无线网络入侵检测系统或无线网络入侵防御系统，以监察无线局部区域网络。
- 在无线局部区域网络之上设置虚拟私有网络，以连接部门网络。
- 对于 Wi-Fi 防御功能有限的流动装置，应使用客户端数码证书，使只有获授权的装置才可访问部门网络或资源。
- 把无线接驳点的覆盖区域分段，以平衡网络负荷及减低受到拒绝服务攻击的可能性／影响。
- 弃置无线组件时，删除有关装置所载的所有敏感数据，例如系统配置、共享密码匙、数码证书和密码。
- 关掉无线接驳点的通用即插即用功能，以防止恶意软件通过连接的装置绕过防火墙。

<u>终端用户控制措施</u>

- 在无线客户端（例如流动装置）安装防火墙。
- 关掉无线客户端的共享或网络共享功能。
- 已连接第三方无线局部区域网络的无线客户端不得同时连接部门网络。
- 通过虚拟私有网络连接部门网络资源。
- 严格控制无线界面装置（例如膝上计算机的通用串行总线权标），因为访问凭证（例如服务设定标识符及／或密码匙）通常储存在卡内。
- 只在用户需要时才开启无线连接，不需要时则关闭。
- 遵从第 14.2 节—防范恶意软件和《流动安全实务指南》第 4 节—流动装置安全的指南。

(g) 通过无线通信的传递

无线局部区域网络通常被视为不可信任的网络，如无适当的安全控制措施，不得用于传递保密数据。无线局部区域网络与内部可信赖网络之间的网络通讯必须经过加密及认证。采用虚拟私有网络是达致这种端对端安全的可行方法。

下表简列各类数据使用无线通信进行传递的适用范围。

数据类别	使用无线通信传递数据的适用范围
机密以上	不可使用
机密	可使用，但必须得到决策局局长／部门首长的批准并以指定装置传递数据，以及有足够的认证和传递数据加密安全控制，并达到机密数据必须达到的加密水平。 应使用虚拟私有网络，以加强无线局部区域网络连接的认证和加密功能。此外，亦须制订适当的密码匙管理及配置政策，以辅助技术方案。 如果无线键盘能够符合在认证及加密方面的行业安全标准，并且经部门信息技术安全主任确认符合规格，则无需获得决策局局长／部门首长的批准。
限阅	可使用，但必须有足够的认证和传递数据加密安全控制，并达到限阅数据必须达到的加密水平。 宜使用机密数据必须达到的同一加密水平，并制订与机密数据相似的适当密码匙管理及配置政策。
非保密	可使用。在遵从只有获授权人士才允许访问储存数据的网络的原则下，具备足够及适当的认证和传递数据加密措施的无线通信可视作适合决策局／部门使用。 与机密及限阅数据一样，亦须制订适当的密码匙管理及配置政策，以辅助技术方案。

(h) 互联网安全

互联网是由全球计算机网络互相连接而成的网络，通常使用传输控制规约／联网规约组进行通讯。连接互联网使获取信息的途径更为广泛，从而带来很多好处，不过，互联网广泛存在严重的安全问题。

根本问题是互联网的设计并非十分安全。很多传输控制规约／联网规约服务很容易受到安全威胁，例如被偷听及仿冒，利用现成的软件便能够监察并撷取电子信息、密码及档案传送。

互联网服务需要更严格的认证和加密机制，而这些机制须做到真正兼容。为落实政府互联网资源的真确性，政府互联网网域的资源记录须受现行的安全控制措施（即域名系统安全扩展）所保护。同样，就互联网邮件服务而言，所有发给市民的政府互联网邮件须受现行的电邮真确性标准保护，包括「发件人策略框架」、「域名密钥识别邮件」或「网域型邮件验证、报告与一致性」规约。此外，所有互联网服务（包括资讯网站）须推行加密传递，例如超文本传输安全规约，以加强政府互联网服务的真确性和内容

完整性。互联网数据查询或事项处理须鉴定用户身分，为安全访问起见，可能须采用一次性密码和进行多重认证，认证数据也须进行审计和备份。

一般来说，互联网安全涵盖广泛的课题，包括识别及认证、防范恶意软件、软件特许使用权、远程访问、拨号访问、实体安全、安装防火墙，以及与使用互联网相关的其他范畴。

因此，决策局／部门应通过定期和特设的培训以提高人员对信息安全的意识，并着眼于妥善使用互联网服务。所有人员须知道不当使用互联网可能会带来安全风险，这些风险有可能危害政府信息技术基础设施和／或对政府声誉造成负面影响。此外，所有决策局／部门的人员在使用政府提供的互联网服务时应了解其义务和责任，并严格遵从政府所提供互联网服务的使用条款。

使用个人网络邮件、公共云端存储和网络版即时通讯服务会带来重大安全风险，包括在传输过程中可能发生未获授权泄露敏感资料和数据外泄。因此，决策局／部门须定期审慎检视使用者访问这些服务的必要性。只有当有真正的需要和合理理由，并且获决策局局长／部门首长或他们明确授权的首长级人员批准时，才可授予访问权限，并在不再有需要时立即撤销有关权限。决策局／部门应采取技术控制措施，例如网页内容过滤，以防止未获授权访问个人网络邮件、公共云端储存和网页版即时通讯服务。

如果订阅服务遭受破坏，订阅线上服务中使用的政府电子邮件地址及政府信息系统中使用的密码可能会让攻击者获得访问系统的权限。订阅中提供的其他信息也可能外泄，以及被用于网络钓鱼活动和网络攻击。虽然订阅网络服务可能确实有需要，决策局／部门应不断提醒用户相关风险，并提倡采用安全良好作业模式，例如使用严谨而独有的密码、谨慎处理个人资料、启用多重认证（若有的话），并对网络钓鱼保持持续警惕，以及在线上服务订阅使用电子邮件别名。

(i) 通讯闸保护

所有支持互联网设施的决策局／部门均须保护其数据和数据资源免在未获授权的情况下被访问或被公众人士入侵。部门网络必须通过中央安排的互联网通讯闸或决策局／部门内部的互联网通讯闸访问互联网。通讯闸利用屏蔽路由器、防火墙或其他通讯设施可同时提供安全和认证保护。除特定开启的功能外，互联网通讯闸应拒绝其他所有互联网服务。所有不使用的配置、服务、端口及不必要的通讯，例如不需要的日间服务、传入或发出的互联网控制信息规约(ICMP)通讯等，亦应被终止或堵截。不应直接拨号连接互联网服务供货商。有关互联网通讯闸安全的技术指南详情，请参阅以下文件：

- **《互联网通讯闸安全实务指南》**
  可在政府资讯科技情报网下载
  (https://itginfo.ccgo.hksarg/content/itsecure/techcorner/practices.shtml)

决策局／部门如决定在独立计算机（即没有连接政府或部门网络的计算机）安装不经过中央安排的互联网通讯闸或决策局／部门内部的互联网通讯闸的宽带连接，便须在这些独立计算机推行足够的安全控制措施，例如防火墙、抗恶意软件程序、限制用户权限等，以避免可能发生的违反安全事项和滥用系统事故；同时亦须实施适当的审批及控制机制。除已采取适当的安全保护措施并已得到部门信息技术安全主任的批准外，任何计算机须严禁同时以宽带连接互联网和访问内部网络，因为这样会对政府网络构成严重威胁。

为减低用户访问钓鱼网站或含有恶意内容的网站的风险，决策局／部门须拦截用户访问任何已知或怀疑有恶意的互联网规约地址或网站。

(j) 客户端保护

个人防火墙可有效保护用户的工作站，以阻截未获授权的网络通讯，防御如网络蠕虫入侵或其他形式的恶意软件攻击。在用户工作站安装的个人防火墙，为工作站与网络之间提供防火墙服务。个人防火墙在容许网络通讯进入或输出用户工作站前会查询用户授权，藉以控制网络通讯。一些个人防火墙甚至提供应用系统层保护，确保只有获授权的程序在用户工作站运行。

局部区域网络／系统管理员须在有机会直接连接互联网或第三方网络等不可信任网络的计算机安装个人防火墙。大部分个人防火墙适用于独立配置或代理配置，上述配置可集中管理及实施个人防火墙政策。

除考虑个人防火墙保护外，应适当配置在用户工作站运行的互联网浏览器。由于互联网浏览器是连接互联网的主要界面，互联网浏览器配置不当可能会让恶意软件下载至用户的工作站。决策局／部门在配置互联网浏览器时可参考下列指南：

- 除与可信赖来源通讯外，关闭电子信息应用系统或浏览器的 Java、JavaScript 及 ActiveX 等活动内容选项。
- 使用最新版本的浏览器，并安装最新的安全修补程序。
- 关闭自动输入密码或密码记忆功能。
- 除与可信任网站通讯外，启动拦截弹出窗口功能。
- 定期删除浏览器内的缓存文件或临时档案，以保障数据隐私。
- 关闭自动安装插件、附加组件或软件的功能。

向用户推行教育及认知培训亦十分重要，以提醒用户使用适当配置的互联网浏览器的重要。

15.2 数据传送

(a) 传递保密数据

机密类别以上的保密资料必须经过加密处理，并只限于在已获数字政策办公室技术审核及政府安全事务主任批准的独立有线局部区域网络内传递。独立的局部区域网络是指在受监控的单一环境中，没有与其他网络（包括其他政府网络、互联网和远程访问）连接的局部区域网络。

机密／限阅数据在任何通讯网络上传递时应加密，以作保护。机密／限阅资料在不可信任的通讯网络上传递时则必须加密。不可信任的通讯网络包括：

- 互联网
- 使用公共电讯线路的网络（例如租用线路、拨号连接）
- 无线通信
- 都会以太网

可信任的通讯网络应具备以下条件：

- 存放地点受到严密的实体保护，以免经过网络传输的数据被未获授权人士访问、窜改或删除。
- 受到严密保护，例如通过锁上网络设备及保护局部区域网络端口，以免被未获授权人士破坏。
- 制订清晰明确的信息技术安全政策，以控制对网络设备及设定的适当配置和管理。

不符合可信任通讯网络定义的网络被视为不可信任的通讯网络。一般而言，在任何通讯网络传递数据都有安全风险，因为恶意攻击者可撷取保密数据，甚至利用通讯网络的安全漏洞入侵政府网络。决策局／部门应进行安全风险评估，以确定正在使用的通讯网络是否可信任，并识别相关风险。决策局／部门应考虑在数据、应用系统或网络层面进行加密，将在未获授权的情况下被访问的风险减至最低。

(b) 电子信息安全

电子信息（例如电邮、实时通讯）是供内部及外部通讯的一项主要应用科技。政府内部网络有多种电邮产品供内部用户使用。用户须提出正式申请才能使用电邮账户。互联网的电邮与内部网络的电邮一样，应支持认证、加密及数字签名等功能。载有保密数据的电子信息在传递或储存时必须加密。

除非因业务需要而无可避免，否则应限制使用公共电邮。如传递载有保密数据的电子邮件，必须通过已获政府安全事务主任批准的信息系统传递。在内部通讯方面，「政府内部机密邮件系统」、「机密信息应用系统」、「机密电邮流动服务」和「中央管理通讯系统」中已获批准的子系统是政府的指定电邮系统，以便在政府网络内交换机密类别的电邮信息和文件。在互联网交换电邮，不论是否已签署或加密，都不能假设已达到与「政府内部机密邮件系统」或「中央管理通讯系统」相同的安全程度，因为互联网电子信息服务未必符合有关处理机密数据的政府安全要求。有关「政府内部机密邮件系统」和「中央管理通讯系统」的配置和操作程序，请分别参阅载于政府内联网数码政府合署网站：http://cms.host.ccgo.hksarg/和 https://itginfo.ccgo.hksarg/content/cmmp 的相关文件。

(c) 电邮服务器和客户端的安全

在连接互联网前应适当地配置电邮服务器及客户软件。以标准的简单邮递传送规约传送的电邮不会进行完整性检查，互联网电邮地址可轻易被仿冒，以互联网传递电邮一般没有保障。如技术上和运作上可行，电邮的标题应避免透露内部系统或配置的具体数据，以防止把系统数据外泄予外部机构。

决策局／部门可考虑就访问电邮的任何活动进行审计追踪，以记录获授权及未获授权用户尝试阅读或更新电邮的每项活动。须订立有系统的程序，以记录、备存及删除电子信息及备存清晰的记录。应使用警示报表或警报报告安全事故。此外，获授权的管理员必须妥善备存和保护用户电子邮件通讯簿，以免在未获授权的情况下被访问或窜改。

为加强政府电邮系统的安全，用户须为其工作站及电邮帐户设置密码等认证功能，以免在未获授权的情况下被访问和使用。

不应让电邮客户端自动处理附件，因为附件可能含有恶意手稿程序或恶意软件。有关详情请参阅第 15.1(j)节—客户端保护。

局部区域网络／系统管理员应为使用政府电邮系统的用户安排自动更新恶意软件定义。用户应确保每当使用系统访问任何档案或数据时，均已开启其工作站内的抗恶意软件自动防护功能。有关详情请参阅第 14.2 节—防范恶意软件。

用户应保护及定期更改其密码。用户不应打开或转寄任何来历不明或可疑来源的电邮。如用户怀疑或发现电邮附有任何恶意软件或可疑内容，应立即向管理人员及局部区域网络／系统管理员报告有关事故，并遵从相关事故应变计划。如有疑问，用户也应透过其他途径（例如透过电话）验证电子邮件寄件者的身份。

此外，除非能够确保外部电邮系统安全，否则用户不应设定把公务电邮自动转寄至该系统，因为一些包含保密内容的电邮也可能会一并自动转寄出去。如在没有加密的情况下自动转寄这些包含保密内容的电邮，可能违反有关传递保密资料的政府安全要求。此外，不受政府直接控制的电邮系统，会为所储存的数据带来额外安全风险。

有关政府电邮系统的电邮管理及电邮安全详情，请参阅以下文件：

- **《使用电子邮件实务指南》**
  可在政府资讯科技情报网下载
  (https://itginfo.ccgo.hksarg/content/imx/email_practice_guide.asp)

(d) 与外部机构通讯

与外部机构（如非政府机构、政府相关组织、外包人员或外聘服务供货商）的网络通讯应视为不可信任。各决策局／部门在通讯网络与外部机构连接或交换数据时，应遵从相关的信息技术安全政策，并根据应用系统的特定要求推行足够的安全控制措施。

向外部机构提供数据时必须遵守「有需要知道」原则。决策局／部门须确保有关保护保密数据的安排尽量符合政府内部所采用的标准。

必须制订及记录有关决策局／部门与外部机构之间安全传送保密数据的协议。与外部机构达成的数据传送协议应至少包括以下各点：

- 不可向第三方披露保密资料或视乎情况向政府作出弥偿的责任。
- 保护保密数据防止在未获授权的情况下被访问的措施，例如数据加密和访问控制。
- 发生信息安全事故（例如数据外泄）时的责任和义务。
- 记录或阅读保密数据的技术标准。

应制订及备存相关的政策、程序及标准，以保护在传输过程中的数据及实体媒体。这些文件应在数据传送协议内提及。

16. 系统购置、发展及维护

决策局 / 部门须确保信息安全在信息系统的整个生命周期中都是重要的一环，并且尽可能隔离发展、系统测试、验收测试和实际操作等不同环境。

16.1 信息系统的安全要求

(a) 设计层面的安全

设计层面安全的概念对识别应用系统的潜在风险，并在发展 / 购置系统前进行适当补救工作尤为重要。完善的应用系统设计不仅针对用户的问题提出可行的解决方案，更为用户提供安全的操作环境。在系统发展初期以至各个阶段，均应采取措施加强安全及保障隐私，并善用操作系统所提供的安全设施。此外，应用系统本身应视乎系统的安全漏洞和关键性，以及所处理数据的敏感度，内置额外的安全措施。

安全左移方法在整个系统发展生命周期的早期和整个过程中整合了安全考虑因素，以确保适当地识别和纳入必要的安全要求。决策局 / 部门应考虑实施安全左移方法，包括采用安全编码作业模式，以及在系统设计阶段对其信息系统进行安全审查。

决策局 / 部门应在新信息系统或现有信息系统改善计划的要求中制订有关信息技术安全的要求。如能清晰制订安全要求，并于早期阶段处理已识别的风险，预计可大大减少重做系统所需的工作。决策局 / 部门应在信息系统发展周期的设计时间进行安全覆检作为检查点，以确保已识别所需的安全要求，并适当地纳入于系统设计阶段或其他阶段。

有关覆检应根据业务需要、法例和规管要求（例如《个人资料（私隐）条例》），以及政府的安全要求评核有关安全要求，并参照应用系统设计和发展阶段的安全考虑，识别可能出现的遵行问题及安全风险，藉此覆检系统设计。在覆检后，应适当地记录及在设计或其他阶段处理所识别的风险及建议。覆检时应在发展小组中加入一项职务，以评估安全风险、提出潜在的安全问题，以及进行系统设计及程序编码的安全覆检。为确保所需的安全措施和控制措施均已在系统内妥善推行，投产前的安全风险评估应在生产推出之前核实已完成安全覆检的跟进行动及程序编码的覆检。

有关设计层面的安全的更多信息，请参阅以下文档了解详细信息：

- **《设计层面的安全实务指南》**
  可在政府资讯科技情报网下载
  (https://itginfo.ccgo.hksarg/content/itsecure/techcorner/practices.shtml)

(b) 系统规格及设计控制

在系统规格及设计阶段，应进行以下检查：

i) 确保所设计的系统符合可接受的会计政策、会计及应用系统控制措施，以执行足够的认证、授权及问责，以及符合所有适用的立法措施。

ii) 确保已建立威胁模型，并在所有设计及功能规格中加入可减低威胁的措施。另外，可通过分析应用系统中较高风险的进入点和数据，建立最基本的威胁模型。

iii) 与用户共同覆检系统设计，检查在维持数据的完整性方面是否存在任何漏洞。应鼓励用户就所发现的任何漏洞建议修正措施。

iv) 与用户共同评估数据处理能力损失时对用户的影响。评估后应制订应急计划。有关制订应急计划的详情，请参阅第19.1(a)节—应急管理。

v) 与资料拥有人共同评估数据的敏感度，须探讨的数据包括：

- 达到的安全水平
- 数据来源
- 容许用户部门各级人员访问的数据字段
- 容许用户部门各级人员处理计算机档案内数据的方式
- 达到的审计功能程度
- 备存的数据量及在信息系统备存有关数据的目的
- 需备份的数据档案
- 备存的备份份数
- 备份及存盘的频率

vi) 如系统有潜在隐私影响，进行私隐影响评估以审查用于保障个人资料的计划其保护措施是否足够、有效和实际。个人资料私隐专员已发出关于私隐影响评估的资料单张，该单张可于个人资料私隐专员公署网站下载。

(https://www.pcpd.org.hk/chinese/resources_centre/publications/files/InfoLeaflet_PIA_CHI_web.pdf)

用户要求可汇集成为某种形式的安全声明。用户的安全声明继而应作为系统功能规格的一部分，并在设计系统时反映出来。

敏捷开发方法日渐获得软件业界采纳。然而，鉴于敏捷开发方法的特点，敏捷方法与传统方法在安全保证方面明显存在不协调。现提供一些建议，以调整安全保证措施配合敏捷软件开发工作：

(i) 记录安全架构。

(ii) 在发展小组中加入一项职务，以评估安全风险、提出潜在的安全问题，以及进行系统设计及程序编码的安全覆检。

(iii) 记录与安全相关的程序编制活动。

(iv) 如有需要，进行程序代码覆检。

(c) 应用系统设计及发展的安全考虑事项

下文列举了一些在设计及发展应用系统时应遵守的安全原则：

- ***安全架构、设计和结构***。确保在设计基本系统架构时已顾及安全问题。应覆检针对潜在安全问题的详细设计，并设计和制订减低所有潜在威胁的措施。有关保障个人资料方面，决策局 / 部门须进一步参考《个人资料（私隐）条例》中保障资料原则[5]所列明的强制要求。
- ***最小权限***。确保应用系统的设计只授予执行工作所需的最小系统权限。
- ***职务分工***。确保遵从职务分工的做法，将关键功能分为多个步骤并分别交由不同人员处理，以防止关键程序被一人破坏。
- ***有需要知道***。系统文件和应用系统列表的访问权限须设定在最低限度，并须获得应用系统拥有人授权。
- ***保护最弱链路***。应用系统和操作系统的安全取决于最弱链路的安全，因此，应确保各方面均已设置足够的安全保护，以预防攻击者通过因编码方面的疏忽而产生的漏洞入侵系统。
- ***适当认证及授权***。确保推行妥善的访问控制措施，以执行用户的权限及访问权限。对于公共网上服务，应考虑使用全自动区分计算机和人类的公开图灵测试，以控制提交的输入数据。
- ***适当对话管理***。确保应用系统有适当及安全的对话管理，以保护对话不会在未获授权的情况下被访问、窜改或劫持。保护措施包括产生无法预测的对话标识符目、确保通讯渠道安全、限制对话有效期、把敏感对话内容加密、采取适当的注销功能和暂停闲置对话，以及过滤无效对话。
- ***输入验证***。确保应用系统对来自可信任范围以外的所有输入均施加严谨的验证，使任何预期以外的输入均获得妥善处理，不会成为攻击应用系统的途径。预期以外的输入包括过长的输入、不正确的数据种类、预期以外的负值或日期范围，以及预期以外的字符，例如那些被应用系统用作分隔所输入字符串的字符等。
- ***适当误差处理***。确保应用系统会提供有意义及对用户或支持人员有帮助的误差信息，但同时亦须确保这些误差信息不会披露保密数据。确保有关误差已被侦测、报告和妥善处理。
- ***故障处理***。确保应用系统设有安全机制，在应用系统发生故障时拒绝进一步执行编码。
- ***适当配置管理***。确保应用系统和系统均具备适当及安全的配置，包括关闭所有不使用的服务及设定适当的安全配置。
- ***移除不需要的项目。***确保关闭不使用或较不常用的服务、规约、端口及功能，以减少受到攻击的机会。此外，在生产服务器内不需要的内容，如显示于服务器横幅的平台数据、说明数据库及联机软件手册，以及默认或示例档案等亦应移除，以避免系统数据不必要的外泄。
- ***资料机密性***。在储存或传递保密数据时，确保数据已经加密。在展示、打印或使用保密数据作测试时，应遮蔽该等资料（如适用）。

[5] https://www.pcpd.org.hk/tc_chi/data_privacy_law/6_data_protection_principles/principles.html

- ***数据真确性及完整性***。在交换数据过程中，确保数据属真确及完整。
- ***安全使用***。确保备妥使用指南，载列如何安全地使用应用系统的各项功能。
- ***记录管理***。备存重要事件（如关键操作或敏感资料的处理）的审计追踪，以作恒常管制或调查之用。应禁止窜改或更改任何审计追踪。对于特殊情况，应提请管理层注意。

(d) 制订程序编制标准

执行程序编制控制至少须达到以下目的：

- 确保程序符合程序规格，除应有功能外，程序内没有任何未予记录的功能。
- 确保程序符合必要的程序编制标准。
- 防止及侦测欺诈行为。

为方便发展及维修程序，应制订程序编制标准。制订有关标准后，下一项重要工作是确保严格遵守所制订的标准。

(e) 分工

对风险较大及较敏感的系统来说，可能需要把处理极敏感数据的程序分为不同单元的模块和分段，并指派多位程序编制员处理。这样做可达到两个主要目的：

- 把程序编制职责分开可以令不诚实的程序编制员较难在系统内制造程序故障，因为该程序编制员无法控制程序的其他单元，必须与其他程序编制员合谋才能得逞。
- 把程序分为较小单元亦可提高侦测程序编制诈骗的机会，对程序单元可进行更详尽的分析和覆检。

(f) 程序 / 系统测试

首先，用户部门应进行用户验收测试，并负责制订测试计划和测试数据。用户部门亦应详细检查所有输出，以确保产生预期的结果。如发现误差信息，用户部门应有能力明白有关信息和采取相应行动作出修正。

测试计划应涵盖下列个案：

- 有效及无效的数据及个案组合。
- 违反编辑及控制规则的数据及个案。
- 算术运算的舍入、截尾及溢出测试个案。

- 预期以外的输入测试个案，例如过长的输入、不正确的数据种类、预期以外的负值或日期范围，以及预期以外的字符，例如那些被应用系统用作分隔所输入字符串的字符等。

除用户验收测试外，还有其他测试有助验证系统功能的正确性。单元测试用于测试独立程序或模块，以确保程序的内部操作符合规格。界面测试是一项硬件或软件测试，用于评估传递数据的两个或以上组件之间的连接情况。系统测试包括一系列测试，旨在确保改写后的程序可正确地与其他系统组件互相配合。压力测试或负荷测试用于测定指定系统的稳定性，方法是为系统加载超过其正常运行容量的负荷量，以观察其结果。回归测试是一项重新进行某测试方案或测试计划一部分的程序，以确保作出的变更或校正不会导致新的误差。在测试期间，每项测试均应予记录，列明记录的内容及测试目的。事项档案的记录还应包括事项完成后预期的结果，以供系统测试之用。每次更改系统后，使用相同的档案重新进行测试，然后比较前后输出的内容。任何修改只在没有发现任何分歧的情况下方可验收。

由数字政策办公室拣选的支援大规模面向公众数码服务的信息系统，亦须接受政府资讯科技总监办公室通告第 5/2023 号《加强大规模面向公众服务的资讯科技系统投入运作前的准备工作》所规定的额外测试。

16.2 发展及支持程序的安全

(a) 安全的发展环境

决策局 / 部门应评估个别应用系统发展工作涉及的风险，并为特定的应用系统发展工作建立安全的发展环境。决策局 / 部门应考虑：

- 需予处理、储存及传递的数据的敏感度。
- 规例或政策中可应用的内部或外部要求。
- 已制订的应用系统发展安全控制措施。
- 工作人员值得信任的程度。
- 应用系统发展的外包程度。
- 不同发展环境之间的分隔需要。
- 发展环境的访问控制。
- 程序代码与发展环境的变更监察。
- 于场外地方安全储存备份。
- 数据移出 / 移入发展环境的控制。

当决定个别发展环境的保护程度后，决策局 / 部门应记录安全发展程序的相关过程，并提供予有需要的人员。

(b) 应用系统的文件、程序源码和列表的控制

须妥善备存及根据既定程序妥善管理应用系统的文件、程序源码（包括无须编译而可直接执行的手稿程序）和列表，访问这些文件、程序源码和列表时须受「有需要知道」原则限制，并采取严格的访问控制措施。应用系统的文件、程序源码及列表的访问权限须维持在最低程度，并须获应用系统拥有人授权。这些文件应予以适当分类。

程序源码可以程序源库的形式集中储存，并应遵守以下附加指南以控制程序源库的访问：

- 程序源库不应存放在生产系统内。
- 所有程序源库的访问均应于审计记录内记录及备存。
- 维护程序源库时，应遵从严格的更改控制程序。

(c) 安全措施的测试及覆检

决策局 / 部门应确保任何全新及更新的应用系统在投产前，均已在发展过程中彻底测试及验证安全措施，包括拟备有关活动、测试输入及在一系列不同情况下的预期输出的详细列表。测试范围应与系统的性质及关键程度相符。

(d) 应用系统的完整性

须对应用系统采取适当的安全措施，例如版本控制机制和隔离发展、系统测试、验收测试和实际操作等不同环境，以维持应用系统的完整性。

应建立版本控制机制，记录程序源码在应用系统发展过程中的变更，以便在有需要（例如程序复原）时可获取指定版本。应制订、记录及遵从一套版本惯例，例如以 1.0 表示第一个正式版本，1.1 表示第一个正式版本的第一个修改版本。应备存一份变更记录，阐述自上一个版本以来所作的变更。决策局 / 部门可考虑采用版本控制工具，以提升版本控制的效益及减少人为失误。

应按以下考虑因素，隔离发展、系统测试、验收测试和实际操作等不同环境，以减少意外更改或在未获授权的情况下访问操作数据及应用系统的风险：

- 除非得到数据拥有人的批准，以及在测试系统推行相等的安全措施，否则不得复制保密资料至测试环境内。
- 应制订及记录将数据及应用系统由发展转移至操作状态的规则。
- 发展及操作软件应在不同的系统和网域内运行。
- 操作系统及应用系统的变更在提供正式服务前，应在系统测试及验收测试的环境内进行测试。

- 用作测试或发展的系统，应限制未获授权人士及不必要的网络连接（如互联网）的访问。此外，连接互联网的系统应避免选用一些吸引攻击者注意的系统名称，例如会令人联想到发展或测试环境的名称。
- 在操作系统方面，编译程序之类的系统工具应受到限制，以免在未获授权的情况下被访问，除非是技术上或运作上有需要访问这些系统工具，在这情况下应实施控制机制。
- 用户应在测试及操作系统内使用不同的用户帐户，应用系统应显示适当的识别数据以防止出现误差。

(e) 程序／系统更改控制

所有数据处理设施的变更均应获得授权及经过妥善测试。所有建议的程序／系统变更或提升项目应经过检查，以确保不会削弱系统本身或其操作环境的安全。有关人员应接受适当培训，确保充分认识其安全职责，以及任何系统配置更改后对安全和信息系统用途的影响。

维持程序／系统更改控制（包括操作系统、数据库及中间件平台的变更）的目的是：

- 维持程序或系统的完整性。
- 减低修改程序或系统时发生欺诈及出现误差的风险。

所有与安全控制相关的变更应经过确定、记录、测试和覆检，以确保系统能有效抵御攻击或破坏。在推行变更前应及时发出通知，以便有足够时间进行测试及覆检。应建立要求及审批程序／系统变更的程序。宜建立不同的授权级别（部分为非计划推行小组人员）以批准相关变更，并应只在得到正式批准后才可作出变更。授权级别应与变更幅度相称。在任何情况下，所有变更应由变更统筹员协调。变更统筹员应确保变更要求的数据质素和完整性，以及有关要求已得到相关人士的批准。操作及管理程序、业务持续运作计划和审计追踪（如适用）亦应予更新，以反映所作出的变更。

应尽量避免更改由供货商提供的软件套装。如确实有需要修改软件套装，应考虑以下数点：

- 会否损害内建控制及完整性程序。
- 是否需取得供货商同意。
- 可否从供货商的标准程序更新取得所需的变更。
- 如决策局／部门须负责软件日后的维修保养，会否带来影响。
- 有关变更是否与其他使用中的软件兼容。

(f) 程序编目

除非得到数据拥有人的批准，否则应用系统发展及系统支持人员不得访问生产系统内的保密数据。应推行程序编目，以限制生产系统内的保密数据的访问。

程序编目的基本原则是发展或维修小组人员不得将任何程序来源或对象带入生产程式库，或从生产程式库复制任何程序源码或对象。有关工作应由控制单位人员进行。

如须作出修改，须在控制单位人员看管下把提供正式服务的程序复制至发展程式库。在完成修改后，工作小组应要求控制单位将程序编入提供正式服务程式库的目录。此外，应推行版本控制，并备存至少两代软件产品，以便在有需要时可复原程序。

程序或系统强化应在系统启用前进行。强化后的程序 / 系统应作为进一步更改的基础。

为有效维护应用系统，请参阅以下就组织结构、程序及产品各方面详述系统维修周期的指南文件：

- **《系统维修周期指南》（G22）**
  可在政府资讯科技情报网下载
  (http://itginfo.ccgo.hksarg/content/sm/docs/G22.doc)

16.3 测试数据

(a) 测试数据的保护

对于用作测试的数据，须根据其类别予以审慎选择、保护及控制。正式服务的数据不得用作测试，并应避免使用包含个人或保密数据的操作数据库作测试用途。如不能避免，则须覆检及记录有关过程，而且须得到资料拥有人的正式批准，并采取以下控制措施：

- 使用有关数据前，须移除个人资料的部分。
- 使用有关数据前，须删除保密数据的部分或更改至不能辨认的程度。
- 所有这些数据在测试后应立即妥善删除。

17. 外包信息系统的安全

决策局 / 部门须确保外聘服务供应商可访问的信息系统和资产受到保护。

17.1 外包服务的信息技术安全

(a) 外包信息系统的安全

外包服务是指安排由政府以外的机构提供可由决策局 / 部门自行承包的服务。在向外聘服务供货商外包信息系统时，须制订适当的安全管理程序，以保护数据和减低与外包信息技术项目 / 服务相关的安全风险。外聘服务供货商参与政府工作时，须遵守及遵行各决策局 / 部门所制订的部门信息技术安全政策，以及政府发出的其他信息安全要求。决策局 / 部门使用外聘服务或设施时，须确定和评估此举为政府资料及业务运作带来的风险。所处理的全部数据须清晰及妥为分类。传输到外聘服务供应商的资料宜根据数据的性质和使用案例采用适当的技术进行数据掩盖。决策局 / 部门须记录及推行根据数据类别和业务要求而订定的外聘服务或设施安全措施、服务水平和管理要求，并与外聘服务供货商订明安全职责。访问数据的安全权限必须按照「有需要知道」原则授予。

此外，决策局 / 部门不得允许其外聘服务供应商享有访问在生产环境中的政府信息系统和数据的权限。如果认为有需要，例如基于系统维护及支援，访问须由获授权人员严密监管，并且在受控的情况下进行，以保护政府信息资产。严禁外聘服务供应商远程访问生产系统和数据进行日常管理和操作。

把信息系统外包时，应清楚制订、商定和记录外聘服务供货商、有关决策局 / 部门和终端用户的安全职务和职责。决策局 / 部门应注意，虽然信息系统的发展、推行及 / 或维护工作可以外包，但管理信息系统的整体责任仍由决策局 / 部门承担。

决策局 / 部门应确保外聘服务供货商拟备妥善的应急计划及备份程序，同时亦应确保外聘服务供货商根据政府规例、信息技术安全政策及指南，采取足够的安全控制措施。外聘服务供货商应向其人员提供有关安全意识的适当培训，使他们认识信息安全方面的职责。

数据或系统拥有人应知道服务供货商存放数据的位置，并确保已推行措施，以符合相关的安全要求及本地法例。

(b) 合约内的安全要求

决策局 / 部门须制订控制措施，管理有关外聘顾问、承包商及临时人员访问信息系统事宜。与第三方签订的合约或其他形式的协议须订明有关第三方访问或内部控制的安全要求。

除非已推行适当的控制措施，并已签署订明访问系统条款的合约，否则决策局／部门不得容许外聘顾问、承包商、外包人员及临时人员访问决策局／部门拥有或保管的数据和信息系统。

在拟定外包服务合约时，决策局／部门须订明外包的信息系统的安全要求。这些要求须成为招标程序的基础，并用以确定投标者有否遵行要求。

外包合约应规定外聘服务供货商的员工签署不可向外披露数据的协议，以确保外聘服务供货商人员在需访问保密资料时，承担保密的责任。合约亦应包括一系列服务水平协议。服务水平协议用于制订各项所需的安全控制措施的预定效能、说明可量度的成效，以及就任何已确定的违约事件定出补救及应变要求。服务水平协议应处理责任问题、服务的可靠程度，以及提供服务的回应时间。外聘服务供应商亦须承诺未经政府事先书面同意，不得向任何第三方传送或披露政府的保密数据。如果收到第三方的披露保密资料特别请求，而该等请求不能直接拒绝，则外聘服务供应商须立即通知并将请求转交决策局／部门处理。此外，外聘服务供应商须订立在其所有平台上安全删除政府资料的程序，并在数据删除后通过书面确认。此外，合约应包括一套解决问题及事故应变的升级处理程序，并应要求承包商遵行，以尽量减低对决策局／部门造成的影响。

(c) 损害或损失弥偿

所有外聘服务合约应载有适当和有效的弥偿损失条款，以保障政府不会因服务中断或承包商人员行为不当而蒙受损害或损失。

17.2 外包服务交付管理

(a) 对外包服务的监察及覆检

决策局／部门须监察外聘服务供货商，并与他们进行覆检，以确保外聘服务供货商的操作程序得到妥善记录及管理。此外，决策局／部门须妥善管理保密及不可向外披露数据的协议，并须在出现任何影响安全要求的变更时，覆检有关协议。

决策局／部门应使用合约方式保留审核及监察遵行安全要求的权利，以确保政府信息系统、设施及数据已推行足够的控制措施。合约应容许决策局／部门审核服务水平协议所制订的职责，并安排独立第三方进行审计，以及列举审计师的法定权利，否则外聘服务供货商须定期提交令人满意的安全审计／认证报告，以证明所采取的措施达到满意程度。

为管理外包服务的交付，决策局／部门应就下列方面制订程序：

- 根据服务协议监察服务表现。
- 定期举行进度会议，并覆检外聘服务供货商的服务活动。
- 覆检安全事务、操作问题和安全审计报告，并跟进所确定的问题。
- 对外包服务的安全活动（例如变更管理、安全漏洞管理及事故监察和应变）保持足够的整体控制及了解。

(b) 在合约期满或终止时的控制

决策局／部门须确保外聘服务或设施备存的所有政府资料在有关服务期满或终止时根据政府的安全要求予以清除或销毁。有关资料须根据其保密级别及相关的政府安全要求予以销毁。外聘服务供货商人员须在服务终止时，把其管有的所有政府资产交还政府。须制订及记录有关终止程序。有关删除资料及交还资产的详情，请分别参阅第10.3(b)节—删除数据及第 10.1(c)节—交还资产。

17.3 云端运算安全

(a) 共同责任

云端运算中的共同责任是指云端服务供应商（包括公共云端或私有云端服务供应商）与云端客户之间在安全和管理责任上的分工。这种共同责任模型确保问责，并有助于界定双方的角色和责任，以确保云端环境中数据和资源的安全和保护。

在与云端服务供应商签署协议之前，决策局／部门须确保已明确界定、记录及了解双方的共同责任。决策局／部门应仔细检视云端服务供应商的服务条款、数据保护政策和所推行的安全措施。

协议签署后，决策局／部门应确保合约所订明的共同责任持续获得遵行。应进行定期审查，以核证云端服务提供者遵守其在共同责任模型的责任部分。这种方法让决策局／部门能够保护其放在云端的工作负载，从而确保外包信息系统的整体安全。

虽然信息系统的开发、推行和／或维护可以外包，但信息系统的整体问责仍然归决策局／部门所属。

如欲获取更多有关云端服务中的共同责任的资料，可参考以下文件：

- **《云端运算安全实务指南》**
  可在政府资讯科技情报网下载
  (https://itginfo.ccgo.hksarg/content/itsecure/techcorner/practices.shtml)

18. 安全事故管理

决策局 / 部门须确保设有一致及有效的信息安全事故管理方法。

18.1 信息安全事故的管理和改进

(a) 事故监察及侦测

须推行足够的事故监察及侦测安全措施，以便在系统正常操作期间保护系统，同时监察潜在的安全事故。所采取措施的程度和范围取决于系统、系统处理的数据及系统提供的功能的重要性和敏感度。

下列是一些常用的安全事故监察及侦测措施：

- 安装防火墙设备，并采取认证和访问控制措施，以保护重要系统和数据资源。
- 安装入侵检测工具，主动监察、侦测并就系统入侵或黑客活动作出应变。
- 安装抗恶意软件工具和恶意软件侦测及修复工具，以侦测及清除恶意软件，并防止恶意软件影响系统操作。
- 利用安全扫描工具定期进行安全检查，以找出现有的安全漏洞，并进行既定安全政策与实际安全安排之间的差距分析。
- 安装内容过滤工具，以侦测电子邮件或网络通讯的恶意内容或程序代码。
- 开启系统及网络审计记录功能，以便侦测和追踪未获授权的活动。
- 开发程序和手稿程序协助侦测可疑活动、监察系统和数据的完整性，以及分析审计记录数据。

(b) 安全事故报告

须制订及记录一套报告程序，清楚订明适时向有关各方报告任何可疑活动的步骤和程序。报告程序应列明详尽的联络数据，例如电话号码（包括办公时间及非办公时间的联络电话号码和流动电话号码）、电邮地址和传真号码，以确保负责人员之间能够有效沟通。

如果怀疑系统出现任何异常的情况，欢迎决策局 / 部门向政府信息安全事故应急办事处寻求意见，以便及早发现政府的信息技术安全威胁和事故。此举有利于政府维护整体安全，并构建具复原能力和安全的环境。

为有效执行报告程序，应注意以下几点：

- 报告程序应载列清楚标明的联络点，并包括简单但明确的步骤以便遵从。
- 应向所有相关人员发布报告程序，以供参阅和参考。
- 确保所有相关人员熟习报告程序，能够立即报告安全事故。
- 编制安全事故报告表，以规范所收集的资料。
- 考虑报告程序在办公时间及非办公时间是否同样适用，如有需要，应为非办公时间制订一套独立报告程序，并指定相关人员担任非办公时间联络人。
- 有关事故的数据应只按照「有需要知道」原则披露，并只有信息安全事故应变小组组长有权或可授权他人把有关安全事故的资料与他人分享。

为改善信息技术安全事故处理的效率和效益，当意识到发生信息安全事故时（即合理确定信息安全事件已对政府信息系统或数据资产的机密性、完整性或可用性造成损害，或已损害其运作），部门信息安全事故应变小组须：

(i) 于 60 分钟内向政府信息安全事故应急办事处常设办公室作电话汇报，并于 48 小时内提交填妥的信息安全事故初步报告表；

(ii) 如安全事故牵涉关键电子政府服务、对安全有重大影响，或会引起传媒注意，在取得以下资料后尽快与政府信息安全事故应急办事处常设办公室分享：
   - 事故类别及对事故范围、破坏及影响的评估；
   - 为遏止破坏及修正问题而正在或将会采取的行动；
   - 如引起传媒注意时的响应口径；以及
   - 传媒的查询及响应建议（如有）。

(iii) 每天向政府信息安全事故应急办事处常设办公室更新受影响的关键电子政府服务的修复状况，直至服务恢复为止。

(iv) 就任何已向香港警务处、个人资料私隐专员公署[6]报告或向传媒机构发布的安全事故，通知政府信息安全事故应急办事处常设办公室。

在事故解决后的一星期内，应向政府信息安全事故应急办事处常设办公室提交事故事后报告。对于需要较长时间完成调查的个案，有关部门信息安全事故应变小组须根据以下指南就最新的修复情况及调查进度，向政府信息安全事故应急办事处常设办公室提交中期报告：

- 于第一次报告事故后不迟於十四天内向政府信息安全事故应急办事处常设办公室提交第一份中期报告；以及
- 为了让管理层知悉事故的状况，每三个月向政府信息安全事故应急办事处常设办公室提交事故调查进度，直到结案为止。

[6] 若事故涉及个人资料外泄，须尽快透过个人资料私隐专员公署的资料外泄通知表格向个人资料私隐专员公署报告事件：https://www.pcpd.org.hk/english/enforcement/data_breach_notification/dbn.html

(c) 安全事故应变

适当的事先规划可确保有关人员知悉应采取的事故应变行动，而有关行动可在互相协调及有系统的情况下执行，这亦有助相关决策局 / 部门在处理安全事故时作出适当和有效的决定，从而把安全事故可能造成的破坏减至最少。

须制订及记录安全事故应变计划。安全事故应变计划须至少包括以下内容：

- 事故应变小组的结构以及相应的角色和职责；
- 第 18.1 (b) 节所规定的报告程序；
- 缓解事故影响、保留證据、调查事件原因和影响的程序；
- 复原计划；
- 与持份者和公众的沟通计划；以及
- 事故後的审查程序。

安全事故应变计划须至少每两年定期覆检一次，或当决策局 / 部门的操作环境有任何实质改变时进行。决策局 / 部门须确保所有相关人员熟悉该计划，并且全体人员（包括管理层人员）均应知悉该计划，以作为参考和遵行有关要求。这套计划应清晰直接而且容易理解，让全体人员清楚了解他们需采取的行动。应变计划须定期进行测试和更新，以确保可迅速及有效地就信息安全事故作出应变。决策局 / 部门须至少每两年进行一次演习，最好每年进行一次，以评估计划的有效性。事故应变小组成员须参加演习，熟悉自己在安全事故应变计划中的角色，以确保快速及有效地应变安全事故。

所有安全事故、已采取的行动和相关的行动结果须予记录。这些记录有助确认和评估事故，为检控提供证据，并为其后的事故处理阶段工作提供其他有用的资料。整个安全事故应变过程都应保留记录。宜为每宗事故编配事故编号，以便在整个事故处理过程中作出跟进和追踪。

事故记录最低限度须包括以下数据：

- 系统事件和其他相关数据，例如审计记录。
- 已采取的所有行动，包括日期、时间和参与行动人员。
- 所有对外通讯，包括日期、时间、内容及有关各方。

当安全事故在非办公时间发生，7x24 小时的联络点对于即时沟通和快速处理事故至关重要，可以有效减少损害及损失。决策局 / 部门须安排两个 7x24 联络点，以接听信息技术安全问题的紧急电话。联络点须能及时处理安全事故或向负责人员转发紧急安全信息。

有关事故处理指南及程序的详情，请参阅：

- **《信息安全事故处理实务指南》**
  可在政府资讯科技情报网下载
  (https://itginfo.ccgo.hksarg/content/itsecure/techcorner/practices.shtml)

上述文件为决策局 / 部门提供参考，以便制订部门安全事故应变计划，并用作防备、侦测及应对信息安全事故。为使计划行之有效，应定期安排及进行演习。

(d) 培训与教育

决策局 / 部门须确保全体人员均遵守及遵从相应的信息系统安全事故应变计划。各人员应熟习由事故报告、确认，以至采取适当行动恢复系统正常操作的处理事故程序。决策局 / 部门应定期举行事故处理演习，让人员熟习有关程序。决策局 / 部门亦须参加数字政策办公室指定的安全演习。

此外，为了加强系统或功能范围的安全保护措施，并减低发生事故的机会，向系统操作和支持人员提供足够培训亦十分重要，使他们掌握有关安全预防的知识。

(e) 披露事故的资料

除向负责处理安全事故及系统安全工作，或获授权参与调查计算机罪行或滥用计算机事故的人士外，所有人员不得向任何人士披露有关计算机罪行及滥用计算机事故中的受害人、决策局 / 部门、受影响系统或造成该次事故的系统安全漏洞和入侵方法的数据。

披露有关事故的数据，包括入侵方法、系统背景数据如实体位置或操作系统等，可能会鼓励黑客入侵其他有相同安全漏洞的系统，亦可能会影响警方侦查时的鉴证及检控工作。

19. 信息技术安全方面的业务持续运作管理

决策局 / 部门须确保运作复原计划的内容包含信息系统的可用性及安全考虑。

19.1 持续信息技术安全

(a) 应急管理

信息技术应急规划指在紧急情况或系统中断的情况下恢复信息系统及信息技术服务的临时措施。有关临时措施可包括将信息系统及运作迁移至另一场地、使用其他设备恢复信息技术服务，或使用人手操作方式提供信息技术服务。应完整记录及定期测试信息技术应急计划。决策局 / 部门亦应评估持续业务场地或替代工作场地的安全风险，以确保已推行足够的安全控制措施保护政府保密数据。

信息系统的应急计划有不同种类，最常见的两种为业务持续运作计划及运作复原计划。业务持续运作计划着重于机构的关键业务程序在服务中断期间及之后仍可持续运作。在业务持续运作计划中，业务方面的系统拥有人应评估有关系统及数据的关键性、进行业务影响评估、设定复原时间目标、复原点目标及制订最低服务水平。运作复原计划提供详细程序以助信息技术能力的复原，下一节将作进一步阐述。

(b) 运作复原规划

运作复原规划是就信息系统制订运作复原计划的程序。运作复原计划包括一份规划完善的文件，处理信息系统及 / 或主计算机场地因发生灾难以致系统无法运作及数据全失的情况。运作复原计划应包括详细的信息系统备份程序，以及在另一计算机场地复原信息系统的程序。制订计划时应考虑信息系统的主计算机场地在灾难后可能有一段长时间不可使用，而另一计算机场地的信息系统运作不能达到理想水平（如可能需要人手操作辅助以弥补服务水平的下降）。计划应清楚订明有关各方的职责、各项功能的负责人员和联络数据。

计划应载有运作复原策略，包括详细及经过全面测试的数据复原及验证程序。鉴于测试的目的在于增强对程序准确性及成效的信心，因此制订测试的范围、方法及预期结果十分重要。

此外，应编制复原数据所需的一切数据及文件，以及在另一计算机场地预先安排通讯网络服务。运作复原计划还应包括在灾难后把数据复原至已修复的主计算机场地的程序。

决策局 / 部门应决定其运作复原计划是否足以应付可能发生的灾难。运作复原计划应载有最新数据，尤其是在主计算机场地的信息系统出现变更时。定期的运作复原演习是测试运作复原计划准确性及成效的好方法，但由于进行运作复原演习可能十分费时及影响正常操作，决策局 / 部门应根据其业务环境决定进行演习的次数。

(c) 信息技术安全的连续性

决策局 / 部门须计划、推行及定期覆检运作复原计划，以确保在这些情况下采取足够的安全措施。决策局 / 部门应在运作复原计划中，制订职务和职责、信息安全要求，以及信息安全的连续性。在欠缺运作复原计划及应急计划的情况下，决策局 / 部门应假设在任何情况下信息安全要求均与正常操作情况时相同。

19.2 复原能力

(a) 信息系统的可用性

决策局 / 部门应识别在信息系统可用性方面的业务要求。所有信息系统均应具备足够的复原能力，以符合在可用性方面的要求。如现存的系统架构不能确保信息系统的可用性，应考虑具复原能力的信息技术服务及设施。应测试具复原能力的信息系统，以确保组件的故障切换功能能按预期运作。在设计具复原能力的信息系统时，决策局 / 部门需考虑及解决相关数据的完整性或机密性的风险。

20 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。安全措施须根据相关安全要求推行及操作。

20.1 遵行法例及合约要求

(a) 定出适用的法例及合约要求

为避免违反法例及合约要求，决策局 / 部门须就每个信息系统的操作，明确定出、记录及更新所有适用的相关法定、规管及合约要求。应订明及记录符合这些要求所需的具体控制措施及个别职责。应定期覆检信息系统的安全状况，有关覆检应根据适当的安全政策进行，并应审计信息系统是否遵行适用的安全实施标准和已记录的安全控制措施。

(b) 知识产权

任何时候均须尊重版权法的限制。只有获准使用及已购置特许使用权的软件和硬件，才可按照所有特许证协议及程序设置及安装。所有人员必须遵守及遵从有关条款。在未获授权的情况下，须严禁复制、窜改或在未获特许使用权的情况下使用有关软件或硬件。应制订安全控制程序，以确保人员遵行所有软件特许使用权、采购协议及现行版权法例的规定。

应定期（例如每年一次）根据特许证协议，审计所有已安装软件的清单。特许使用权证明、软件手册及采购文件应存放在密封式档案柜等安全地方，并必须定期更新软件清单。购入软件升级版后，可能须根据采购协议弃置旧有版本。

- 所有安装于计算机或在计算机运行的软件应向获授权代理商 / 供货商正式采购。
- 决策局 / 部门应注意免费软件的特许使用权未必涵盖商业用途。
- 应定期覆检系统的软件列表，并须就安装未经批准的软件或在未获授权的情况下修改生产档案展开调查。

(c) 文件记录

决策局 / 部门须备存记录，以证明已遵行安全要求，并协助就相关安全措施是否已有效推行进行审计。已记录的数据应得到保护，以防止遗失及在未获授权的情况下被访问。欠缺有关资料会妨碍安全评估或审计活动，该等活动为决策局 / 部门及政府内部信息安全监管及保证工作的一部分。

决策局／部门应考虑根据其部门信息技术安全政策及指南文件，建立一份数据记录列表，以作为遵行安全要求的证明。有关用作证明遵行要求的数据记录列表样本，请参阅《安全风险评估及审计实务指南》。

(d) 数据保护

决策局／部门有责任了解并遵从所订明的规例。决策局／部门应找出数据可能外泄的途径，并考虑推行防止数据外泄方案，以监察及保护在储存、端点使用或与外部通讯传输中的保密数据，从而保护保密数据免在未获授权的情况下被访问或不慎外泄。

决策局／部门亦应留意其他经济体的规管框架（例如欧盟的《通用数据保障条例》、内地的《个人信息保护法》）（如适用）可能带来的影响。

所有个人资料应列为限阅类别或以上的保密資料。视乎有关个人资料的性质和敏感度，以及数据在未获授权或意外的情况下被访问、处理、删除或作其他用途而引致的损害，可能须采用较高的保密类别和采取合适的安全措施。决策局／部门处理个人资料时，必须确保遵行《个人资料（私隐）条例》，特别是保障资料第 4 原则（有关个人资料的安全）。有关六个保障资料原则的详情，请于个人资料私隐专员公署网站参阅《个人资料（私隐）条例》
(https://www.pcpd.org.hk/sc_chi/data_privacy_law/6_data_protection_principles/principles.html)。

对于可能涉及个人资料的信息系统，应在整个资料生命周期内推行适当的措施，以有效地处理以下事宜：

- 将个人资料的收集限制于标明目的的相关和必需的最低水平。
- 将个人资料的处理限制于标明目的的足够、相关和必需的程度内。
- 采用匿名化技术（例如移除或掩盖个人身分），以尽量减少个人资料曝光的机会。
- 确保在不再需要时删除个人资料。

當设计载有个人资料的信息系统时，应采取适当的技术层面和组织层面的安全措施，以保障个人资料免遭未获授权或意外的访问、处理、删除或其他用途，包括但不限于确保遵行所有适用的法律和规例、进行私隐影响评估以识别和管理资料保障风险、确保程序和系统的设计使个人资料的收集和处理仅限于必需的标明目的，并提高人员对个人资料外泄时可能造成的后果（如违反安全政策、破坏政府形象、纪律处分）的意识。

为了更好地保护信息系统中的个人资料，决策局／部门应遵守个人资料私隐专员公署制订的以下准则。

- 資訊及通訊科技系統的貫徹數據保障設計指南
  (https://www.pcpd.org.hk/tc_chi/resources_centre/publications/files/Guide_to_DPbD4ICTSystems_May2019.pdf)
- 私隐管理系统
  (https://www.pcpd.org.hk/pmp/pmp.html)

20.2 安全审查

(a) 安全风险评估

安全风险评估旨在评估信息系统的信息技术安全风险，根据风险源头（例如威胁、漏洞）和事件（例如事故场景）识别风险、根据风险的影响和可能性决定风险的级别，并对风险进行缓急排序以作处理。此外，在安全风险评估过程中，进行漏洞识别活动（例如漏洞扫描、渗透测试），以协助识别信息技术安全风险。安全风险评估完成后，应将已发现但尚未完全处理的风险记录在信息系统风险记录册中。

信息系统及生产应用系统须至少每两年进行一次安全风险评估。为免生疑问，（甲）连续两次评估工作之间相隔的期间，是指（一）在获得批准拨款后两次工作的开始日期，或（二）两次就已识别的风险作出评估的报告的发布日期之间的期间，而有关相隔的期间不得超过两年；以及（乙）在计算相隔的期间时，不包括针对已识别的风险而推行安全保障措施的时间。

决策局／部门应根据资料的保密类别、与互联网连接的资料、涉及的个人资料、外包安排，以及适用于每个信息系统的可用性要求等准则，识别及记录其信息系统的相关资料。

信息系统或生产应用系统在提供正式服务前，以及在进行大规模升级和变更前，也须进行安全风险评估。由于负责分析所收集资料及权衡安全措施的人员须具备深厚的专业知识和丰富的经验，因此应委任独立于覆检范围的合资格安全专家进行安全风险评估。当聘请服务供应商进行安全风险评估时，须在展开评估前决定和商定细节（例如评估范围、方法、报告格式）。安全风险评估须根据业界良好作业模式进行，包括现场审查，当中包括对信息技术基础设施的彻底检查和与关键人员的访谈，以全面了解环境，并识别可能无法从场外审查中识别的风险。

决策局／部门须在安全风险评估期间定期与服务供应商举行检查点会议，以监察进度、提供回馈，以及迅速解决意想不到的问题。决策局／部门须监督安全风险评估，并确保工作质素符合服务协议。虽然完成自我评估清单可以视为是持续监控的有用工具，但不足以被视为彻底和公正的安全风险评估，亦不得用作全面安全风险评估的替代品。

安全风险评估只能概括地提供信息系统在某特定时间存在的风险情况。决策局 / 部门应考虑根据信息系统的风险等级更频密地进行安全风险评估。

有关安全风险评估的指南，请参阅《安全风险评估及审计实务指南》。

(b) 安全审计

安全审计是以信息技术安全政策或标准为基础，以确定现行保护措施的整体状况，以及核实现行保护措施是否已妥善执行的程序或事件。安全审计的目的在于了解现有环境是否已根据既定的信息技术安全政策得到妥善保护。安全审计须至少每两年进行一次，以确保有关各方已遵行安全政策和采取有效的安全措施。决策局 / 部门须备存有关安全过程及程序的最新文件，以便促进安全审计过程。

决策局 / 部门应按照已规划的安全审计的性质，考虑所委聘的安全审计师是否适当人选。须选择独立和可信赖的第三方作为安全审计师，以确保审计观点正确、公平和客观。委聘内部或外部安全审计师的工作应慎重计划，尤其是委聘处理保密数据的安全审计师。在审计过程中，拣选审计师和进行审计的工作必须客观持平。审计师不得审核自己有份参与的工作。此外，决策局 / 部门应避免长期聘请同一安全审计师，以避免独立性下降。

安全审计须由具备足够技术和经验的审计师，在系统管理员的陪同下进行。应清晰界定和分派参与审计各方的职务、职责和责任。

安全审计须由具有相关专业资格的独立安全审计师（如注册信息系统审计师（CISA）、注册信息系统安全专家（CISSP）和注册信息安全专业人员（CISP））进行。审计师还应具有审核类似系统或行业的相关经验。

安全审计须评估信息系统有否遵行政府信息安全要求和决策局 / 部门的信息安全政策和指南。安全审计不得被视为对安全风险评估工作中所建议的修正措施的核证过程。安全审计须包括与不同持份者的访谈，以及就系统设定、记录、政策、程序和其他相关文件的审查。

当发现任何违规情况时，决策局 / 部门须：

- 确定违规原因。
- 评估是否有需要采取行动。
- 采取任何需要的行动。
- 覆检任何修正行动的成效。
- 记录及备存审计及所采取修正行动的结果。
- 审查类似的问题是否适用于其他信息系统。

有关安全审计的指南，请参阅《安全风险评估及审计实务指南》。

(c) 技术性遵行覆检

须限制及控制使用软件及程序进行安全风险评估或安全审计。为使用这些软件及程序而作出的所有信息系统变更，应受到严格的变更管理控制。决策局／部门应根据最小权限原则，分配有适当访问权限的专用账户，以进行安全漏洞扫描、渗透测试、配置审查及源码扫描。在完成有关工作或活动后，应立即删除有关账户，或重设有关帐户的密码。

决策局／部门须至少每年一次、在提供正式服务前，以及在进行就与信息系统相关的大规模升级和变动前，对所有与互联网连接的信息系统进行漏洞扫描。漏洞扫描也应纳入信息系统安全风险评估的风险识别程序中。所有与互联网连接的信息系统的安全风险评估工作须包括渗透测试。决策局／部门应定期、在提供正式服务前，以及在进行就与信息系统相关的大规模升级和变动前，对所有与互联网连接的信息系统进行配置审查和源码扫描。应在系统正式服务前评估所确定的安全漏洞及问题，并采取适当整改行动处理。

由于漏洞扫描、渗透测试、配置审查及源码扫描可能会危及信息系统的安全，所以应计划、记录并小心进行这些活动。安全漏洞扫描、渗透测试及源码扫描应只由获授权的合资格人士或在该等人士监督下进行。

有关技术性漏洞管理的细节，请参阅第 14.6 节《技术性漏洞管理》。

(d) 信息安全遵行的监察及审计机制

决策局／部门须遵從附录 D 所规定由政府引入的机制，用以简化监察及评估决策局／部门关于信息安全遵行情况的各项程序。

有关上述机制的详情，请参阅政府资讯科技情报网的信息技术安全主题专页 (https://itginfo.ccgo.hksarg/content/itsecure/isc_new/index.asp)。

21. 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：

电子邮件：	it_security@digitalpolicy.gov.hk
Lotus Notes 电子邮件：	IT Security Team/DPO/HKSARG@DPO
「中央管理通讯系统」电子邮件：	IT Security Team/DPO

*** 完 ***

附录 A 终端用户信息技术安全操作指示样本

本文件旨在协助终端用户了解他们在信息技术安全方面的责任。

决策局 / 部门应采用随附的终端用户操作指示样本，自行编制其终端用户安全操作指示。决策局 / 部门应根据其部门信息技术安全政策和计算机操作环境，特别编制切合需要的终端用户操作指示。决策局 / 部门应向所有在职及新入职人员派发相关文件，并定期提醒各人员阅览文件。

本终端用户操作指示文件不能取代决策局 / 部门或政府现行的安全文件。用户须阅读所有现行安全文件的要求并遵从行事。

终端用户
信息技术安全操作指示

[部门名称]

[*人员姓名*]已获委任为部门信息技术安全主任，负责监督[*决策局／部门名称*]的信息技术安全工作。安全是每名人员的个人责任。终端用户应根据数据类别小心保护数据或信息系统。每名用户必须对其在信息系统上所进行的一切活动负责。

为防止他人在未获授权的情况下访问或披露保密或个人资料，有关各方均须遵守现行的政府信息技术安全要求，包括《保安规例》和《基准信息技术安全政策》。任何人员不得发布、私自复制或向未获授权人士传递其因公职身分而取得的保密文件或资料，除非有关人员基于政府利益而须这样做，则作别论。「有需要知道」原则须适用于所有保密数据，这类数据须只提供给有需要和有权访问数据的政府内部及外部人员，以便他们有效执行工作。如对某人员是否有权访问某份文件、某数据类别或某些数据有疑问，应向部门安全事务主任查询。

用户须妥善地保管及保护计算机和储存装置，以防止他人在未获授权的情况下访问或披露其所管有的资料。同时，须推行适当的安全措施，以保护政府信息资产及信息系统。用户如察觉任何可疑活动或怀疑发生违反安全事项，须尽快在办公时间内向[*求助台*]报告。如在办公时间外发生安全事故，请联络以下人员：[*填上姓名及联络资料*]。

违反信息安全要求者可能会受到纪律处分。

以下是处理政府数据或使用信息系统时应做与不应做的事项。请注意，下文所列事项并非详尽无遗，故应视乎情况同时参照部门信息技术安全政策、《保安规例》和《基准信息技术安全政策》[S17]。

应做的事项

- 保密类别须清楚标明，例如就载有限阅数据的电邮而言，应在标题之前注明[限阅]。
- 所有保密数据必须加密储存。所有保密数据在任何通讯网络上传递时均应加密。机密或限阅数据在不可信任的通讯网络上传递时必须加密。
- 在政府内部以电邮方式传递机密数据时，须使用「政府内部机密邮件系统」、「机密信息应用系统」、「机密电邮流动服务」和「中央管理信息平台」中已获批准的子系统。
- 在发送电子邮件之前，尤其是当电子邮件包含保密或个人资料时，小心检查收件人的电子邮件地址。
- 检查邮箱中是否有可疑活动以及电子邮件帐户设置中是否存在不熟悉的变更。例如，在没有通知的情况下设定了邮件规则的配置、收件匣不再接收电子邮件，或「已传送」资料夹包含你未撰写过的外发电子邮件。
- 透过检查通信中使用的电子邮件地址、划一资源定位址和拼写，验证收到的消息和内容的真实性。
- 经常备份关键数据，以及保留备份的离线副本，并采取足够的保护措施。
- 减少在流动电话处理和储存保密或个人资料。
- 在使用流动电话时，让其处于持续和直接受到监察的情况，并在不使用时将其存放在与其储存的资料保密类别相应的实体受保护区域。

- 应采取适当的安全措施，以妥善保护所管有的设备、装置或用户身分数据，例如启动密码保护、注销或关机、无人看管时把有关设备、装置或数据锁于柜／抽屉内。
- 确保工作环境安全及稳妥，例如使用荧幕防窥片，以防止敏感资料意外泄露及避免遭受窃听。
- 应按照「有需要知道」原则发放数据及授予数据访问权限。
- 应根据部门密码管理要求设定密码，例如采用由至少八个大写字母、小写字母、、数字及特殊字符混合组成的密码，并定期更改密码。如怀疑密码已被破解，应立即更改密码并向上级报告。
- 应就每个系统或服务帐户使用独特且足够复杂的密码，例如公务电邮帐户的密码应与私人电邮账户的不同。
- 为线上帐户启用多重认证（如有），尽量减低凭证被窃的风险。
- 应安装最新的安全修补程序，并定期删除缓存文件或临时档案，以保障数据隐私。
- 应推行配备最新恶意软件标识符和定义档案的恶意软件侦测措施，以便在使用前扫描电邮、已下载文件、抽取式媒体或流动装置上的档案。
- 应不理会或删除滥发电邮[7]。小心仿冒诈骗电邮[8]可引致感染恶意软件甚或违反安全事项。
- 应采用加密方法保护无线或流动装置，以保护所传递的数据，并启动密码保护功能，以防止他人擅用该等装置。
- 应关闭无需使用的无线及流动服务。
- 关掉不使用的无线连接，如 Wi-Fi、近距离无线通讯、蓝牙和红外线连接。
- 关闭自动连接 Wi-Fi 以避免自动连接不安全的网络，例如在公共场所。

[7] 滥发电邮指滥发无用的讯息（例如广告），使电邮帐户不胜负荷。
[8] 仿冒诈骗电邮指仿冒收件者认识的人送出电邮，意图窃取资料。

- 使用政府提供的互联网服务时，应遵从《使用互联网服务的指导原则》[9]。

不应做的事项

- 不应在私人拥有的流动装置、抽取式媒体或物联网装置储存保密数据。
- 不应在无人看管和没有推行足够实体访问控制措施（例如房门已打开、物品遗留桌上）的情况下，离开工作站及计算机设备。
- 不应将写有密码的纸张放置于工作间附近（例如贴在屏幕上的便条纸），或使用容易猜到的密码（例如在词典中查到的单字）或与个人资料相关的密码（例如姓名、出生日期或职位名称），或与他人共享密码。
- 不应向未获授权人士披露个人、系统或部门数据。
- 不应把私人拥有的装置连接至政府内部信息系统或网络。
- 不应经拨号调解器、无线界面或宽带链路将工作站连接至外部网络。
- 不应向非应邀和任何可疑的电子讯息（包括但不限于电子邮件、即时讯息和短讯）作出回应、开启附件或点击连结。
- 不应从未经确认可信赖的网站下载和开启档案。
- 不应使用政府电子邮件地址注册与工作无关的在线服务。
- 不应重复使用与政府电子邮件帐户相同的密码订阅其他在线服务。
- 不应使用任何私人电子邮件服务进行官方通信，尤其是在以官方身分与公众或外部机构通讯的情况下。
- 未经部门信息技术安全主任事先批准，不应在工作站安装软件。
- 不应关掉政府拥有装置的现有端点保护功能。
- 不应于工作站访问来自不明抽取式媒体的档案。
- 未经决策局 / 部门指定人员事先批准，不应在工作站安装及执行未获授权软件。

[9] https://itginfo.ccgo.hksarg/content/itsecure/techcorner/practices/Guide_use_of_Internet.htm

附录 B 评级指南

决策局／部门在为信息系统评级时，应参考以下考虑因素。

1. 第 2 级信息系统

第 2 级信息系统是指对政府或社会运作重要的信息系统，其故障或中断会对政府运作带来严重影响，或可能引致公众混乱及灾难性後果。

一般来说，信息系统故障或中断对政府造成的影响可分为三个严重程度，详情如下：

影响程度	描述
高 （H）	对政府造成重大损失／严重损害或不利
中 （M）	对政府造成中等损失／一些损害
低 （L）	对政府造成轻微损失／少许损害

下表总结一些在判断影响时的要素，以供考虑。这些要素可以分为四个不同的方面。决策局／部门应慎重考虑系统发生故障或中断时在不同方面的影响程度。

方面	信息系统故障或中断时应考虑可能会导致的影响	影响程度（高／中／低）
防御/ 安全风险	(a) 危害人命或财产 (b) 无法维持治安 (c) 无法执行法定责任 (i) 在及时的情况下 (ii) 在信心和／或正确性足够的情况下 (iii) 在规划资源受限等情况下 (d) 导致实体／信息资产损坏或丢失 (i) 实体设施、系统或网络 (ii) 设备、组件或必需品 (iii) 数据、个人资料、知识产权等 (e) 令安全控制措施松弛等	
经济影响	(a) 直接或可能导致政府财务损失 (i) 直接的财务损失 (ii) 税款损失或征收税款延误 (iii) 延迟检讨政府收费 (iv) 执行跟进行动（例如清理和／或整理数据）有额外支出 (v) 在付款过程中延迟所产生的额外开支／补偿等。	

政府形象	(a) 影响政府声誉 (b) 影响公众信心等	
为用户提供的服务	根据终端用户的类型及用户人口，当服务中断或在效率下降时，影响有多严重？ (a) 影响大量用户还是只影响少数用户？ (b) 目标终端用户是公众，或只在所属决策局／部门内，还是其他决策局／部门？ (c) 干扰政府高层官员分析信息与决策过程？等。	
其他	请包括任何适用于其信息系统的其他考虑范畴。	
	整体影响程度：	

（注：请同时考虑服务中断对其他相互依赖的信息系统的影响。）

一般来说，如果有一个或多个方面的影响程度被评估为「高」，你应考虑将系统或服务的整体影响程度视为「高」。如果整体影响程度为「高」，则该信息系统应视为第 2 级信息系统。

2. 第 3 级信息系统

有很多必要服务对社会及其经济的运作和安全是关键的。第 3 级信息系统是指与提供有关的必要服务直接相关且其中断或破坏可能对经济、民生、公共安全等造成严重损害的第 2 级信息系统。

为识别第 3 级信息系统，决策局／部门应识别其所提供的必要服务，并随后根据定义决定第 3 级信息系统。一般来说，必要服务通常分布在对社会有重大影响的不同行业（例如航空、银行和金融、广播、通信、能源、医疗保健、陆路运输、海事、媒体、安全和紧急服务、供水和污水处理等）。在识别必要服务时，决策局／部门应根据服务性质以及服务对社会及其经济的运作和安全的影响，考虑其所提供服务的关键性。在识别必要服务后，决策局／部门应随后识别与提供相关必要服务直接相关的第 2 级信息系统，所识别的信息系统被视为第 3 级信息系统。

上述考量可作为决策局／部门为其信息系统评级的参考。决策局／部门应参考上述指南作出自行评估。如有疑问，欢迎决策局／部门就系统评级的评估咨询数字政策办公室的意见。

附录 C 信息系统应有的信息技术安全等级保护

第 2 级信息系统与第 3 级信息系统须根据其系统等级分别采取以下更严格的安全控制措施，以达致信息系统应有的信息技术安全等级保护。第 3 级信息系统亦须采用第 2 级信息系统安全控制措施。

政府信息安全组织（第 5 节）	
第 3 级信息系统	a) 设有第 3 级信息系统的决策局 / 部门的部门，其信息技术安全主任的角色须由高层管理人员中的首长级人员担任。 b) 就设有第 3 级信息系统的决策局 / 部门，须成立由高层管理人员及部门信息技术安全主任参与的信息安全督导委员会，以确保在信息安全方面投入足够的资源和关注。信息安全督导委员会须定期召开会议。委员会的讨论结果须妥为记录，包括关于信息安全相关问题的管理层指示，以便作出跟进行动。委员会的结构、职务和职责也须记录在案。 c) 就设有第 3 级信息系统的决策局 / 部门，须最少有一名信息技术安全管理组的成员持有最少一项业界认可的信息技术安全认证（例如注册信息系统审计师（CISA）、注册信息系统安全专家（CISSP）和注册信息安全专业人员（CISP）等）。
管理职责（第 7 节）	
第 3 级信息系统	a) 就设有第 3 级信息系统的决策局 / 部门，有关决策局 / 部门须采用第 7.2(c)节所订明的信息技术安全风险管理架构。决策局 / 部门须为其第 3 级信息系统备存风险记录册。风险记录册须至少记录已识别的信息技术安全风险、其发生的可能性和严重性、减低该风险的措施和所需的监测。

人力资源安全（第 9 节）		
第 3 级信息系统	a)	就设有第 3 级信息系统的决策局 / 部门，有关决策局 / 部门须制订信息技术安全培训计划，以便为其人员提供适切和有系统的信息技术安全意识活动。培训计划亦须确保参与第 3 级信息系统支援和操作的所有人员，包括产销商、承包商和服务供应商，熟悉信息技术安全要求及当前的信息技术安全威胁、影响和缓解措施。若无法为产销商、承包商和服务供应商制定或提供培训计划，决策局 / 部门须与对方订立合约责任，要求对方向其人员提供相关信息技术安全培训。
访问控制（第 11 节）		
第 2 级信息系统	a)	须至少每六个月一次定期由独立方检查 / 审计高权限帐户的使用情况，以确保这些帐户是为合法目的而使用。
	b)	如果没有技术解决方案限制通过高权限帐户访问信息系统和应用系统中的信息，决策局 / 部门须采用行政程序以管理有关访问（例如从另一个指定人员保存的密封信封获取密码、由两名员工使用分拆的密码登入）。
	c)	须确实执行第 11.4(b)节规定的严谨密码政策。此外，如果任何信息系统被入侵时可能会影响第 2 级信息系统的安全（例如，信息系统与第 2 级信息系统共用同一个网络分段、或能够对第 2 级信息系统进行管理功能的特定设备），亦须确实执行严谨密码政策。
	d)	在技术上可行的情况下，须针对第 2 级信息系统的特权帐户的任何交互式登录实施多重认证。

操作安全（第 14 节）	
第 2 级信息系统	a) 须备存本地和场外备份。场外信息备份须存放于稳妥及安全的地方，并远离设备的的所在地。 b) 须制订及记录容量管理计划。 c) 为了减低软件终止支援的影响，须在终止支援日期之前至少六个月制定迁移计划，并且相关的安全措施须在终止支援日期前实施。 d) 所有已知的安全漏洞须尽快修复，通常在安全修补程式发布后一个月内完成。决策局／部门须进行风险评估，考虑漏洞的潜在影响和被利用的可能性，以决定漏洞缓解的方法和时间表。风险评估的结果须妥为记录。如漏洞未能在一个月内得以缓解，决策局／部门须告知其部门信息技术安全主任有关理据、相关风险以及缓解方法和时间表，以提高漏洞缓解状态的可见性。决策局／部门亦须每月向信息技术安全主任提供有关漏洞缓解状态的中期更新情况，直至漏洞得以缓解。
第 3 级信息系统	e) 就设有第 3 级信息系统的决策局／部门，有关决策局／部门须建立信息技术安全监察流程，当中包括 24×7 的信息技术安全监控。信息技术安全监察流程让决策局／部门能够整合来自多个来源的数据（例如防火墙、入侵侦测系统／入侵防御系统、端点侦测与回应／网络侦测与回应的解决方案），以提供全面的安全情况，以便对潜在的安全事件作出更快捷有效的应变。此外，安全监察流程须有助监察网络和系统内的活动，并提供持续的威胁侦测、监察和事故应变能力，包括利用安全信息和事件管理工具协助全面分析及关联来自多个来源的安全事件数据。

系统购置、发展及维护（第 16 节）		
第 2 级信息系统	a)	须采用安全左移方法，包括依照第 16.1(a)节规定在系统设计阶段采取安全编码作业模式和安全审查。在提供正式服务前的安全风险评估须核实安全覆检的跟进行动，以确保系统在正式投入运作前已推行所需的安全措施及控制措施。
	b)	系统强化须在系统投入运作前进行，强化后的系统须作为进一步更改的基础。
信息技术安全方面的业务持续运作管理（第 19 节）		
第 2 级信息系统	a)	须制订信息技术应变计划以确保第 2 级信息系统在出现极严重的服务中断（例如火灾、水浸等天灾）或紧急情况（例如恐怖袭击、大型示威或炸弹威胁而需撤出场地）时仍可持续运作。须完整记录及定期测试信息技术应变计划，并与业务持续运作计划互相配合。
第 3 级信息系统	b)	须具备足够的复原能力，以防止所提供的必要服务中断。须定期测试复原能力，以确保组件的故障切换功能的运作能够符合预期目标。
遵行要求（第 20 节）		
第 2 级信息系统	a)	须每年至少一次对第 2 级信息系统进行漏洞扫描，并在信息系统正式投入运作前，以及在进行大规模升级和变更前进行漏洞扫描。
	b)	渗透测试须包含在所有第 2 级信息系统的相应安全风险评估工作中。对于与互联网连接的第 2 级信息系统，决策局／部门须确保每年至少进行一次渗透测试。

第 3 级信息系统	c)	第 3 级信息系统须至少每年进行一次安全风险评估，并在信息系统正式投入运作前，以及进行大规模升级和变更前进行。安全风险评估须包括漏洞扫描、渗透测试、配置覆检和源码扫描。安全风险评估包含的渗透测试须由具有专业资格或认证（例如，道德黑客认证课程（CEH）、Offensive Security 认证专家（OSCP））的独立服务供应商进行。安全风险评估完成后的安全风险评估报告，包括系统风险记录册、相应的漏洞扫描报告、渗透测试报告、漏洞修正计划等，须经部门信息技术安全主任认可。

附录 D 信息安全遵行监察与审计机制

政府引入以下信息安全遵行监察及审计机制，以简化监察及评估决策局／部门关于信息安全遵行状况的各个程序：

1. 就设有第 3 级信息系统的决策局／部门，有关决策局／部门须向数字政策办公室提交其信息技术安全管理组的编制、汇报机制、职务及职责。如有需要，数字政策办公室可要求决策局／部门澄清相关资料。若资料有任何重大变更，决策局／部门须在三十天内通知数字政策办公室。
2. 决策局／部门须向数字政策办公室提交其第 2 级信息系统、第 3 级信息系统的清单及系统评级的评估详情(获决策局局长／部门首长或他们明确授权的首长级人员同意)。若所提交的清单有任何变动，包括系统评级的变动，决策局／部门亦须在三十天内通知数字政策办公室。数字政策办公室可要求各决策局／部门提交进一步资料，以确保各决策局／部门对系统等级的评估符合第 7.2(b)节所订明的信息技术安全等级保护。
3. 第 3 级信息系统的事故应变计划须在数字政策办公室要求下提交检查及覆检。
4. 决策局／部门须提交一份标准表格《安全遵行状况表》向数字政策办公室概括其所有系统的信息安全风险评估及安全审计的资料。每次完成安全风险评估或安全审计后，应在六个月内向数字政策办公室提交中期表格，以追踪保障措施的推行情况。如所有保障措施已在六个月内推行，《安全遵行状况表（中期）》将视为《安全遵行状况表（终期）》，否则应在完成安全风险评估或安全审计后一年内，向数字政策办公室提交《安全遵行状况表（终期）》。
5. 第 3 级信息系统安全风险评估报告，包括系统风险记录册、相应的漏洞扫描报告、渗透测试报告及漏洞修正计划，均须于评估完成后三十天内提交予数字政策办公室，以供进行检查和覆检。
6. 第 3 级信息系统的安全审计报告须在审计完成后三十天内提交予数字政策办公室，而若出现违规，则须在提交审计报告后三十天内进一步提交修正计划。
7. 决策局／部门须参与由数字政策办公室进行的抽样安全审计，并在议定的时间内优先完成审计。这项工作评估决策局／部门进行安全风险评估及安全审计的质素，以及对政府信息安全要求的遵行情况。决策局／部门须提交标准表格《遵行审计跟进状况表》，以报告遵行审计所需的跟进工作的完成情况。每次完成遵行审计后，决策局／部门应在六个月内向数字政策办公室提交中期表格，以追踪建议的落实情况。如所有建议均已在六个月内落实，《遵行审计跟进状况表（中期）》将被视为《遵行审计跟进状况表（终期）》，否则应在完成遵行审计后一年内，向数字政策办公室提交《遵行审计跟进状况表（终期）》。

8. 决策局 / 部门须完成数字政策办公室定期进行的安全问卷调查，以收集安全状况资料。通过问卷调查可了解决策局 / 部门有关信息安全的计划、惯例及行动。这些资料可反映决策局 / 部门在回应安全政策、安全威胁或其他安全问题方面的就绪程度。