數字政策辦公室

資訊保安

基準資訊科技保安政策

[S17]

第 8.1 版

2024 年 7 月

版權公告

修改記錄

修改次數	修改詳情	經修改頁數	版本編號	日期
1	修改報告可於政府資訊科技情報網查閱		2.0	2003 年 4 月
2	將「資訊科技署」更改為「政府資訊科技總監辦公室」		2.1	2004 年 7 月
3	將英文版中香港電腦保安事故協調中心的簡稱由「HKCERT/CC」更新為「HKCERT」	無	2.2	2004 年 9 月
4	作出相應更新，以符合經修訂的政府保安要求	11-1, 11-2	2.3	2004 年 11 月
5	修改報告可於政府內聯網「資訊科技情報網」查閱		3.0	2006 年 5 月
6	修改第 8.3.1 及 9.1.6 節並加入遵守《個人資料（私隱）條例》的要求	8-1, 9-1	3.1	2008 年 11 月
7	修改報告可於政府內聯網「資訊科技情報網」查閱		4.0	2009 年 12 月
8	修改報告可於政府內聯網「資訊科技情報網」查閱		5.0	2012 年 9 月
9	修改報告可於政府內聯網「資訊科技情報網」查閱		6.0	2016 年 12 月
10	修改報告可於政府內聯網「資訊科技情報網」查閱 (https://itginfo.ccgo.hksarg/content/itsecure/review2021/documents.shtml)		7.0	2021 年 3 月
11	修改報告可於政府內聯網「資訊科技情報網」查閱		8.0	2024 年 4 月

12	將「政府資訊科技總監辦公室」更改為「數字政策辦公室」 將「香港電腦保安事故協調中心」更改為「香港網絡安全事故協調中心」		8.1	2024年7月

目錄

1. 目的

隨着各界有效使用互聯網服務，以及普遍採用雲端運算和流動資訊處理技術，資訊系統的保安及持續性對經濟和社會至關重要。辦公室工作和公共服務愈來愈依賴資訊科技，為政府業務帶來了新重點，就是我們所依賴的主要資訊系統和數據必須安全並得到妥善保護，確保所有決策局／部門均能暢順運作，藉此鞏固市民信心、保障資訊保安及私隱，這是政府業務能以具效益、有效率和安全的方式運作的基礎。

本文件概述為保護香港特別行政區政府所有資訊系統及數據資產而訂定的強制性基本保安要求。決策局／部門須通過下列方式制訂、記錄、推行、維持和覆檢適當的保安措施，以保護其資訊系統及數據資產：

- 在內部訂立符合本文件所載規定的適當資訊科技保安政策、規劃和監管措施，包括採用所有架構及要求；
- 確保推行本文件所述的適當保安措施；
- 確保定期覆檢保安措施的持續適用性、足夠性和效益；以及
- 改善保安措施的適用性、足夠性和效益。

本文件所述的保安要求是以科技中立的角度制訂。本政策的要求著重基本目標和控制措施，以保護在處理、儲存及傳遞中的資料。

2. 範圍

2.1. 適用性

本文件採用國際標準化組織（ISO）及國際電工委員會（IEC）所訂立的資訊保安、網絡保安和私隱保護—資訊保安管理體系—要求（ISO/IEC 27001:2022）及資訊保安、網絡保安和私隱保護—資訊保安控制（ISO/IEC 27002:2022），並在有關保安範疇及控制措施的部分作調整。本文件就下列14個範疇提出強制性指引：

- 管理職責（見第7節）；
- 資訊科技保安政策（見第8節）；
- 人力資源保安（見第9節）；
- 資產管理（見第10節）；
- 接達控制（見第11節）；
- 加密方法（見第12節）；
- 實體及環境保安（見第13節）；
- 操作保安（見第14節）；
- 通訊保安（見第15節）；
- 系統購置、發展及維護（見第16節）
- 外判資訊系統的保安（見第17節）
- 保安事故管理（見第18節）；
- 資訊科技保安方面的業務持續運作管理（見第19節）；以及
- 遵行要求（見第20節）

本文件載列的是各項基本保安要求。決策局／部門需因應本身的情況及已確定的風險，推行更嚴謹的保安措施。

2.2. 對象

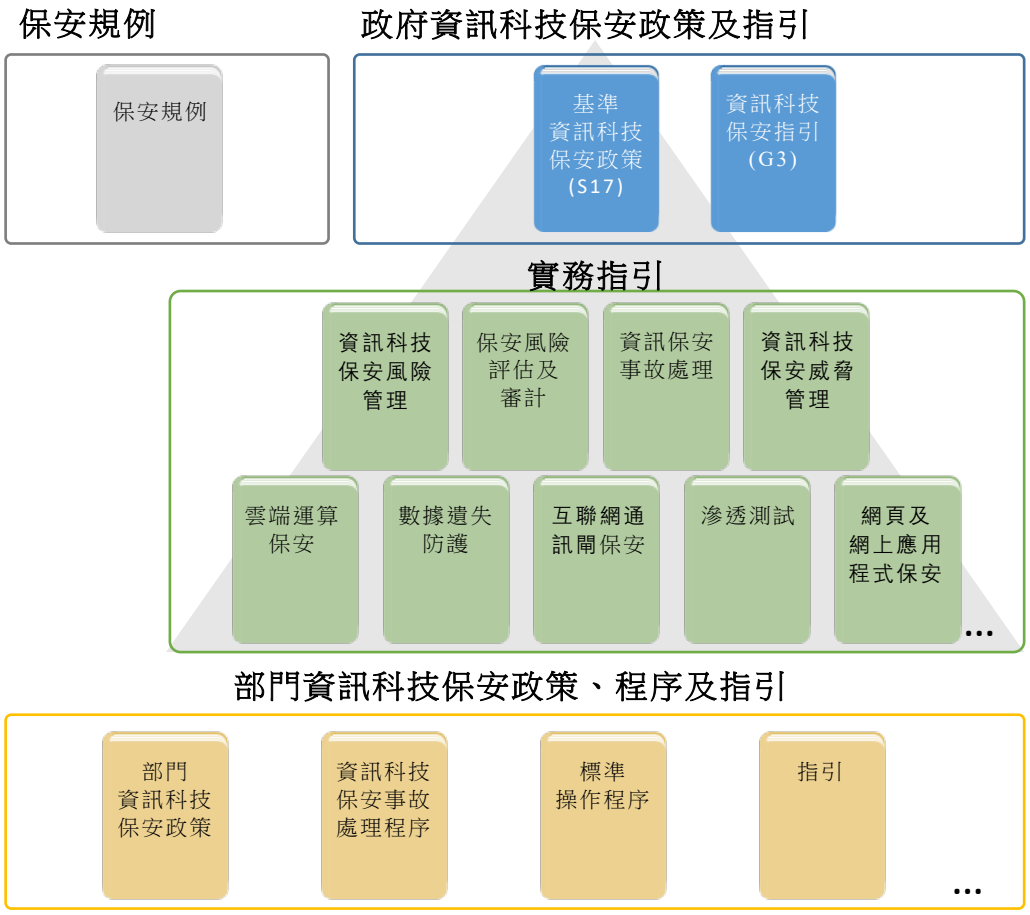
本政策是為各決策局／部門內擔當不同職務的各級人員制訂，當中包括管理人員、資訊科技管理員和一般的資訊科技終端用戶。全體人員均有責任通篇閱讀整份文件，以了解並遵行資訊科技保安政策。

另外，本文件亦供為政府提供資訊科技服務的供應商、承辦商及顧問作為參考。

2.3. 政府資訊科技保安文件

政府已發布一系列保安規例、政府資訊科技保安政策及指引，協助決策局／部門制訂及推行保障政府資訊保安的資訊科技政策及控制措施。決策局／部門須遵行《保安規例》、《基準資訊科技保安政策》[S17]及《資訊科技保安指引》[G3]內的政策要求，以及遵從相關的實務指引內的實施指引。這些保安文件是資訊保安管理不可或缺的參考資料。

下圖顯示政府內部多份資訊科技保安文件之間的關係：



2.3.1. 《保安規例》

由保安局授權的《保安規例》訂明哪些文件、材料及資訊需列作保密資料，並確保這些文件、材料及資訊在政府業務運作過程中得到充分保護。

2.3.2. 政府資訊科技保安政策及指引

由數字政策辦公室制訂的政府資訊科技保安政策及指引旨在提供相關參考，方便推行資訊保安措施，以保障資訊資產。這些文件參考了 ISO 及 IEC 所出版的資訊保安、網絡保安和私隱保護—資訊保安管理系統—要求（ISO/IEC 27001:2022）及資訊保安、網絡保安和私隱保護—資訊保安控制（ISO/IEC 27002:2022）。

政府資訊科技保安政策及指引訂明保安要求的最低標準，並提供有關推行適當保安措施以保護資訊資產和資訊系統的指導。

《基準資訊科技保安政策》 [S17]	最高層次的指令文件，為所有決策局／部門制訂保安規格必須達到的最低標準。這份文件列明了對決策局／部門至關重要的保安工作領域。《基準資訊科技保安政策》可視為必須遵守的強制性基準規例，各決策局／部門亦可採取其他合適的措施加強保安。
《資訊科技保安指引》 [G3]	就《基準資訊科技保安政策》所列明的保安要求闡釋當中的政策要求，以及訂定相關實施標準。決策局／部門必須遵行《資訊科技保安指引》，以有效實施相關保安要求。

我們亦因應不同專題和特定的技術要求制訂了一系列實務指引，以補充《資訊科技保安指引》的內容，並就特定保安範疇提供指導說明，協助決策局／部門應對及減低新興科技及保安威脅所帶來的風險。

這些實務指引已載於政府資訊科技情報網的資訊科技保安專題網頁 (https://itginfo.ccgo.hksarg/content/itsecure/techcorner/practices.shtml)。

2.3.3. 部門資訊科技保安政策、程序及指引

決策局／部門須根據上文第 2.3.1 及 2.3.2 節所述《保安規例》及政府資訊科技保安政策及指引內列明的所有政府保安要求及實施指引，制訂本身的部門資訊科技保安政策、程序及指引。

3. 參考標準

a) 香港特別行政區政府《保安規例》

b) 公務員事務局《公務員事務規例》

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) 信息安全技術 網絡安全等級保護基本要求，GB/T 22239-2019，發布於2019年5月10日

4. 定義及慣用詞

4.1. 定義

a)	第 1 級資訊系統	由硬件及軟件組成的系統，用作收集、處理、儲存、傳遞或棄置資料，不論其資金來源及項目類型。
b)	第 2 級資訊系統	對政府或社會運作重要的第 1 級資訊系統，其故障或中斷會對政府運作帶來嚴重影響，或可能引致公眾混亂及災難性後果。
c)	必要服務	對社會及其經濟的運作和安全必要的服務。
d)	第 3 級資訊系統	與提供有關的必要服務直接相關且其中斷或破壞可能對經濟、民生、公共安全等造成嚴重損害的第 2 級資訊系統。
e)	機密性	在任何方面只有獲授權人士及資訊系統能夠知悉或接達資訊系統所儲存或處理的資料。
f)	完整性	在任何方面只有獲授權人士及資訊系統能夠修改資訊系統所儲存或處理的資料。
g)	可用性	資訊系統在獲授權人士及資訊系統提出要求時，可供該人士資訊系統接達及使用。
h)	資訊科技保安政策	明文規定的管理指示，詳細闡述如何妥善使用和管理電腦及網絡資源，以保護有關資源和資訊系統所儲存或處理的資料免在未獲授權的情況下被披露、竄改或破壞。
i)	保密資料	按《保安規例》劃分的各類保密資料。
j)	人員	受聘為政府工作的人士，或其服務是用以為政府工作的人士的統稱，包括無論僱用期及僱用條件的所有公職人員、通過中介公司聘用的非政府借調人員，以及其他提供定期合約服務的人士等。此等人士在接達保密資料方面可能有不同權限，亦受到不同的保安審查規定規管。有關人力資源保安的具體規定載於《基準資訊科技保安政策》第 9 節。

k)	數據中心	放置資訊系統及相關設備的中央數據處理設施。
l)	電腦室	放置電腦設備的專用房間。
m)	惡意軟件	蓄意進行未獲授權的程序以破壞資訊系統的機密性、完整性或可用性的程式。惡意軟件的例子包括電腦病毒、蠕蟲、木馬程式及間諜軟件。
n)	流動裝置	可儲存及處理資料的便攜式電腦及通訊裝置。例子包括便攜式電腦、流動電話、平板電腦、數碼相機、錄音或錄像裝置。
o)	抽取式媒體	可插入電腦裝置及從電腦裝置移除的便攜式電子儲存媒體，例如磁性、光學和閃存記憶裝置。例子包括外置硬磁碟或固態硬碟、軟磁碟、壓縮磁碟、光碟、磁帶、記憶卡、閃存盤和類似的通用串列匯流排儲存裝置。
p)	物聯網裝置	具有網絡連接和運算功能的裝置，通過感應或致動的方式自動與實體環境互動。

4.2. 慣用詞

本文件的慣用詞載列如下：

須 「須」表示強制性規定。

應 「應」表示良好作業模式，應盡可能貫徹執行。

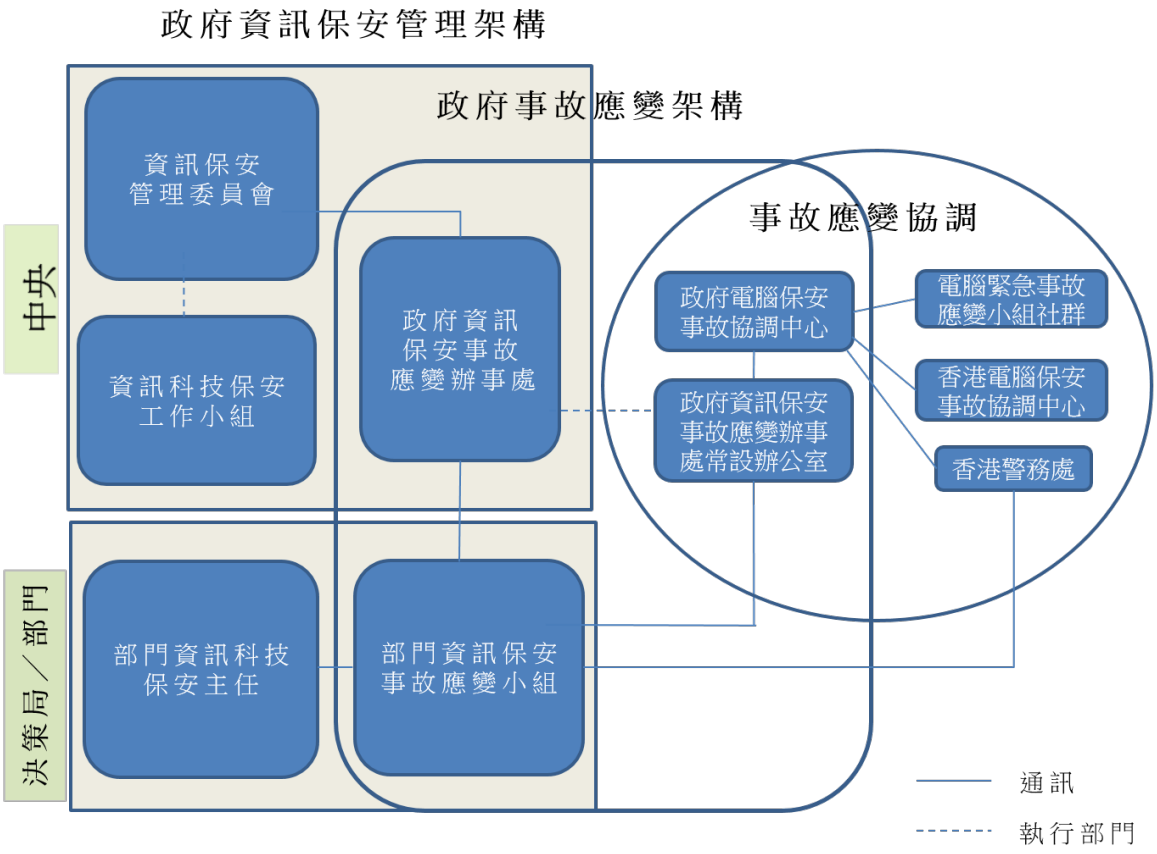
宜 「宜」表示期望達到的良好作業模式。

5. 政府資訊保安組織架構

5.1. 政府資訊保安管理架構

為協調及推動政府內部的資訊科技保安工作，政府設立了由以下五方組成的資訊保安管理架構：

- 資訊保安管理委員會
- 資訊科技保安工作小組
- 政府資訊保安事故應變辦事處
- 政府電腦保安事故協調中心
- 決策局／部門



政府資訊保安管理架構

以下幾節將詳細介紹有關各方所擔當的職務和職責。

5.1.1. 資訊保安管理委員會

資訊保安管理委員會為中央組織，成立於 2000 年 4 月，以監督整個政府內部的資訊科技保安工作。委員會定期舉行會議，以：

- 覆檢與政府資訊科技保安有關規例、政策及指引，並批准有關修訂；
- 界定與資訊科技保安相關的具體職務和職責；以及
- 通過資訊科技保安工作小組就實施與資訊科技保安有關規例、政策及指引，向決策局／部門提供指導及協助。

資訊保安管理委員會的核心成員包括下列決策局／部門的代表：

- 數字政策辦公室
- 保安局

委員會將按需要就特定事宜從其他決策局／部門增選代表。數字政策辦公室會依照本文件的要求，協助覆檢並釐清各決策局／部門提交的文件。

5.1.2. 資訊科技保安工作小組

資訊科技保安工作小組作為資訊保安管理委員會的執行部門，負責發布與政府資訊科技保安相關的規例、政策及指引，並監督其遵行情況。資訊科技保安工作小組於 2000 年 5 月成立，其職責如下：

- 協調各項工作，以期就實施與資訊科技保安相關的規例、政策及指引向決策局／部門提供指導及協助；
- 監督決策局／部門對《基準資訊科技保安政策》的遵行情況；
- 訂定及覆檢與資訊科技保安相關的規例、政策及指引；以及
- 提高政府內部對資訊科技保安的意識。

資訊科技保安工作小組的核心成員包括下列決策局／部門的代表：

- 數字政策辦公室
- 保安局
- 香港警務處
- 政務司司長辦公室

工作小組將按需要就特定事宜從其他決策局／部門增選代表。

5.1.3. 政府資訊保安事故應變辦事處

為處理決策局／部門內部的資訊保安事故，各決策局／部門須成立資訊保安事故應變小組。同時，政府資訊保安事故應變辦事處將集中協調並支援各決策局／部門資訊保安事故應變小組的運作。政府資訊保安事故應變辦事處常設辦公室是該辦事處的執行部門。

政府資訊保安事故應變辦事處的主要功能如下：

- 設立中央資料庫，並監督政府內部處理所有資訊保安事故的工作；
- 定期編製政府資訊保安事故統計報告；
- 充當中央協調辦事處，以協調處理多點保安攻擊（即不同的政府資訊系統同時受到攻擊）的工作；以及
- 促使各決策局／部門的資訊保安事故應變小組之間互相分享和交流資訊保安事故處理的經驗和資料

政府資訊保安事故應變辦事處的核心成員包括下列決策局／部門的代表：

- 數字政策辦公室
- 保安局
- 香港警務處

5.1.4. 政府電腦保安事故協調中心

政府電腦保安事故協調中心於 2015 年 4 月成立。除與政府資訊保安事故應變辦事處常設辦公室合作，協調政府內部的資訊及網絡安全事故外，政府電腦保安事故協調中心亦會與電腦緊急事故應變小組社群分享事故資訊及威脅情報，並就良好作業模式進行交流，藉此加強地區內的資訊和網絡安全能力。政府電腦保安事故協調中心的主要功能如下：

- 就即將及已經發生的威脅向決策局／部門發出保安警報；以及
- 在處理網絡安全事故時，充當香港網絡安全事故協調中心與其他電腦保安事故緊急應變小組之間的橋樑。

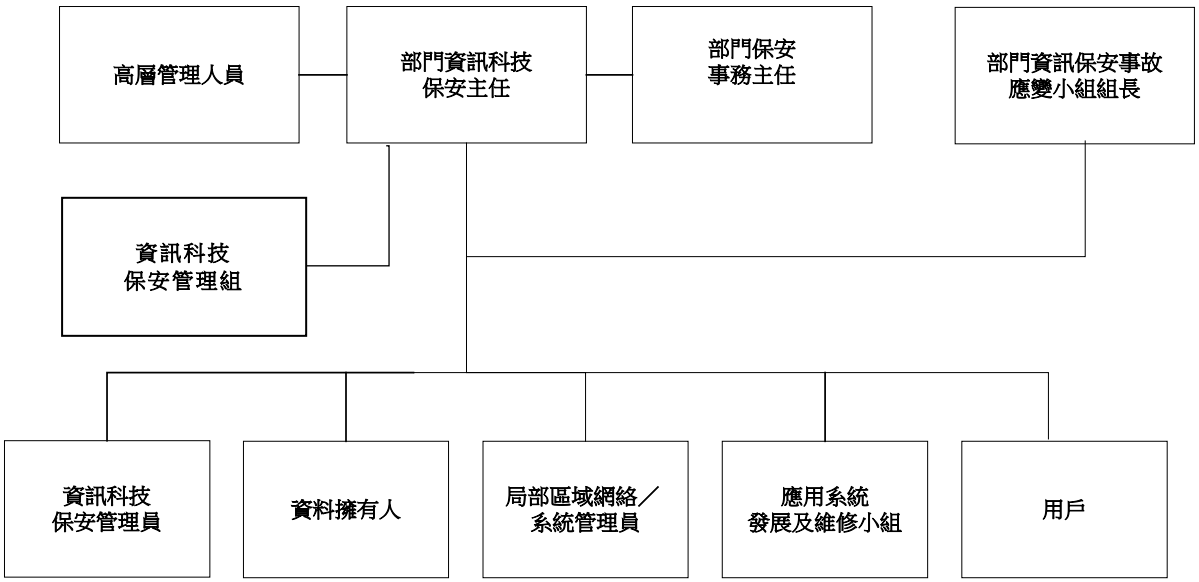
5.1.5. 決策局／部門

決策局／部門須負責確保其資訊資產和資訊系統的安全。有關決策局／部門內部資訊科技保安人員的職務和職責詳情，載於第 5.2 節—部門資訊科技保安組織。

5.2. 部門資訊科技保安組織

本章節闡述部門資訊科技保安組織中個別人員的職務和職責。為確保職務分工恰當，除非受到資源限制，否則不應指派一名人員擔當多項職務。

下圖為部門資訊科技保安管理架構的示例：



部門資訊科技保安管理組織架構圖示例 [1]

5.2.1. 高層管理人員

決策局／部門的高層管理人員須正確認識資訊科技保安、保安問題和解決方法。高層管理人員的職責包括：

- 在決策局／部門內發揮領導才能，推動和優先考慮資訊科技保安；
- 指揮及落實制訂保安措施；
- 提供推行保安措施所需的資源；
- 確保各級管理、行政、技術及操作人員對資訊科技保安工作的參與及問責，並向他們提供一切支援；
- 在決策局／部門上下推動保安意識和問責文化；以及
- 確保決策局／部門的資訊科技保安策略配合業務目標。

[1] 實際的資訊科技保安管理架構可能會因應各部門的情況而有所不同。

5.2.2. 部門資訊科技保安主任

決策局局長／部門首長須從高層管理人員中委任一名人員，擔任部門資訊科技保安主任，負責資訊科技保安工作。負責決策局／部門資訊科技管理工作的首長級人員可視作適合擔當部門資訊科技保安主任的職務。視乎部門規模，首長級的部門職系人員如了解有關決策局／部門的緩急需要、該決策局／部門資訊系統及數據資產的重要性，以及保障該決策局／部門所須達到的保安級別，亦可視作合適人選。

保安局和數字政策辦公室會為部門資訊科技保安主任提供培訓，以便他們執行職務。部門資訊科技保安主任須出席指定的培訓。部門資訊科技保安主任的職務和職責須清晰界定，包括但不限於：

- 制訂和維持資訊保護計劃，以協助全體人員保護所使用的資訊及資訊系統；
- 制訂適當的保安監管程序，以評估、指導、監察及傳達決策局／部門內有關資訊科技保安的工作；
- 推動高層管理人員定期討論資訊科技保安問題，以獲得足夠的支援和資源；
- 帶領有關制訂、維持及推行資訊科技保安政策、標準、程序及指引的工作；
- 在資訊科技操作的各階段監督、監察、覆檢和改善資訊科技保安管理工作的效益和效率；
- 監察並確保遵行政府資訊科技保安要求；
- 監督決策局／部門內的整體資訊科技保安意識及培訓計劃；
- 在資訊科技保安事務上與其他決策局／部門協調；
- 監督決策局／部門內的整體資訊科技風險管理程序，包括確保進行必要的資訊保安風險評估和審計，並應對不斷變化的風險形勢、監管變化、技術改良和系統關鍵性；
- 向決策局／部門的負責人傳達政府資訊保安事故應變辦事處就即將及已經發生的威脅所發出的保安警報；以及
- 就違反保安事件主動展開調查並作出修正。

5.2.3. 部門保安事務主任

決策局局長／部門首長會指派一名部門保安事務主任負責部門內的保安相關工作。部門保安事務主任將擔當執行人員的職務，以：

- 履行決策局／部門內的所有保安職責；以及
- 就保安政策的制訂及覆檢提出建議。

部門保安事務主任可兼任部門資訊科技保安主任。如決策局／部門委任他人為部門資訊科技保安主任，部門資訊科技保安主任須與部門保安事務主任合作，共同監督決策局／部門的資訊科技保安工作。

5.2.4. 部門資訊保安事故應變小組組長

部門資訊保安事故應變小組是協調處理決策局／部門內資訊保安事故的中央聯絡點。決策局局長／部門首長應從高層管理人員中挑選一名人員，擔任資訊保安事故應變小組組長。資訊保安事故應變小組組長應有權委任資訊保安事故應變小組的核心成員。資訊保安事故應變小組組長的職責包括：

- 全面監督及協調處理決策局／部門內所有資訊系統的資訊保安事故；
- 就控制損毀、系統復原、外部機構委聘及其所參與工作的程度，以及復原後恢復正常服務的後勤工作的關鍵事項作出決策；
- 因應事故對決策局／部門業務運作的影響，在適當情況下啓動部門的運作復原程序；
- 代表管理層批核為事故處理程序投放的資源；
- 代表管理層批核就事故的立場所作的公眾發布；
- 與政府資訊保安事故應變辦事處合作，報告資訊保安事故，以便作中央記錄及採取必要的跟進行動；以及
- 促進決策局／部門內部互相交流和分享資訊保安事故處理及相關事宜的經驗和資料。

5.2.5. 資訊科技保安管理組

決策局／部門須設立資訊科技保安管理組，向部門資訊科技保安主任報告並協助部門資訊科技保安主任履行職責。各決策局／部門的資訊科技保安管理組的規模及組成可能有所不同，視乎各決策局／部門的業務及運作需求而定。資訊科技保安管理組的職責包括：

- 協助部門資訊科技保安主任制訂、建立和備存決策局／部門的整體資訊科技保安策略和路線圖，包括制定資訊科技保安政策、基準、標準、指令等；
- 協調決策局／部門內的保安意識及培訓計劃；
- 協調資訊科技保安措施的推行並監察資訊科技保安流程的進度，以確保資訊科技保安管理的成效並符合政府保安要求；
- 推動資訊科技保安威脅和風險管理活動，並支援與資訊科技保安相關的運作復原和業務持續運作計劃職能；以及
- 履行部門資訊科技保安主任指示的任何其他職責。

5.3. 其他職務

5.3.1. 資訊科技保安管理員

資訊科技保安管理員須負責提供有關保安及風險管理方面的支援服務。資訊科技保安管理員的職責還包括：

- 協助找出並緩解系統的保安漏洞；
- 協助進行修補程式管理流程；
- 執行保安管理工作，例如推行接達控制和管理用戶權限；
- 備存和覆檢審計記錄；
- 監察威脅情報來源並適時了解新興保安威脅；以及
- 操作和維護保安工具和系統，例如入侵偵測和防禦系統。

資訊科技保安管理員不應由系統管理員兼任。資訊科技保安管理員與系統管理員兩者的職務應有清晰的分工。

資訊科技保安管理員雖然負責管理審計記錄，但不應竄改或更改任何審計記錄。

決策局／部門可委任一名資訊科技保安審計師，負責審計資訊科技保安管理員的工作，以確保其盡忠職守。

5.3.2. 資料擁有人

資料擁有人須為整理和擁有資訊系統內所儲存資料的人士。資料擁有人的主要職責是：

- 決定資料的保密類別、授權資料的用途，以及保護資料的相應保安要求。

5.3.3. 局部區域網絡／系統管理員

局部區域網絡／系統管理員須負責決策局／部門內部電腦系統和網絡的日常管理、運作及配置工作，而互聯網系統管理員則負責處理與連接互聯網的資訊系統相關的工作。局部區域網絡／系統管理員及互聯網系統管理員的職責包括：

- 根據部門資訊科技保安主任制訂的程序／指引，推行保安機制和控制措施。

5.3.4. 應用系統發展及維修小組

應用系統發展及維修小組須負責通過使用優良的程序、技術和工具，以發展優良的資訊系統。該小組的職責包括：

- 聯絡資料擁有人，以便在應用程式的開發和維護過程中訂定和執行系統保安要求；以及
- 確保使用優良的程序、技術和工具開發安全的系統。

5.3.5. 用戶

資訊系統的用戶必須是獲授權接達和使用資料的人員。用戶須為自己的一切活動負責。用戶的責任包括：

- 參與決策局／部門指示的保安意識及培訓計劃；
- 盡量了解、認識、遵從及運用一切可行及可用的保安機制；
- 防止其所保管的資料外泄和遭他人在未獲授權的情況下接達；以及
- 盡力安全地保管電腦和儲存裝置，防止他人在未獲授權的情況下接達或惡意攻擊該等裝置。

6. 核心保安原則

本章節闡述一些廣為接納並從宏觀角度應對資訊保安事宜的原則。這些原則屬基本原則，甚少改變。決策局／部門須遵守這些原則，以制訂、推行和了解保安政策。下列資訊保安原則並非詳盡無遺：

- **資訊系統保安目標**

  資訊系統保安的目標或宗旨可通過下述三項整體目標說明：機密性、完整性和可用性。保安政策和措施須按這三項目標制訂及推行。

- **風險為本的方法**

  須採用風險為本的方法，以一致及有效的方式為資訊系統識別保安風險、訂定應對風險的緩急次序和應對有關風險。須依照第7.2節所述的資訊科技保安等級保護推行適當的保安措施，以保護資訊資產及系統，並把保安風險減至可接受的水平。

- **設計層面的保安**

  須採用設計層面的保安概念，將保安要求納入軟件發展周期，確保資訊系統和應用程式採取適當的保安和資料保護措施。在開發過程的所有階段均須考慮和引入保安元素，以盡量減少重做系統所需的工作。

- **預防、偵測、應變和復原**

  資訊保安涵蓋預防、偵測、應變和復原措施。預防措施用於避免或制止不利情況發生。偵測措施用於識別已出現的不利情況。應變措施是指在不利情況（或事故）發生時所作出的協調行動，以控制損毀。復原措施則是令資訊系統的機密性、完整性和可用性回復至預定狀態。

- **處理、傳輸和儲存資料時的保護措施**

  處理、傳輸和儲存資料時，須視乎情況考慮及推行保安措施，以維持資料的機密性、完整性和可用性，例如欠缺保護的無線通訊容易遭受攻擊，傳輸保密資料時須採取保安措施。

- **外部系統假定為不安全**

  一般來說，外部系統須假定為不安全。決策局／部門在把其資訊資產或資訊系統連接至外部系統時，須根據業務要求及相關的風險水平，以實體或邏輯方式推行保安措施。

- **重要資訊系統的復原能力**

  所有重要資訊系統須具備復原能力，以應付嚴重的服務中斷情況。決策局／部門亦須採取措施，以偵測服務中斷情況、盡量減低破壞，以及迅速應變和使系統迅速復原。於復原計劃中，須考慮並適當地推行損害控制措施，以限制事故範圍、強度及影響，令系統能有效復原。

- **審計和問責**

  資訊保安須加入審計和問責元素。審計是指通過審計追蹤、系統記錄、警報或其他提示訊息等證據，核實資訊系統內的活動。問責是指審核所有曾與資訊系統互動的人士／機構的活動和所涉及的程序。須根據資料的敏感度，明確界定和定出有關各方所擔當的職務和職責，並據此授予權限。

  決策局／部門須備存記錄，以證明已遵行保安要求，並協助就相關保安措施是否已有效推行進行審計。

- **持續改進**

  為了因應不斷轉變的環境和技術而作出更新，須推行一套持續改進程序，以監察、覆檢及改善資訊科技保安管理工作的效益和效率。保安措施的效能須定期予以評估，以確定是否達到資訊科技保安目標。

7. 管理職責

決策局局長／部門首長須落實執行有效的保安安排，以確保政府的資訊系統和數據資產得到保障，以及資訊科技服務能安全運作。

7.1. 一般管理

7.1.1. 決策局／部門須訂定其部門資訊科技保安組織架構，以及界定相關的職務和職責。

7.1.2. 決策局／部門須確保其保安保護措施能因應不斷轉變的環境和技術而更新。

7.1.3. 決策局／部門須充分利用職務分工，以避免由一人負責整個資訊系統的所有保安工作。

7.1.4. 決策局／部門須確保在其財政預算中預留撥款，以提供必需的保安保護措施和資源。

7.1.5. 在符合《個人資料（私隱）條例》的情況下，決策局／部門須保留權利查閱政府資訊系統所儲存或傳遞的各項資料。

7.2. 保安風險管理

7.2.1 決策局／部門須採用風險為本的方法處理資訊保安，以確保轄下資訊資產的機密性、完整性和可用性，並須確保資訊系統（包括外判系統）符合其他所有保安要求，並監察其員工及承辦商對保安政策、指引等的遵行情況。

7.2.2 決策局／部門須採取資訊科技保安等級保護，為其所有資訊系統（包括基礎設施及部門共享資訊科技服務）評級，無論其資金來源為何，並依系統等級推行分級的保安控制措施。所有資訊系統的系統評級詳情須妥善記錄。資訊系統等級須由決策局局長／部門首長或他們明確授權的首長級人員批准。

8. 資訊科技保安政策

決策局／部門須訂定並確實執行其資訊科技保安政策，以根據業務和保安要求，就保護資訊系統和資產的工作提供管理方向和支援。

8.1. 資訊科技保安的管理方向

8.1.1. 決策局／部門須發布及執行本身的資訊科技保安政策。決策局／部門須以《基準資訊科技保安政策》文件為基礎，制訂其政策。

8.1.2. 決策局／部門須定期覆檢資訊保安政策、標準、程序和指引。

8.1.3. 決策局／部門須清晰制訂並向用戶傳達有關正確使用資訊科技服務及設施的政策。

9. 人力資源保安

決策局／部門須確保參與政府工作的人員適合擔當有關職務，了解他們的職責，並對資訊保安風險有所警覺。決策局／部門須在新聘、更改或終止僱用過程中維護政府利益。

9.1. 新聘、僱用期間或終止僱用

9.1.1. 決策局／部門須在有關人員獲派任新職位時，告知他們其資訊科技保安職責，並須在他們受僱期內，定期提醒他們有關職責。

9.1.2. 資訊保安是政府全體人員均須承擔的責任。決策局／部門須向各人員提供有關保安意識的適當培訓，並定期為他們提供有關資訊科技保安政策的最新資訊。

9.1.3. 決策局／部門須定期教育及培訓人員，使他們能履行與資訊科技保安有關的職責和職務。

9.1.4. 獲授權可接達限閱以上類別保密資料的公務員，須按照公務員事務局局長的規定接受操守審查。至於並非公務員的人員，決策局／部門應根據業務要求、有關人員所處理資料的類別和表面所知的風險，對該等人員進行適當的背景審查。

9.1.5. 決策局／部門須在其資訊科技保安政策中訂明，根據《公務員事務規例》，公務員如違反有關政策的任何條文規定，可能會受到紀律處分，而視乎違規事件的嚴重程度，有關人員可能受到不同程度的紀律處分。

9.1.6. 決策局／部門須在其資訊科技保安政策中訂明，所有並非公務員的人員（即上文第 9.1.5 節沒有涵蓋的人員）如違反有關政策的任何條文規定，則視乎違規事件的嚴重程度，可能受到根據其僱用條件而施行的相關處分，包括但不限於終止其向政府提供的服務。

9.1.7. 可使用或可在無人陪同的情況下接達資訊系統和有關資源的人員須經過嚴格挑選，亦須了解本身的職責和職務。決策局／部門須正式通知有關人員他們已獲授權接達資訊系統。

9.1.8. 任何人員不得發布、私自複製或向未獲授權人士傳遞其因公職身分而取得的保密文件或資料，除非有關人員基於政府利益而須這樣做，則作別論。「有需要知道」原則須適用於所有保密資料，這類資料應只提供給有需要和獲授權接達資料的人員，以便他們有效執行工作。如對某人員是否獲授權接達某份文件、某資料類別或某些資料有疑問，應向部門保安事務主任查詢。

9.1.9. 在終止或更改僱用後仍然生效的資訊保安職責和職務須予界定，並須通知有關人員及確實執行。

10. 資產管理

決策局／部門須給予所有硬件、軟件及資訊資產適當保護，並確保所有資訊系統及資產均得到適當程度的保護。

10.1. 對資產的責任

10.1.1. 決策局／部門須確保能妥善持有、保存及備存一份資訊系統、硬件資產、軟件資產、有效保用證、服務協議和法律／合約文件的清單。

10.1.2. 除非符合「有需要知道」原則，並已獲部門資訊科技保安主任授權，否則不得披露可能會削弱系統保安的資訊系統資料。

10.1.3. 所有人員不得向任何未獲授權人士披露資訊系統的性質和位置，以及所採取的資訊系統控制措施，或執行有關措施的方式。

10.1.4. 任何人員如被調職或停止向政府提供服務，該調職或離職人員或外聘服務供應商僱員須將電腦資源和有關資料移交及交還政府。

10.2. 資料分類

10.2.1. 決策局／部門須遵行政府保安要求中有關資料分類、標籤和處理的要求。

10.2.2. 所有保密資料不論儲存於何種媒體都必須加密儲存。

10.3. 儲存媒體的處理

10.3.1. 決策局／部門須管理使用和運送存有保密資料的儲存媒體的事宜。

10.3.2. 存有保密資料的儲存媒體須加以保護，以免在未獲授權的情況下被接達、誤用或受到實體損壞。

10.3.3. 在棄置或重用儲存媒體前，必須把所有保密資料徹底清除或銷毀。

11. 接達控制

決策局／部門須防止資訊系統和資產被未獲授權用戶接達及破解，並只容許獲授權的電腦資源連接至政府內部網絡。

11.1. 接達控制的業務要求

11.1.1. 決策局／部門在向用戶分配資訊系統的資源和權限時，須貫徹最小權限原則。

11.1.2. 除非獲相關資料擁有人授權，否則不得接達資料。

11.1.3. 接達儲存保密資料的資訊系統，須受邏輯接達控制要求限制。

11.1.4. 任何人士在未經適當認證前，不得接達保密資料。

11.2. 用戶接達管理

11.2.1. 須詳細記錄有關批准、授予及管理用戶接達權限的程序，包括用戶登記／取消登記、密碼傳送及密碼重設。

11.2.2. 須按照「有需要知道」原則授予用戶數據接達權限。

11.2.3. 須限制和控制行使特別權限的情況。

11.2.4. 須明確界定及定期覆檢用戶權限及數據接達權限。須訂定及記錄覆檢頻率，並須備存有關批准和覆檢接達權限的記錄。

11.2.5. 所有用戶權限及數據接達權限如在一段預定時間內無任何操作或不再需要時，必須註銷。須訂定及記錄無任何操作的時間和相應的覆檢頻率。

11.2.6. 每個用戶名稱只限代表一名用戶。除非得到部門資訊科技保安主任明確的批准，否則不得使用共用或群組用戶名稱。

11.3. 用戶責任

11.3.1. 用戶須為以其用戶名稱進行的一切操作承擔責任。

11.3.2. 除非在必要情況（例如需要求助台提供協助、與他人共用個人電腦及共用檔案）下，否則密碼不得共用或外泄。如須共用密碼，則須事先得到部門資訊科技保安主任明確的批准。密碼無需再共用時，應立即更改。長期共用的密碼應經常更改。

11.3.3. 須時刻妥善保護所儲存的密碼。通過不可信任的通訊網絡傳輸的密碼須加密處理。如無法加密處理，則須採用輔助控制措施，把所面對的風險減至可接受的水平。

11.4. 系統及應用系統接達控制

11.4.1. 認證方式須與所接達資料的敏感度相稱。

11.4.2. 須控制連續數次登入失敗的情況。

11.4.3. 決策局／部門須制訂嚴格的密碼政策，密碼政策須至少詳細規定最短密碼長度、初次密碼設定、受限制字詞及格式、及密碼更改周期，並包括挑選合適的系統及用戶密碼的指引。

11.4.4. 任何人員均不得擷取或以其他方式取得可容許未獲授權接達的密碼、解密匙或任何其他接達控制裝置。

11.4.5. 任何資訊系統啓用前，所有由供應商提供的預設密碼均須予更改。

11.4.6. 如懷疑密碼已／正外泄，或因維修及支援服務的需要而向供應商透露密碼，須立即更改密碼。

11.5. 流動資訊處理及遠程接達

11.5.1. 決策局／部門須制訂適當的使用政策及程序，訂明有關流動資訊處理及遠程接達的保安要求。同時，須採取適當的保安措施，以防止他人在未獲授權的情況下接達或披露這些設備所儲存及處理的資料。此外，應向獲授權用戶提供有關保安威脅的訊息，而該等用戶亦應承擔及確認知悉其保安責任。

11.5.2. 須推行保安措施，以防止他人在未獲授權的情況下遠程接達政府資訊系統及數據。

11.6. 物聯網裝置

11.6.1. 決策局／部門須界定並採取適當的保安措施，以確保物聯網裝置與數據的保安均與資料的類別相稱。

11.6.2. 除非在技術上不可行，否則物聯網裝置須同樣遵行本文件所列明對流動裝置的保安要求。保密資料不得在私人擁有的物聯網裝置上儲存或處理。

12. 加密方法

決策局／部門須確保適當和有效地使用加密方法，以保護資料的機密性、真確性和完整性。

12.1. 加密控制措施

12.1.1. 決策局／部門須於密碼匙的整個生命周期管理密碼匙，包括密碼匙的產生、儲存、存檔、獲取、分發、退役及銷毀。

13. 實體及環境保安

決策局／部門須防止資產在未獲授權的情況下被實體接達、破壞、竊取和破解，以及防止對辦公場地和資訊系統造成阻礙。

13.1. 安全區域

13.1.1. 在設立特定用途的電腦中心時，須慎重進行選址及場地規劃，並應視乎所建造的是特定用途設施或一般辦公室，參考相關的保安規格。

13.1.2. 數據中心及電腦室須設於實體保安完善的環境，並受到嚴密保護，以抵禦自然或其他因素所導致的災難和保安威脅，從而將損失範圍及服務中斷的影響減到最低。

13.1.3. 數據中心及電腦室須按所處置的資訊系統類別遵行政府關於實體保安的要求。

13.1.4. 須定期更新及覆檢獲授權進入數據中心、電腦室、放置或儲存電腦設備及數據的其他關鍵操作地點的人員清單。

13.1.5. 凡用作進入任何資訊系統及網絡的密碼匙、智能卡、密碼等，其實體安全須得到保障，或受到清晰明確及嚴格執行的保安程序所規管。

13.1.6. 獲授權人員須時刻監視所有進入數據中心或電腦室的訪客，並須妥善備存訪客出入記錄作審核用途。

13.1.7. 所有人員須確保其辦公室的保安。如辦公室設有資訊系統或放置了資訊資產，並可從公共地方直接進入，則應在無人使用時或辦公時間後鎖上。

13.2. 設備

13.2.1. 所有資訊系統須設於安全的環境，或由人員看管，以防止被未獲授權人士接達。須定期檢查設備及通訊設施，以確保其持續可用，並偵測是否有任何故障。

13.2.2. 管有流動裝置或抽取式媒體以作業務用途的人員，須保障有關裝置的安全。在沒有採取妥善保安措施的情況下，須避免裝置無人看管。

13.2.3. 在沒有採取適當控制措施的情況下，不得將資訊科技設備帶離場地。

13.2.4. 如系統在一段預定時間內無任何操作，則須啓動重新認證功能或登出系統並中斷連線，以免系統被非法接達。此外，在結束每天的工作前或長時間不操作的情況下，用戶須關掉工作站（如情況合適）。

13.2.5. 須小心放置顯示資訊系統所載資料的屏幕，確保未獲授權人士無法窺看屏幕所顯示的保密資料。

14. 操作保安

決策局／部門須確保資訊系統安全操作、防範惡意軟件、記錄資訊科技程序及事件和監察可疑活動，以及防止技術性保安漏洞被利用。

14.1. 操作程序和責任

14.1.1. 決策局／部門須按照精簡功能原則管理資訊系統，並移除或限制使用所有不必要的服務或元件。

14.1.2. 須慎重考慮會影響現行保安保護機制的變更。

14.1.3. 須妥善記錄、遵從，以及定期覆檢資訊系統的操作及管理程序。

14.2. 防範惡意軟件

14.2.1. 所有局部區域網絡伺服器、個人電腦、流動裝置及通過遠程接達連接政府內部網絡的電腦，都必須開啓抗惡意軟件保護功能。

14.2.2. 決策局／部門須保護其資訊系統免受惡意軟件的影響，並定期和在有需要時更新惡意軟件定義，以及其偵測和修復引擎。

14.2.3. 除非經過惡意軟件檢查及清除所有感染，否則不得使用從不明來源或源頭取得的儲存媒體和檔案。

14.2.4. 用戶不得蓄意編寫、產生、複製、傳播、執行或參與製造惡意軟件。

14.2.5. 電腦及網絡所採用的軟件必須從可信賴的來源取得。

14.2.6. 決策局／部門利用科技堵截與業務無關的網站時，應權衡輕重。

14.2.7. 從互聯網下載的所有軟件及檔案必須經抗惡意軟件解決方案掃描及檢驗。

14.2.8. 任何人員均不應啓動從互聯網下載的流動程式碼或軟件，除非有關程式碼是從已知及可信賴的來源取得。

14.3. 備份

14.3.1. 須定期進行備份工作。

14.3.2. 決策局／部門須為其資訊系統制訂和推行備份及復原政策。

14.3.3. 須定期覆檢備份工作。須定期進行備份復原測試。須訂定並記錄備份覆檢和復原測試的頻率。

14.3.4. 應防止備份媒體在未獲授權的情況下被接達、濫用或損毀。

14.3.5. 儲存必要及／或重要業務資料的備份媒體，須存放在與主要場地保持一段安全距離的地方，以免因主要場地發生災難而受到破壞。須保存一份並未連接資訊系統的備份複本，以防止備份數據在資訊系統被破解時遭到破壞。

14.4. 記錄

14.4.1. 決策局／部門須根據業務需要和數據的保密類別，制訂並記錄與轄下資訊系統工作記錄（包括保存期）有關的政策。

14.4.2. 保安記錄須提供足夠的資料，以作為對保安措施的成效及遵行情況進行全面審計的憑證。

14.4.3. 記錄保存期須與其作為有效審計工具的日期長短相稱。在保存記錄期間，須確保記錄安全，以免被竄改，並確保只有獲授權人士才可閱覽記錄。

14.4.4. 除非得到首長級人員的批准，作為審計工作所需，否則記錄不得用作剖析個別用戶的操作情況。

14.4.5. 各資訊系統的時鐘須與一個可信賴的時間來源同步。

14.5. 操作環境的控制

14.5.1. 各種電腦設備及軟件須在控制措施及審計監督下安裝。

14.5.2. 須利用更改控制程序控制資訊系統的變更，並備存變更記錄，以追蹤曾作出的變更。

14.6. 技術性保安漏洞管理

14.6.1. 決策局／部門須進行保安漏洞管理流程，包括識別、評估、緩解和追蹤其資訊系統的漏洞。

14.6.2. 決策局／部門須根據風險水平，制訂適當的修補程式管理策略，包括其資訊系統的修補程式檢測及修補頻率。決策局／部門須採用風險為本的方法，考慮每個保安漏洞的潛在影響和被利用的可能性，為其制定修補計劃。所有部署在與互聯網連接的資訊系統的伺服器和相關裝置都須受到嚴格的修補程式管理。

14.6.3. 決策局／部門須根據修補程式管理策略使用產品供應商推薦的最新保安修補程式或採取其他輔助保安措施，以保護其資訊系統免受已知保安漏洞的影響。

14.6.4. 在使用保安修補程式前，應進行適當的風險評估及測試，以盡量減少對資訊系統的不利影響。

14.6.5. 未經決策局／部門指定人員事先批准，不得將未獲授權的應用軟件載入政府資訊系統。

14.7. 資訊科技保安威脅管理

14.7.1. 決策局／部門須建立威脅識別、偵測和監察機制，並定期覆檢該機制，以確保其在資訊系統性質和技術進步方面的成效。

14.7.2. 須定期檢查記錄（尤其是處理／儲存保密資料的系統／應用系統的記錄），除檢查記錄是否全面外，亦須檢查其完整性。所有疑因違反保安事項而引致的系統及應用系統誤差，均須予以呈報和記錄。

15. 通訊保安

決策局／部門須確保在政府內部及與任何外部機構之間傳送的資料的安全。

15.1. 網絡保安管理

15.1.1. 須妥善備存內部網址、配置及相關系統或網絡的資料。未經有關決策局／部門批准，不得公開這些資料。

15.1.2. 須妥善保護與其他政府網絡或公眾可接達的電腦網絡連接的所有內部網絡。

15.1.3. 須妥善配置及管理資訊／通訊系統，並定期覆檢。

15.1.4. 決策局／部門須將其網絡劃分為分隔的網域，以建立安全邊界，並加強對不同網域之間的控制。

15.1.5. 與另一個網絡連接的接線不得導致被連接的一方網絡處理的資料安全受到損害，反之亦然。決策局／部門須制訂及推行適當的保安措施，以確保部門資訊系統連接至其他決策局／部門或外部機構轄下的資訊系統時，其保安標準不會有所降低。

15.1.6. 未獲授權的電腦資源（包括私人擁有的電腦資源）不得連接至政府內部網絡。如有運作上的需要，事前須得到部門資訊科技保安主任的批准。決策局／部門須確保該等電腦資源的使用同樣符合相關的資訊科技保安要求。

15.1.7. 決策局／部門須記錄、監察及控制接駁政府內部網絡的無線通訊。

15.1.8. 須採取適當的認證及加密保安措施，以保護通過接駁政府內部網絡的無線通訊的數據傳輸。

15.1.9. 必須通過中央安排的互聯網通訊閘或決策局／部門內部已推行安全架構及適當保安措施的互聯網通訊閘接達互聯網。如情況不許可，或為順應使用形式[2]，決策局／部門宜考慮准許使用獨立電腦接達互聯網，惟決策局／部門必須在適當的級別設立審批和控制機制。

15.1.10. 除非得到部門資訊科技保安主任的批准，否則所有人員不得利用撥號調解器、無線界面或寬頻鏈路等通訊裝置，將已連接政府內部網絡的工作站或流動裝置同時連接至外部網絡。

[2] 使用形式可包括公幹時上網、收發電子郵件及使用政府的便攜式電腦等。在上述情況下，仍須採取任何適用的保安措施保護獨立電腦。

15.2. 資料傳送

15.2.1. 機密以上保密類別的資料必須經過加密處理，並只限於在已獲政府保安事務主任批准及數字政策辦公室技術認可的獨立局部區域網絡內傳遞。

15.2.2. 機密／限閱資料在不可信賴的通訊網絡上傳遞時必須加密，在任何通訊網絡上傳遞時亦應盡可能加密。

15.2.3. 如傳遞載有保密資料的電子郵件，必須通過已獲數字政策辦公室技術審核及政府保安事務主任批准的資訊系統傳遞。

15.2.4. 系統管理員須訂立及維持有系統的程序，以記錄、保存及刪除電子郵件訊息及相關的記錄。

15.2.5. 必須妥善備存和保護包含獲授權用戶或政府網站資料的內部電子郵件通訊錄，以免在未獲授權的情況下被接達和竄改。

15.2.6. 必須制訂及記錄有關決策局／部門與外部機構之間安全傳送保密資料的協議。

15.2.7. 不應打開或轉寄可疑來源的電子訊息。

16. 系統購置、發展及維護

決策局／部門須確保資訊保安在資訊系統的整個生命周期中都是重要的一環，並且盡可能隔離發展、系統測試、驗收測試和實際操作等不同環境。

16.1. 資訊系統的保安要求

16.1.1. 在發展系統時，須根據系統的保安要求進行保安規劃，並推行適當的保安措施及控制措施。

16.2. 發展和支援程序的保安

16.2.1. 決策局／部門須建立及適當地保護用作系統發展的環境，以及涵蓋整個系統發展周期的整合工作。

16.2.2. 須妥善備存應用系統的文件、程式源碼和清單，接達這些文件、程式源碼和清單時須受「有需要知道」原則限制。

16.2.3. 在推行保安措施前，須正式測試及覆檢有關措施。

16.2.4. 須對應用系統採取適當的保安措施，例如版本控制機制和隔離發展、系統測試、驗收測試和實際操作等不同環境，以維持應用系統的完整性。

16.2.5. 須記錄有關要求及審批程式／系統變更的更改控制程序。

16.2.6. 決策局／部門須確保已正式通知有關人員資訊系統配置更改後對保安和資訊系統用途的影響。

16.2.7. 除非得到資料擁有人的批准，否則應用系統發展及系統支援人員不得接達生產系統內的保密資料。

16.3. 測試數據

16.3.1. 對於用作測試的數據，須根據其類別予以審慎選擇、保護及控制。如確有需要使用生產環境的保密資料，須覆檢及記錄有關過程，並得到資料擁有人的批准。

17. 外判資訊系統的保安

決策局／部門須確保外聘服務供應商可接達的資訊系統和資產受到保護。

17.1. 外判服務的資訊科技保安

17.1.1. 外聘服務供應商須遵守及遵行各決策局／部門所制訂的部門資訊科技保安政策，以及政府發出的其他資訊保安要求。

17.1.2. 決策局／部門使用外聘服務或設施時，須確定和評估此舉為政府資料及業務運作帶來的風險。決策局／部門須記錄及推行根據資料類別及業務要求而訂定的外聘服務或設施保安措施、服務水平和管理要求，並訂明及商定外聘服務供應商的保安職責。

17.2. 外判服務交付管理

17.2.1. 決策局／部門須監察外聘服務供應商，並與他們進行覆檢，以確保外聘服務供應商的操作程序得到妥善記錄及管理。此外，決策局／部門須妥善管理保密及不可向外披露資料的協議，並須在出現任何影響保安要求的變更時，覆檢有關協議。

17.2.2. 決策局／部門須保留審核及監察遵行保安要求的權利，以確保外聘服務供應商為政府資訊系統、設施及資料採取足夠的控制措施。另外，外聘服務供應商須定期提交保安審計報告，以證明所採取的措施達到滿意程度。

17.2.3. 決策局／部門須確保外聘服務或設施備存的所有政府資料在有關服務期滿或終止時或在政府的要求下，根據政府的保安要求予以清除或銷毀。

17.3. 雲端運算保安

17.3.1. 限閱或以上保密類別的資料不得利用公共雲端服務儲存或處理。

17.3.2. 在與雲端服務供應商簽署協議之前，決策局／部門須確保已明確界定、記錄並明白雙方的共同責任。

18. 保安事故管理

決策局／部門須確保設有一致及有效的資訊保安事故管理方法。

18.1. 保安事故的管理和改進

18.1.1. 決策局／部門須制訂一套事故偵測及監察機制，以偵測、遏制並最終防止保安事故的發生。

18.1.2. 決策局／部門須保留系統記錄及其他證明資料，以供證明及追蹤保安事故之用。

18.1.3. 決策局／部門須為其資訊系統制訂、記錄、測試及備存一套保安事故應變計劃。

18.1.4. 所有人員須對現行保安事故應變計劃有充分認識，並須遵守和遵從有關程序。

18.1.5. 如發現或懷疑資訊系統或服務出現任何保安事故或保安問題，必須即時向負責人士匯報，並根據事故處理程序處理。

18.1.6. 除向負責處理保安事故及系統保安工作，或獲授權參與調查電腦罪行或濫用電腦事故的人士外，所有人員不得向任何人士披露有關電腦罪行及濫用電腦事故中的受害人、決策局／部門、受影響系統或造成該次事故的系統保安漏洞和入侵方法的資料。

19. 資訊科技保安方面的業務持續運作管理

決策局／部門須確保運作復原計劃中的內容包含資訊系統的可用性及保安考慮。

19.1. 持續資訊科技保安

19.1.1. 決策局／部門須計劃、推行及定期覆檢運作復原計劃，以確保在這些情況下採取足夠的保安措施。

19.2. 復原能力

19.2.1. 決策局／部門須確保有足夠復原能力，以符合資訊科技服務及設施在可用性方面的要求。

20. 遵行要求

決策局／部門須避免違反與保安要求相關的法律、法定、規管或合約責任。保安措施須根據相關保安要求推行及操作。

20.1. 遵行法例及合約要求

20.1.1. 決策局／部門須就每個資訊系統的操作定出及記錄所有適用的相關法定、規管及合約要求。

20.1.2. 決策局／部門須備存記錄，以證明已遵行保安要求，以及協助就相關保安措施是否已有效推行進行審計。

20.1.3. 決策局／部門須遵行政府要求中所載有關資訊系統保安的規定，包括但不限於保密資料的儲存、傳遞、處理及銷毀。同時，應保護沒有列入任何保密類別的資料，以防止該等資料不慎外泄。

20.1.4. 處理個人資料時須遵守《個人資料（私隱）條例》（第 486 章）的規定。所有個人資料應列為限閱或以上類別。視乎有關個人資料的性質和敏感度，以及資料在未獲授權或意外的情況下被接達、處理、刪除或作其他用途而引致的損害，可能須採用較高的保密類別和採取合適的保安措施。

20.2. 保安審查

20.2.1. 資訊系統及生產應用系統須至少每兩年進行一次保安風險評估。資訊系統或生產應用系統在投入生產前，以及在進行大規模升級和變更前，也須進行保安風險評估。

20.2.2. 須至少每兩年對資訊系統進行一次審計，以確保有關各方已遵行資訊科技保安政策和採取有效的保安措施。在審計過程中，揀選審計師和進行審計的工作必須客觀持平。審計師不得審核自己有份參與的工作。

20.2.3. 須限制及控制使用軟件及程式進行保安風險評估或保安審計。

21. 聯絡方法

本文件由數字政策辦公室編製及備存。如有任何意見或建議，請寄往：

電子郵件： it_security@digitalpolicy.gov.hk

Lotus Notes 電子郵件： IT Security Team/DPO/HKSARG@DPO

「中央管理通訊系統」電子郵件： IT Security Team/DPO

完