数字政策办公室

信息安全

基准信息技术安全政策

[S17]

第 8.1 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	修改报告可于政府内联网「资讯科技情报网」查阅		2.0	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」		2.1	2004 年 7 月
3	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」	无	2.2	2004 年 9 月
4	作出相应更新，以符合经修订的政府安全要求	11-1, 11-2	2.3	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		3.0	2006 年 5 月
6	修改第 8.3.1 及 9.1.6 节并加入遵守《个人资料（私隐）条例》的要求	8-1, 9-1	3.1	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		4.0	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		5.0	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		6.0	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)		7.0	2021 年 3 月
11	修改报告可于政府内联网「资讯科技情报网」查阅		8.0	2024 年 4 月

12	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」		8.1	2024 年 7 月

目录

1. 目的

随着各界有效使用互联网服务，以及普遍采用云端运算和流动信息处理技术，信息系统的安全及持续性对经济和社会至关重要。办公室工作和公共服务愈来愈依赖信息技术，为政府业务带来了新重点，就是我们所依赖的主要信息系统和数据必须安全并得到妥善保护，确保所有决策局／部门均能畅顺运作，借此巩固市民信心、保障信息安全及隐私，这是政府业务能以具效益、有效率和安全的方式运作的基础。

本文件概述为保护香港特别行政区政府所有信息系统及数据资产而订定的强制性最低安全要求。决策局／部门须通过下列方式制订、记录、推行、维持和复检适当的安全措施，以保护其信息系统和数据资产：

- 在内部订立符合本文件所载规定的适当信息技术安全政策、规划和监管措施，包括采用所有架构及要求；
- 确保推行本文件所述的适当安全措施；
- 确保定期复检安全措施的持续适用性、足够性和效益；以及
- 改善安全措施的适用性、足够性和效益。

本文件所述的安全要求是以技术中立的角度制定。本政策的要求着重基本目标和控制措施，以保护在处理、储存及传递中的资料。

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做调整。本文件就下列 14 个范畴提出强制性指南：

- 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）

本文件载列的是各项基本安全要求。决策局／部门需因应本身的情况及已确定的风险，推行更严谨的安全措施。

2.2. 对象

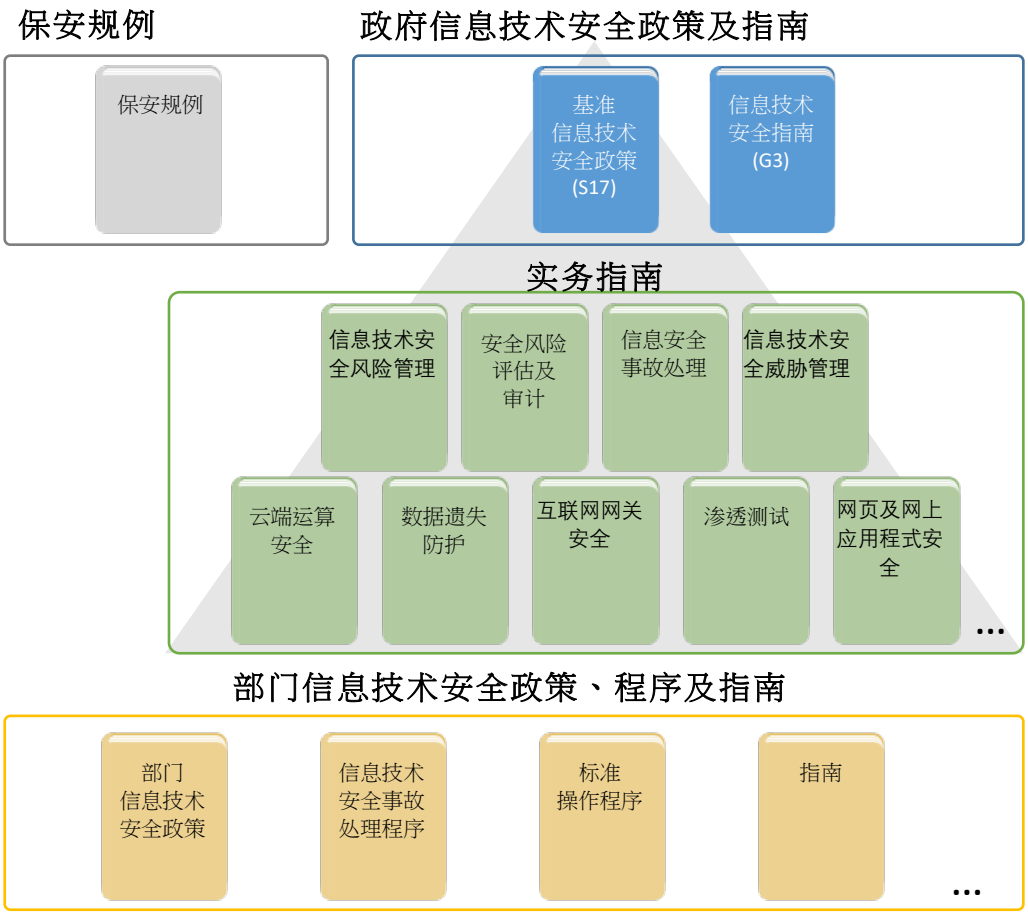
本政策是为各决策局／部门内担当不同职务的各级人员制订，当中包括管理人员、信息技术管理员和一般的信息技术终端用户。全体人员均有责任通篇阅读整份文件，以了解并遵行信息技术安全政策。

另外，本文件亦供为政府提供信息技术服务的供应商、承包商及顾问作为参考。

2.3. 政府信息技术安全文件

政府已发布一系列安全规例、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。

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／部门亦可采取其它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。

我们亦因应不同专题和特定的技术要求制订了一系列实务指南，以补充《信息技术安全指南》的内容，并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技术及安全威胁所带来的风险。

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) 公务员事务局《公务员事务规例》

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

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、传递或弃置数据，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和信息系统能够知悉或访问信息系统所储存或处理的资料。
f) 完整性	在任何方面只有获授权人士和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和信息系统提出要求时，可供该人士和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资料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。

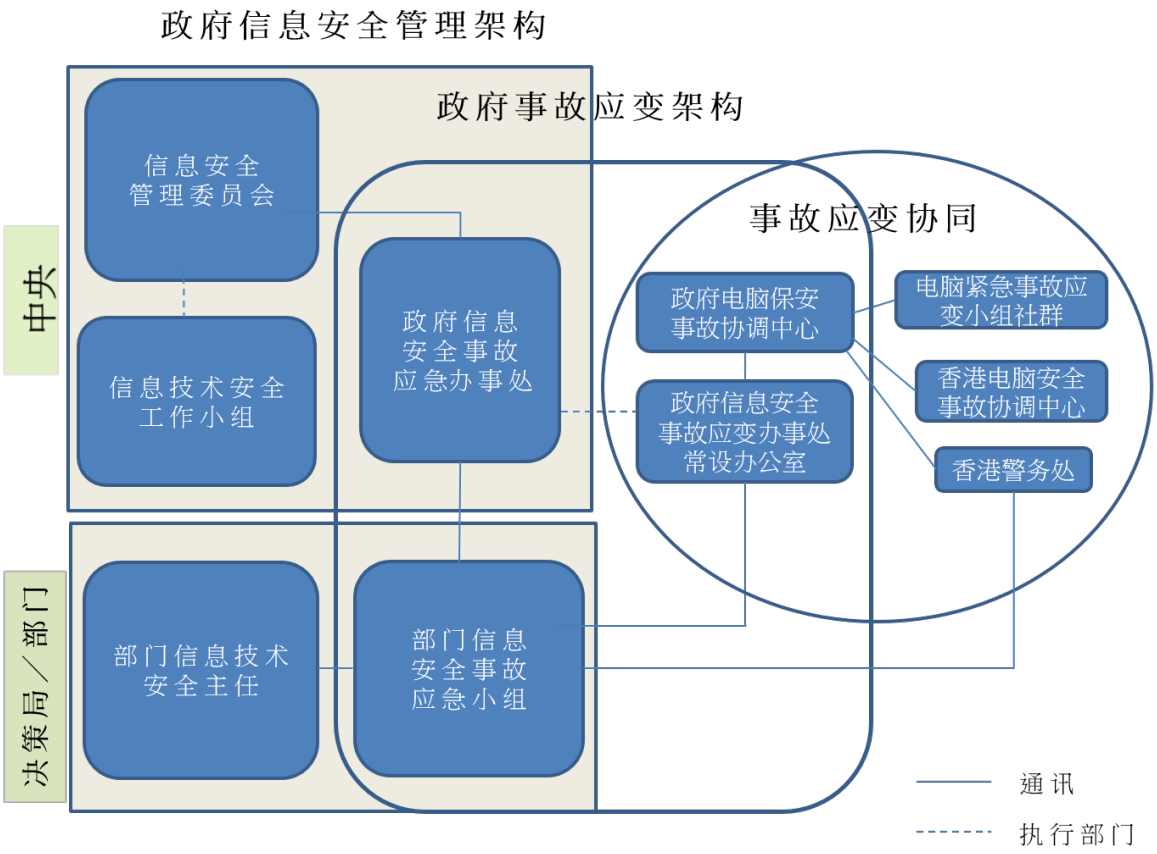
宜 「宜」表示期望达到的良好作业模式。

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它决策局／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它决策局／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急小组。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急小组的运作。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：

- 设立中央资料库，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急小组之间互相分享和交流信息安全事故处理的经验和资料。

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急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。

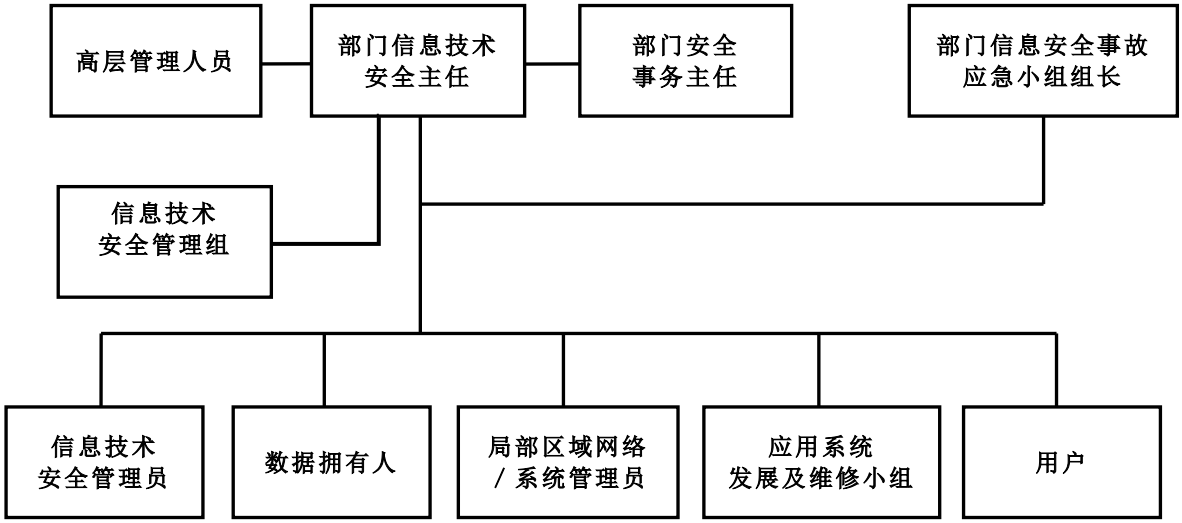
5.1.5. 决策局／部门

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。

[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。

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它决策局／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
- 就违反安全事件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急小组组长

部门信息安全事故应急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急小组组长。信息安全事故应急小组组长应有权委任信息安全事故应急小组的核心成员。信息安全事故应急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. 其它职务

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数据的人士。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：

- 联络数据拥有人，以便在应用程序的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资料的人员。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。

- **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。

- **设计层面的安全**
  须采用设计层面的安全概念，将安全要求纳入软件发展周期，确保信息系统和应用程序采取适当的安全和数据保护措施。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。

- **预防、侦测、应急和复原**
  信息安全涵盖预防、侦测、应急和复原措施。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。应急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。

- **处理、传输和储存资料时的保护措施**
  处理、传输和储存资料时，须视乎情况考虑及推行安全措施，以维持资料的机密性、完整性和可用性，例如欠缺保护的无线通讯容易遭受攻击，因此传输保密资料时须采取安全措施。

- **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。

- **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，以及迅速应急和使系统迅速复原。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。

- **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／机构的活动和所涉及的程序。须根据资料的敏感度，明确界定和定出有关各方所担当的职务和职责，并据此授予权限。

  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。

- **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。

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数据资产得到保障，以及信息技术服务能安全运作。

7.1. 一般管理

7.1.1. 决策局／部门须订定其部门信息技术安全组织架构，以及界定相关的职务和职责。

7.1.2. 决策局／部门须确保其安全保护措施能因应不断转变的环境和技术而更新。

7.1.3. 决策局／部门须充分利用职务分工，以避免由一人负责整个信息系统的所有安全工作。

7.1.4. 决策局／部门须确保在其财政预算中预留拨款，以提供必需的安全保护措施和资源。

7.1.5. 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资料。

7.2. 安全风险管理

7.2.1 决策局／部门须采用风险为本的方法处理信息安全，以确保辖下信息资产所载数据的机密性、完整性和可用性，并须确保信息系统（包括外包系统）符合其它所有安全要求，并监察其员工及承包商对安全政策、指南等的遵行情况。

7.2.2 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（包括基础设施和部门共享信息技术服务）评级，无论其资金来源为何，并依系统等级推行分级的安全控制措施。所有信息系统的系统评级详情须妥善记录。信息系统等级须由决策局局長／部门首长或他们明确授权的首长级人员批准。

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

8.1.1. 决策局／部门须发布及执行本身的信息技术安全政策。决策局／部门须以《基准信息技术安全政策》文件为基础，制订其政策。

8.1.2. 决策局／部门须定期复检信息安全政策、标准、程序和指南。

8.1.3. 决策局／部门须清晰制订并向用户传达有关正确使用信息技术服务及设施的政策。

9. 人力资源安全

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、更改或终止聘用过程中维护政府利益。

9.1. 新聘、雇用期间或终止雇用

9.1.1. 决策局／部门须在有关人员获派任新职位时，告知他们其信息技术安全职责，并须在他们受雇期内，定期提醒他们有关职责。

9.1.2. 信息安全是政府全体人员均须承担的责任。决策局／部门须向各人员提供有关安全意识的适当培训，并定期为他们提供有关信息技术安全政策的最新信息。

9.1.3. 决策局／部门须定期教育及培训人员，使他们能履行与信息技术安全有关的职责和职务。

9.1.4. 获授权可访问限阅以上类别保密资料的公务员，须按照公务员事务局局长的规定接受操守审查。至于并非公务员的人员，决策局／部门应根据业务要求、有关人员所处理资料的类别和表面所知的风险，对该等人员进行适当的背景审查。

9.1.5. 决策局／部门须在其信息技术安全政策中订明，根据《公务员事务规例》，公务员如违反有关政策的任何条文规定，可能会受到纪律处分，而视乎违规事件的严重程度，有关人员可能受到不同程度的纪律处分。

9.1.6. 决策局／部门须在其信息技术安全政策中订明，所有并非公务员的人员（即上文第 9.1.5 节没有涵盖的人员）如违反有关政策的任何条文规定，则视乎违规事件的严重程度，可能受到根据其雇用条件而施行的相关处分，包括但不限于终止其向政府提供的服务。

9.1.7. 可使用或可在无人陪同的情况下访问信息系统和有关资源的人员须经过严格挑选，亦须了解本身的职责和职务。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。

9.1.8. 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，这类数据应只提供给有需要和获授权访问资料的人员，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、某资料类别或某些资料有疑问，应向部门安全事务主任查询。

9.1.9. 在终止或更改雇用后仍然生效的信息安全职责和职务须予界定，并须通知有关人员及确实执行。

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，并确保所有信息系统及资产均得到适当程度的保护。

10.1. 对资产的责任

10.1.1. 决策局／部门须确保能妥善持有、保存及备存一份信息系统、硬件资产、软件资产、有效保用证、服务协议和法律 / 合约文件的清单。

10.1.2. 除非符合「有需要知道」原则，并已获部门信息技术安全主任授权，否则不得披露可能会削弱系统安全的信息系统资料。

10.1.3. 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，以及所采用的信息系统控制措施，或执行有关措施的方式。

10.1.4. 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应商雇员须将计算机资源和有关资料移交及交还政府。

10.2. 资料分类

10.2.1. 决策局／部门须遵行政府安全要求中有关资料分类、标签和处理的要求。

10.2.2. 所有保密资料不论储存于何种媒体都必须加密储存。

10.3. 储存媒体的处理

10.3.1. 决策局／部门须管理使用和运送存有保密资料的储存媒体的事宜。

10.3.2. 存有保密资料的储存媒体须加以保护，以免在未获授权的情况下被访问、误用或受到实体损坏。

10.3.3. 在弃置或重用储存媒体前，必须把所有保密资料彻底清除或销毁。

11. 访问控制

决策局／部门须防止信息系统和资产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

11.1.1. 决策局／部门在向用户分配信息系统的资源和权限时，须贯彻最小权限原则。

11.1.2. 除非获相关数据拥有人授权，否则不得访问资料。

11.1.3. 访问储存保密资料的信息系统，须受逻辑访问控制要求限制。

11.1.4. 任何人士在未经适当认证前，不得访问保密资料。

11.2. 用户访问管理

11.2.1. 须详细记录有关批准、授予及管理用户访问权限的程序，包括用户登记／取消登记、密码传送及密码重设。

11.2.2. 须按照「有需要知道」原则授予用户数据访问权限。

11.2.3. 须限制和控制行使特别权限的情况。

11.2.4. 须明确界定及定期覆检用户权限及数据访问权限。须订定并记录覆检频率，并须备存有关批准和覆检访问权限的记录。

11.2.5. 所有用户权限及数据访问权限如在一段预定时间内无任何操作或不再需要时，必须注销。须订定及记录无任何操作的时间和相应的覆检频率。

11.2.6. 每个用户名称只限代表一名用户。除非得到部门信息技术安全主任明确的批准，否则不得使用共享或群组用户名称。

11.3. 用户责任

11.3.1. 用户须为以其用户名称进行的一切操作承担责任。

11.3.2. 除非在必要情况（例如需要求助台提供协助、与他人共享个人计算机及共用档案）下，否则密码不得共用或外泄。如须共享密码，则须事先得到部门信息技术安全主任明确的批准。密码无需再共用时，应立即更改。长期共用的密码应经常更改。

11.3.3. 须时刻妥善保护所储存的密码。通过不可信任的通讯网络传输的密码须加密处理。如无法加密处理，则须采用辅助控制措施，把所面对的风险减至可接受的水平。

11.4. 系统及应用系统访问控制

11.4.1. 认证方式须与所访问数据的敏感度相称。

11.4.2. 须控制连续数次登入失败的情况。

11.4.3. 决策局／部门须制订严格的密码政策，密码政策须至少详细规定最短密码长度、初次密码设定、受限制字词及格式、及密码更改周期，并包括挑选合适的系统及用户密码的指南。

11.4.4. 任何人员均不得撷取或以其它方式取得可容许未获授权访问的密码、解密匙或任何其它访问控制装置。

11.4.5. 任何信息系统启用前，所有由供应商提供的默认密码均须予更改。

11.4.6. 如怀疑密码已／正外泄，或因维修及支持服务的需要而向供应商透露密码，须立即更改密码。

11.5. 流动信息处理及远程访问

11.5.1. 决策局／部门须制订适当的使用政策及程序，订明有关流动信息处理及远程访问的安全要求。同时，须采取适当的安全措施，以防止他人在未获授权的情况下访问或披露这些设备所储存及处理的资料。此外，应向获授权用户提供有关安全威胁的讯息，而该等用户亦应承担及确认知悉其安全责任。

11.5.2. 须推行安全措施，以防止他人在未获授权的情况下远程访问政府信息系统及数据。

11.6. 物联网装置

11.6.1. 决策局／部门须界定并采取适当的安全措施，以确保物联网装置与数据的安全均与资料的类别相称。

11.6.2. 除非在技术上不可行，否则物联网装置须同样遵行本文件所列明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。

12. 加密方法

决策局／部门须确保适当及有效地使用加密方法，以保护资料的机密性、真确性及完整性。

12.1. 加密控制措施

12.1.1. 决策局／部门须于密码匙的整个生命周期管理密码匙，包括密码匙的产生、储存、存盘、获取、分发、退役及销毁。

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，以及防止对办工场地和信息系统造成阻碍。

13.1. 安全区域

13.1.1. 在设立特定用途的计算机中心时，须慎重进行选址及场地规划，并应视乎所建造的是特定用途设施或一般办公室，参考相关的安全规格。

13.1.2. 数据中心及计算机室须设于实体安全完善的环境，并受到严密保护，以抵御自然或其它因素所导致的灾难和安全威胁，从而将损失范围及服务中断的影响减到最低。

13.1.3. 数据中心及计算机室须按所处置的信息系统类别遵行政府关于实体安全的要求。

13.1.4. 须定期更新及覆检获授权进入数据中心、计算机室、放置或储存计算机设备及数据的其它关键操作地点的人员清单。

13.1.5. 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。

13.1.6. 获授权人员须时刻监视所有进入数据中心或计算机室的访客，并须妥善备存访客出入记录作审核用途。

13.1.7. 所有人员须确保其办公室的安全。如办公室设有信息系统或放置了信息资产，并可从公共地方直接进入，则应在无人使用时或办公时间后锁上。

13.2. 设备

13.2.1. 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。

13.2.2. 管有流动装置或抽取式媒体以作业务用途的人员，须保障有关装置的安全。在没有采取妥善安全措施的情况下，须避免装置无人看管。

13.2.3. 在没有采取适当控制措施的情况下，不得将信息技术设备带离场地。

13.2.4. 如系统在一段预定时间内无任何操作，则须启动重新认证功能或登出系统并中断联机，以免系统被非法访问。此外，在结束每天的工作前或长时间不操作的情况下，用户须关掉工作站（如情况合适）。

13.2.5. 须小心放置显示信息系统所载资料的屏幕，确保未获授权人士无法窥看屏幕所显示的保密资料。

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、记录信息技术程序及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

14.1.1. 决策局／部门须按照精简功能原则管理信息系统，并移除或限制使用所有不必要的服务或组件。

14.1.2. 须慎重考虑会影响现行安全保护机制的变更。

14.1.3. 须妥善记录、遵从，以及定期覆检信息系统的操作及管理程序。

14.2. 防范恶意软件

14.2.1. 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。

14.2.2. 决策局／部门须保护其信息系统免受恶意软件的影响，并定期和在有需要时更新恶意软件定义，以及其侦测和修复引擎。

14.2.3. 除非经过恶意软件检查及清除所有感染，否则不得使用从不明来源或源头取得的储存媒体和档案。

14.2.4. 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。

14.2.5. 计算机及网络所采用的软件必须从可信赖的来源取得。

14.2.6. 决策局／部门利用技术堵截与业务无关的网站时，应权衡轻重。

14.2.7. 从互联网下载的所有软件及档案必须经抗恶意软件解决方案扫描及检验。

14.2.8. 任何人员均不应启动从互联网下载的流动程序码或软件，除非有关程式码是从已知及可信赖的来源取得。

14.3. 备份

14.3.1. 须定期进行备份工作。

14.3.2. 决策局 / 部门须为其信息系统制订和推行备份及复原政策。

14.3.3. 须定期覆检备份工作。须定期进行备份复原测试。须订定并记录备份覆检和复原测试的频率。

14.3.4. 应防止备份媒体在未获授权的情况下被访问、滥用或损毁。

14.3.5. 储存必要及／或重要业务资料的备份媒体，须存放在与主要场地保持一段安全距离的地方，以免因主要场地发生灾难而受到破坏。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。

14.4. 记录

14.4.1. 决策局／部门须根据业务需要和数据的保密类别，制订并记录与辖下信息系统工作记录（包括保存期）有关的政策。

14.4.2. 安全记录须提供足够的资料，以作为对安全措施的成效及遵行情况进行全面审计的凭证。

14.4.3. 记录保存期须与其作为有效审计工具的日期长短相称。在保存记录期间，须确保记录安全，以免被窜改，并确保只有获授权人士才可阅览记录。

14.4.4. 除非得到首长级人员的批准，作为审计工作所需，否则记录不得用作剖析个别用户的操作情况。

14.4.5. 各信息系统的时钟须与一个可信赖的时间来源同步。

14.5. 操作环境的控制

14.5.1. 各种计算机设备及软件须在控制措施及审计监督下安装。

14.5.2. 须利用更改控制程序控制信息系统的变更，并备存变更记录，以追踪曾作出的变更。

14.6. 技术性安全漏洞管理

14.6.1. 决策局／部门须进行安全漏洞管理流程，包括识别、评估、缓解和追踪其信息系统的漏洞。

14.6.2. 决策局／部门须根据风险水平，制订适当的修补程序管理策略，包括其信息系统的修补程序检查和修补频率。决策局／部门须采用风险为本的方法，考虑每个安全漏洞的潜在影响和被利用的可能性，为其制定修补计划。所有部署在与互联网连接的信息系统的服务器和相关装置都须受到严格的修补程序管理。

14.6.3. 决策局／部门须根据修补程序管理策略使用产品供应商推荐的最新安全修补程序或采取其它辅助安全措施，以保护其信息系统免受已知安全漏洞的影响。

14.6.4. 在使用安全修补程序前，应进行适当的风险评估及测试，以尽量减少对信息系统的不利影响。

14.6.5. 未经决策局／部门指定人员事先批准，不得将未获授权的应用软件载入政府信息系统。

14.7. 信息技术安全威胁管理

14.7.1. 决策局／部门须建立威胁识别、侦测和监察机制，并定期覆检该机制，以确保其在信息系统性质和技术进步方面的成效。

14.7.2. 须定期检查记录（尤其是处理／储存保密资料的系统／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系统及应用系统误差，均须予以呈报和记录。

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资料的安全。

15.1. 网络安全管理

15.1.1. 须妥善备存内部网址、配置及相关系统或网络的数据。未经有关决策局／部门批准，不得公开这些资料。

15.1.2. 须妥善保护与其它政府网络或公众可访问的计算机网络连接的所有内部网络。

15.1.3. 须妥善配置及管理信息／通讯系统，并定期覆检。

15.1.4. 决策局／部门须将其网络划分为分隔的网域，以建立安全边界，并加强对不同网域之间的控制。

15.1.5. 与另一个网络连接的接线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。

15.1.6. 未获授权的计算机资源（包括私人拥有的计算机资源）不得连接至政府内部网络。如有运作上的需要，事前须得到部门信息技术安全主任的批准。决策局／部门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。

15.1.7. 决策局／部门须记录、监察及控制接驳政府内部网络的无线通讯。

15.1.8. 须采取适当的认证及加密安全措施，以保护通过接驳政府内部网络的无线通讯的数据传输。

15.1.9. 必须通过中央安排的互联网网关或决策局／部门内部已推行安全架构及适当安全措施的互联网网关访问互联网。如情况不许可，或为顺应使用形式 2，决策局／部门宜考虑准许使用独立计算机访问互联网，惟决策局／部门必须在适当的级别设立审批和控制机制。

15.1.10. 除非得到部门信息技术安全主任的批准，否则所有人员不得利用拨号调解器、无线界面或宽带链路等通讯装置，将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。

[2] 使用形式可包括公干时上网、收发电子邮件及使用政府的便携式计算机等。在上述情况下，仍须采取任何适用的安全措施保护独立计算机。

15.2. 资料传送

15.2.1. 机密以上保密类别的数据必须经过加密处理，并只限于在已获政府安全事务主任批准及数字政策办公室技术认可的独立局部区域网络内传递。

15.2.2. 机密／限阅数据在不可信赖的通讯网络上传递时必须加密，在任何通讯网络上传递时亦应尽可能加密。

15.2.3. 如传递载有保密资料的电子邮件，必须通过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信息系统传递。

15.2.4. 系统管理员须订立及维持有系统的程序，以记录、保存及删除电子邮件讯息及相关的记录。

15.2.5. 必须妥善备存和保护包含获授权用户或政府网站资料的内部电子邮件通讯簿，以免在未获授权的情况下被访问和窜改。

15.2.6. 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资料的协议。

15.2.7. 不应打开或转寄可疑来源的电子讯息。

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

16.1.1. 在发展系统时，须根据系统的安全要求进行安全规划，并推行适当的安全措施及控制措施。

16.2. 发展和支援程序的安全

16.2.1. 决策局／部门须建立及适当地保护用作系统发展的环境，以及涵盖整个系统发展周期的整合工作。

16.2.2. 须妥善备存应用系统的文件、程式源码和清单，访问这些文件、程式源码和清单时须受「有需要知道」原则限制。

16.2.3. 在推行安全措施前，须正式测试及覆检有关措施。

16.2.4. 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。

16.2.5. 须记录有关要求及审批程序／系统变更的更改控制程序。

16.2.6. 决策局／部门须确保已正式通知有关人员信息系统配置更改后对安全和信息系统用途的影响。

16.2.7. 除非得到资料拥有人的批准，否则应用系统发展及系统支援人员不得访问生产系统内的保密数据。

16.3. 测试数据

16.3.1. 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。如确有需要使用生产环境的保密资料，须覆检及记录有关过程，并得到数据拥有人的批准。

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

17.1.1. 外聘服务供应商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，以及政府发出的其它信息安全要求。

17.1.2. 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。决策局／部门须记录及推行根据资料类别及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，并订明及商定外聘服务供货商的安全职责。

17.2. 外包服务交付管理

17.2.1. 决策局／部门须监察外聘服务供应商，并与他们进行覆检，以确保外聘服务供应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资料的协议，并须在出现任何影响安全要求的变更时，覆检有关协议。

17.2.2. 决策局／部门须保留审核及监察遵行安全要求的权利，以确保外聘服务供应商为政府信息系统、设施及资料采取足够的控制措施。另外，外聘服务供应商须定期提交安全审计报告，以证明所采取的措施达到满意程度。

17.2.3. 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或在政府的要求下，根据政府的安全要求予以清除或销毁。

17.3. 云端运算安全

17.3.1. 限阅或以上保密类别的数据不得利用公共云端服务储存或处理。

17.3.2. 在与云端服务供货商签署协议之前，决策局／部门须确保已明确界定、记录并明白双方的共同责任。

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. 安全事故的管理和改进

18.1.1. 决策局／部门须制订一套事故侦测及监察机制，以侦测、遏制并最终防止安全事故的发生。

18.1.2. 决策局／部门须保留系统记录及其它证明资料，以供证明及追踪安全事故之用。

18.1.3. 决策局／部门须为其信息系统制订、记录、测试及备存一套安全事故应变计划。

18.1.4. 所有人员须对现行安全事故应变计划有充分认识，并须遵守和遵从有关程序。

18.1.5. 如发现或怀疑信息系统或服务出现任何安全事故或安全问题，必须即时向负责人士汇报，并根据事故处理程序处理。

18.1.6. 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资料。

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中的内容包括信息系统的可用性及安全考虑。

19.1. 持续信息技术安全

19.1.1. 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。

19.2. 复原能力

19.2.1. 决策局／部门须确保有足够复原能力，以符合信息技术服务及设施在可用性方面的要求。

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

20.1.1. 决策局／部门须就每个信息系统的操作定出及记录所有适用的相关法定、规管及合约要求。

20.1.2. 决策局／部门须备存记录，以证明已遵行安全要求，以及协助就相关安全措施是否已有效推行进行审计。

20.1.3. 决策局／部门须遵守政府要求中所载有关信息系统安全的规定，包括但不限于保密资料的储存、传递、处理及销毁。同时，应保护没有列入任何保密类别的资料，以防止该等资料不慎外泄。

20.1.4. 处理个人数据时须遵守《个人数据（私隐）条例》（第 486 章）的规定。所有个人资料应列为限阅或以上类别。视乎有关个人数据的性质和敏感度，以及资料在未获授权或意外的情况下被访问、处理、删除或作其它用途而引致的损害，可能须采用较高的保密类别和采取合适的安全措施。

20.2. 安全审查

20.2.1. 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。信息系统或生产应用系统在投入生产前，以及在进行大规模升级和变更前，也须进行安全风险评估。

20.2.2. 须至少每两年对信息系统进行一次审计，以确保有关各方已遵行信息技术安全政策和采取有效的安全措施。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。

20.2.3. 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。

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