數字政策辦公室

資訊保安

資訊科技保安指引

[G3]

第 10.1 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		4.0	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」		4.1	2004 年 7 月
3	豐富／加強本文件，以提供更多有關： – 應用系統保安的詳盡指引（載於第 10.1.1 節「應用系統設計及發展的保安考慮事項」及第 10.7 節「網上應用系統保安」） – 適當處理／限制資料披露的詳盡指引（載於第 10.4 節「程式／系統測試」及第 11.3 節「電郵保安」） – 網絡通訊／埠及系統服務的適當限制的詳盡指引（載於第 11.2 節「互聯網保安」） 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”	10-2 10-6 10-7 10-4 11-4 11-3 無	4.2	2004 年 9 月
4	作出相應更新，以符合經修訂的政府保安要求	9-3, 9-10, 11-2	4.3	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		5.0	2006 年 5 月
6	根據經修訂的政府保安要求對附錄 B 作出相應更新 對附錄 C 作出相應更新並摘錄全部六項保障資料原則	B-2 C-1	5.1	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		6.0	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		7.0	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		8.0	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)		9.0	2021 年 3 月
11	根據公務員學院成立對第 9.1(c)節作出相應更新 關於消磁產品配置靈活性對第 10.3(b)節作出更新 關於嚴謹密碼策略對第 11.4(b)和 11.4(c)節作出更新 根據新版本的文件對第 16.1(b)節作出相應更新	24 30, 31 36-38 80	9.1	2022 年 8 月
12	修改報告可於政府內聯網「資訊科技情報網」查閱		10.0	2024 年 4 月
13	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」更改爲「香港網絡安全事故協調中心」 關於威脅情報平台及來源的例子對第 9.1(c) 和 14.7(b)節作出更新		10.1	2024 年 7 月

目錄

1. 目的

本文件就《基準資訊科技保安政策》所列明的保安要求詮釋當中的政策要求，以及訂定相關實施標準，同時為有效推行相應的保安措施提供一套指引。

本文件所載的資料不是為任何特定的電腦平台而編製。決策局／部門須遵行本文件所載的指引推行保安控制措施，以符合相關的保安要求。在不影響保安標準的情況下，決策局／部門宜按需要制訂適合本身情況的保安措施。

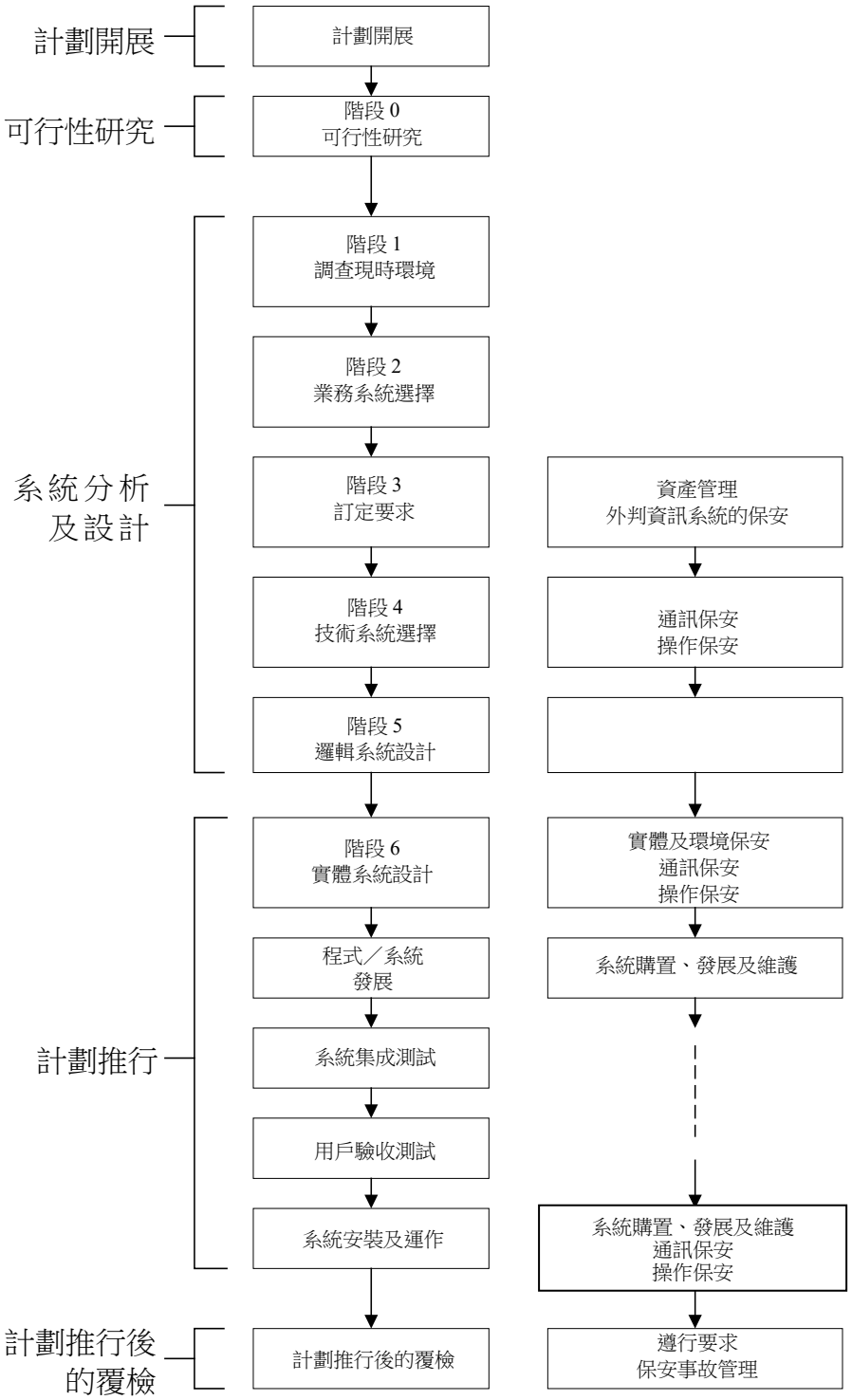
2. 範圍

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、網絡安全和私隱保護—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 個範疇闡述相關指引：

- 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）。

基本上，上述範疇在系統發展周期的各個階段均應予考慮，但若干階段亦各有需注意的範疇。下頁的圖示列出這些範疇。



系統發展周期各個階段涉及的保安範疇

2.2 對象

本文件是為各決策局／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，並了解及遵行，以有效實施相關保安要求。

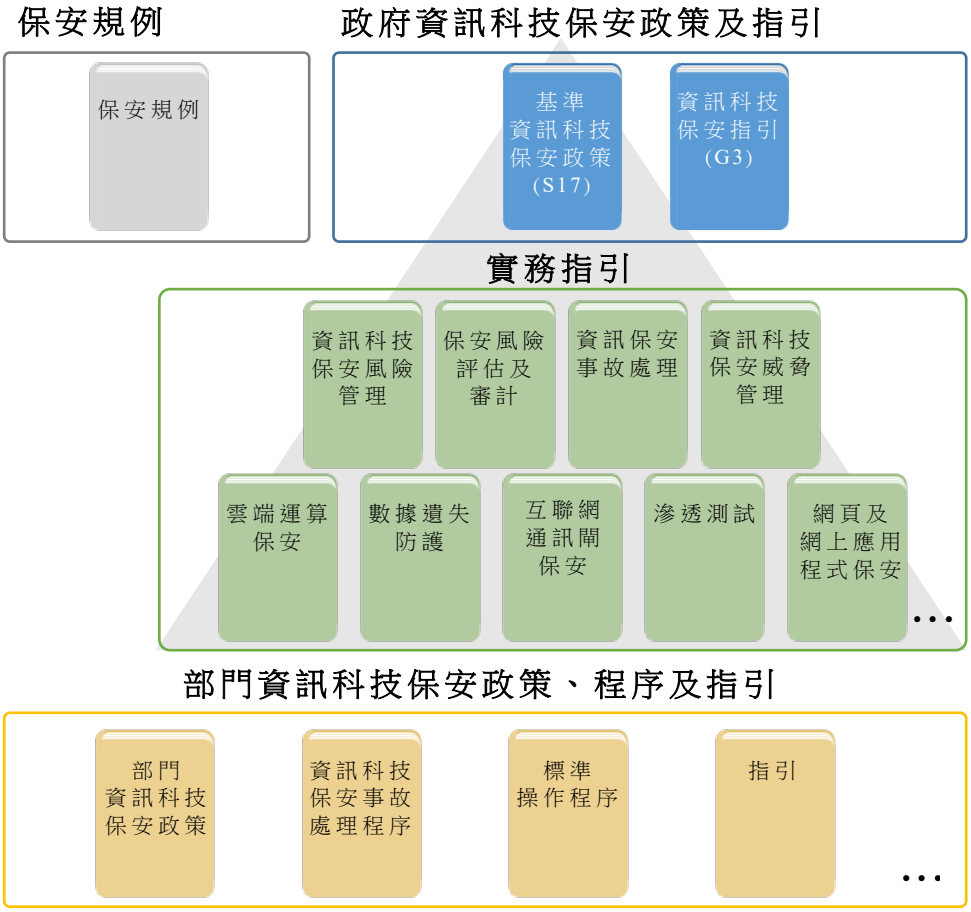
另外，本文件亦供為政府提供資訊科技服務的供應商、承辦商及顧問使用。

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。

決策局／部門須對第 1 級資訊系統採取本文件所載的所有強制性保安要求，並對第 2 級及第 3 級資訊系統額外採取附錄 C 所載的更嚴格保安要求，以達致資訊科技保安等級保護，從而確保所有政府資訊系統均受到與資訊系統風險等級相稱的保安控制措施所適當保護。

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、材料及資訊需被列作機密資料，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》必須視為必須遵守的強制性基準規例，各決策局／部門亦可採取其他適當的措施加強保安。
《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。

此外，尚有數份補充《資訊科技保安指引》的實務指引，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。這些實務指引包括《互聯網通訊閘保安實務指引》、《資訊科技保安風險管理實務指引》、《資訊科技保安威脅管理實務指引》、《保安風險評估及審計實務指引》和《資訊保安事故處理實務指引》等。

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) 《基準資訊科技保安政策》[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) 信息安全技術網絡安全等級保護基本要求, GB/T 22239-2019, 發佈於 2019 年 5 月 10 日

f) 《電子政府互用架構》[S18]

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，可供該人士及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。

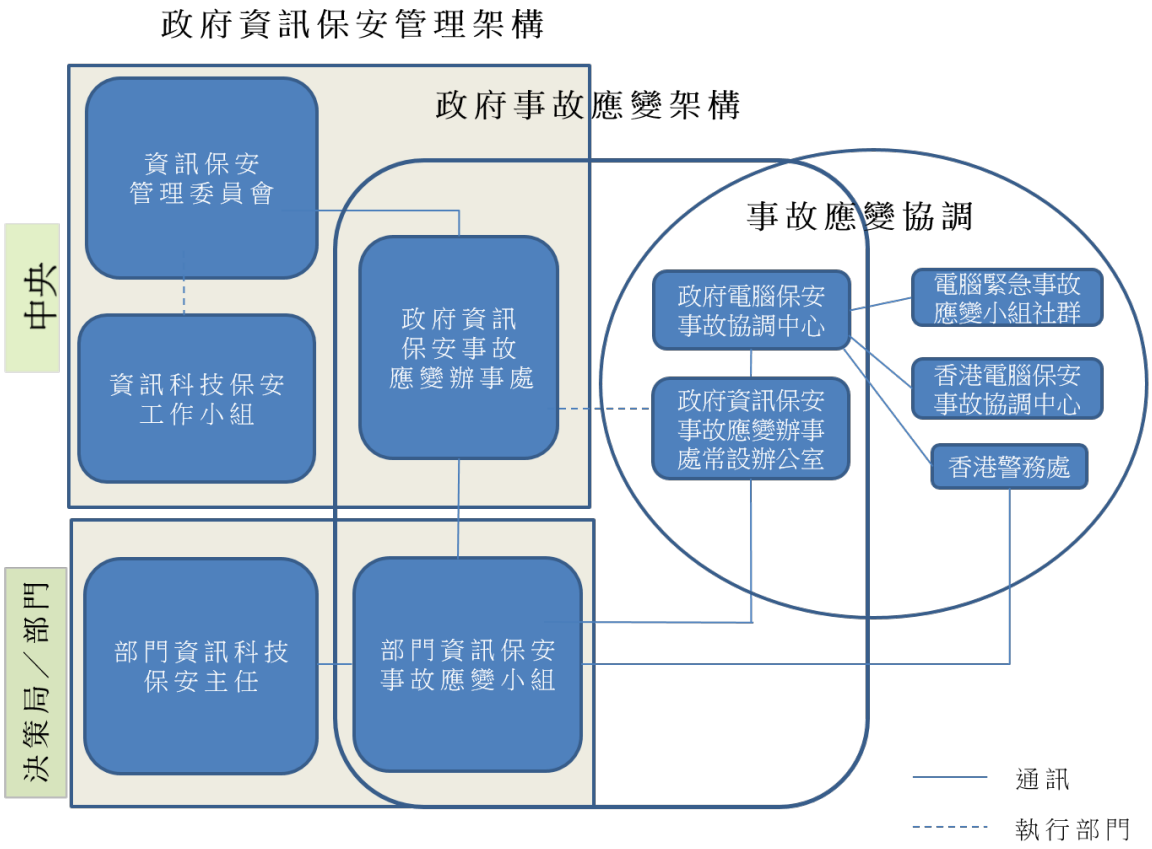
宜　　「宜」表示期望達到的良好作業模式。

5. 政府資訊保安組織

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相關規例、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相關規例、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保安事故外，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
- 在處理網絡保安事故時，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。

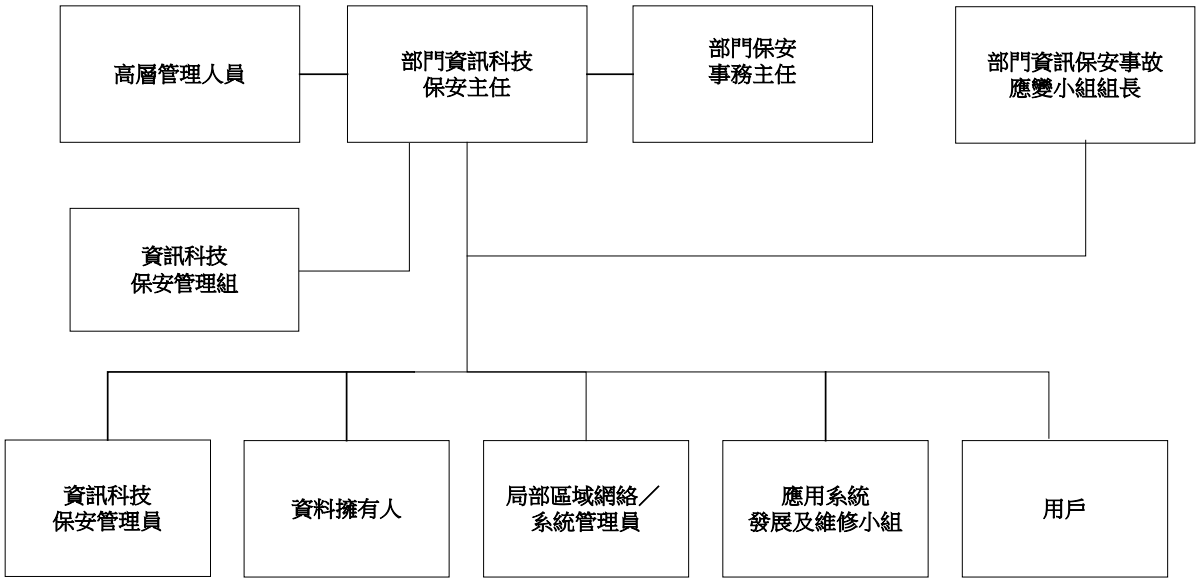
5.1.5 決策局／部門

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。

[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。

- 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。

高層管理人員應考慮成立資訊保安督導委員會，或將資訊保安列作管理層會議定期討論項目之一。

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。

如決策局／部門最終不能委任一名首長級人員為部門資訊科技保安主任，有關決策局局長／部門首長則應委任一名高層人員，並授予足夠的權力在處理嚴重威脅事件或保安事故時調動資源和作出決定，該項委任亦應向決策局／部門的所有相關工作人員發布。

為了讓獲指派擔任部門資訊科技保安主任的人員具備更多保安管理和相關科技的知識或技術，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。
- 監控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保安風險管理程序，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等關鍵事項作出決策；
- 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程序；
- 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。

  這些保安目標可作為指引，以制訂標準、程序和控制措施，供保安設計及保安方案各個範疇使用。簡單來說，就資訊系統而言，只有獲授權用戶才可知悉、接達、更改或刪除資訊系統所儲存或處理的資料。此外，資訊系統須在獲授權用戶提出要求時，可供該用戶接達及使用。

- **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 (b)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。

  風險為本的方法一般包括風險評估和風險處理兩個程序。這些程序可以加入到不同的程序中，例如項目管理、漏洞管理、事故管理、問題管理，甚至臨時就某特定主題進行的程序。風險評估程序包括：

  (a) 制訂及持續覆檢接受風險準則，以及資訊保安風險評估的啓動準則；
  (b) 找出風險擁有者和在失去資訊機密性、完整性和可用性情況下相關的風險；
  (c) 根據潛在的影響和發生的可能性來確定風險水平以分析風險；
  (d) 通過比較風險分析的結果與既定準則作出評估，並訂定處理經分析的風險的緩急次序。

  風險處理程序須用作選擇合適的風險處理方案，並決定所需的控制措施，以落實執行選定的方案。這個風險為本程序須確保已包括一切所需的控制措施，以及訂立一套風險處理計劃，並由風險擁有者批准有關計劃和接受餘下的保安風險。

  風險擁有者須負責評估、管理及監察已被確認的風險和選定的風險控制措施的推行情況。

- **設計層面的保安方法**

  須採用設計層面的保安概念，將保安要求納入系統發展周期，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。

  設計層面的保安是一種軟件及硬件開發方法，目的是在系統發展周期的每個階段中透過設計和建立安全性來減少系統漏洞和攻擊面。這包括在設計中納入保安規格、在每個階段持續進行保安評估，以及遵循良好作業模式。針對資訊科技保安，設計層面的保安解決了系統生命周期中的資訊科技保護問題。這包括專門用於增強系統的資訊科技復原能力的保安設計。因此，決策局／部門須盡可能採用設計層面的保安方法。

- **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。

  防禦是第一道防線。採取適當的保安保護措施，有助減低發生保安事故的風險。然而，如保安措施遭攻破，決策局／部門亦須有能力迅速偵測保安事故及快速應變以控制損毀，並須及時令資訊系統和有關數據復原。因此，決策局／部門須指派適當人員管理資訊科技保安事宜，以及制訂資訊保安事故處理計劃。

- **處理、傳輸和儲存資料時的保護措施**

  處理、傳輸和儲存資料[2]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，因此傳輸保密資料時須採取保安措施。

  決策局／部門制訂保安措施時，須審慎考慮及評估有關風險，包括資料被他人在未獲授權的情況下竄改、破壞或披露，以及在不同情況下查閱資料的要求被拒等。

[2] 就本文件而言，「已儲存資料」是指儲存於即使切斷電源仍能保存資料的非揮發性媒體內的數據。非揮發性媒體包括但不限於硬磁碟、固態硬碟、光碟、磁帶、通用串列匯流排閃存記憶裝置及非揮發性記憶體（NVRAM）。儲存在任何資訊科技設備（如伺服器、工作站、手提電腦、流動裝置、打印機、網絡裝置等）的非揮發性媒體內的數據均被視為「已儲存資料」。儲存在揮發性媒體（如隨機接達記憶體）內的數據因會在電源被切斷後逐漸流失，因此不被視為「已儲存資料」。

- **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。

  外部系統未必根據政府保安要求設計、開發及維護，因此決策局／部門須考慮在其資訊資產或資訊系統連接至外部系統時，採取多重防禦措施。來自外部系統的任何資料，包括用戶輸入的數據，均可能是潛在的攻擊來源，資訊系統須因此進行分隔或隔離，並應按系統所需的保安水平推行不同程度的接達控制和保護措施。

- **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。

  損害控制是指推行保安控制措施，以限制保安事故所帶來的影響。資訊系統的復原能力是指資訊系統在不利或壓力情況下，甚至在效率下降或幾近不能操作的狀態下，仍可繼續操作並維持基本功能。復原能力亦包括可因應業務需要，在所定時間內令系統恢復有效運作的能力。

- **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。

  審計有助重組完整的系統行為記錄，故可於保安事故發生時，有助找出和調查有關系統所出現的問題。問責則往往能確定涉事的單一個別人士，讓有關方面能追查其在資訊系統上的活動。

- **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。

  決策局／部門須找出將予監察和測量的資訊保安程序和控制措施，並決定監察、測量及評估結果的方法。須定期覆檢保安措施，以確保措施維持足夠、適當及有效。保安覆檢的結果須包括對可予持續改善之處作出的決定，以及視乎情況對保安措施作出任何變更的需要。

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

(a) 職務和職責

決策局／部門須應用資訊保安管理中有關制衡的核心保安原則和良好作業模式。不論項目種類為何，在項目管理的每個階段均須考慮資訊保安。

無論資訊系統的資金來源為何，決策局／部門須確保其所有資訊系統，包括基礎設施及部門共享資訊科技服務，均按其風險程度得到妥善保護。須採取第 7.2(b)節所提及的資訊科技保安等級保護，以便對資訊系統進行有效的資訊科技保安風險管理。此外，決策局／部門須確保保安保護措施能夠迅速應對並配合不斷變化的環境和技術。

決策局／部門須參照第 5.2 節－部門資訊科技保安組織，訂定其部門資訊科技保安管理架構。決策局／部門應委派一名高層要員，負責監督制訂和實施合適的保安政策和程序，並確保在行政及操作過程中有足夠的制衡機制。決策局／部門在分派職責時，應參照部門資訊科技保安管理架構、政策及程序。

獲分派職責的人員可將保安工作委託予其他人員，惟他們仍須有最終責任確保已推行足夠的保安措施。同時，獲分派職責的人員應確保受委託人員無論在能力、知識、經驗及資歷上均適合處理該工作。有關人員應檢查所有委託工作是否已妥當處理，而委託內容亦須詳細記錄並定期覆檢。

(b) 職務分工

職務分工是指將一項工作的各個步驟分別交由不同人員處理，以杜絕程序被一人破壞的可能性。有關安排須充分利用職務分工，並明確區分職務和職責，以盡量減少由一人獨攬執行和控制整個資訊系統所有保安工作和／或重要操作的權限。

如因受人手或其他技術問題所限而無法推行職務分工，則應採取輔助控制措施，以提供相同的保障，例如適當地備存有關人員在系統上所作的關鍵操作記錄，並由適當授權級別的人員突擊抽查和／或定期覆檢記錄檔案。

(c) 預算

決策局／部門須控制預算，以確保有足夠撥款推行所需的保安保護措施。管理層應根據短期及長期目標或目的，制訂資訊保安的預算方案、預測及資源分配計劃。應根據風險等級分配資源來保護資訊系統。

(d) 查閱資料的權利

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，包括電郵、文件目錄，以及討論區、新聞群組和網站的接達記錄。這些檢查有助確保內部政策的遵行情況、配合內部調查，以及促進政府資訊系統的保安管理。

7.2 保安風險管理

(a) 風險爲本的方法

為應對不斷轉變的環境和技術，決策局／部門須採用風險為本的方法處理資訊保安，以確保資訊資產的機密性、完整性及可用性，以及資訊系統符合其他所有保安要求。決策局／部門只須採取一些簡單的措施，便應能夠有效減低及控制由人為及／或操作問題所導致的資訊保安潛在風險，使風險降至可接受的水平。決策局／部門須根據個別業務及實際操作環境，考慮採用良好作業模式。

(b) 資訊科技保安等級保護

為確保所有政府資訊系統均受到與資訊系統風險等級相稱的保安控制措施所適當保護，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，包括第 1 級、第 2 級和第 3 級資訊系統，推行分級的保安控制措施。決策局／部門須對一般資訊系統採取本文件所載的所有強制性保安要求，並對第 2 級和第 3 級資訊系統額外採取附錄 C 所載的更嚴格保安要求。決策局／部門須確保資訊系統等級在資訊系統的整個生命周期內與其業務目標保持一致。

第 2 級資訊系統是指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。決策局／部門應考慮數據的保密級別及服務中斷的後果，以決定其關鍵性。關鍵性的評估應包括以下各方面：

- 防禦／保安風險（例如對人命、財產或個人私隱造成傷害、無法執行法定責任及維持治安）。
- 經濟影響（例如可能減慢經濟增長或導致政府經濟損失）。
- 政府形象（例如對政府聲譽、公眾信心的影響）。
- 相互影響（例如一個系統的服務質素下降可能導致另一個資訊系統的服務中斷）。

此外，決策局／部門在為系統評級時，應包括適用於其資訊系統的其他考慮層面，並根據在資訊系統發生故障或中斷時影響的範圍（即受影響用戶人數）、嚴重性（即中斷或損毀引致的後果）、停止運作的容忍程度（即服務中斷可造成嚴重影響的臨界點），以及可能對業務造成的最大影響作出評估。

此外，有很多必要服務對社會及其經濟的運作和安全是關鍵的。第 3 級資訊系統是指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。

決策局／部門在為資訊系統評級時，須參考附錄 B 的考慮因素。所有資訊系統的評級詳情均須妥善記錄。資訊系統等級須經決策局局長／部門首長或他們明確授權的首長級人員批准。

(c) 資訊科技保安風險管理架構

為確保決策局／部門以有條理的方法進行及監察保安風險評估，決策局／部門應採用以下資訊科技保安風險管理架構，當中包括一系列風險管理程序，並利用風險記錄冊，以達致有效的資訊科技保安風險管理及溝通。以下是該架構的重點以供參考。

- 部門背景建立－建立決策局／部門的資訊科技保安風險管理背景，其中包括決策局／部門的風險偏好和承受能力。
- 風險評估－對決策局／部門的所有資訊系統進行第 20.2(a)節規定的保安風險評估，即根據風險源頭（例如漏洞、威脅）和事件（例如事故場景）識別資訊系統的資訊科技保安風險，根據風險的影響和可能性決定已識別風險的級別，對已分析的風險進行緩急排序以作風險處理，並將已排序的風險記錄在資訊系統的風險記錄冊中。

- 風險處理－就資訊系統的每項風險決定適當的風險處理方法（例如風險降低、規避、轉移和接受），將其級別降低至決策局／部門的風險偏好範圍內，並將其處理方法記錄在資訊系統的風險記錄冊中。
- 風險關聯、匯總和規格化－透過在部門背景中進行風險關聯、匯總和規格化，將資訊系統的各個風險記錄冊整合到部門的資訊科技保安風險記錄冊中，以便決策局／部門進行資訊科技保安風險監控和溝通。
- 風險監控和報告－監控部門的資訊科技保安風險和相應的風險處理，並向部門資訊科技保安主任和其他有關各方報告。

如欲獲取更多有關資訊科技保安風險管理架構的資料，可參考以下文件：

- 資訊科技保安風險管理實務指引
  可在政府資訊科技情報站下載
  (https://itginfo.ccgo.hksarg/content/itsecure/techcorner/practices.shtml)

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

(a) 部門資訊科技保安政策

資訊科技保安政策須訂定保安規格的最低標準及列明哪些方面對機構至關重要。因此，儘管仍有其他可加強資訊保安的可取措施，但資訊科技保安政策必須視為強制性基本規則。

決策局／部門須以《基準資訊科技保安政策》文件為基礎，制訂部門資訊科技保安政策。

部門資訊科技保安政策須涵蓋妥善使用資訊系統、數據資產、網絡資源、資訊科技服務及設施，以及保安事故預防及應變程序等範疇。擬訂政策時須考慮以下內容：

- 決策局／部門本身對保安的要求
- 第 2.3 節所列明的現行政府資訊科技保安要求
- 《個人資料（私隱）條例》
- 《公開資料守則》
- 《辦公實務手冊》的檔案管理資料

在擬訂有關政策時須額外考慮以下內容：

- 香港特別行政區政府的施政目標和方向
- 香港特別行政區政府現行的政策、規則、規例和法律
- 決策局／部門本身的要求和需要
- 推行、分配及執行方面的問題

決策局／部門應制訂程序，迅速為調查違反保安事故的相關工作和政策推行問題提供協助。成立部門資訊保安事故應變小組和制訂保安事故應變計劃可加強政策的成效。

(b) 評估及定期覆檢

資訊保安政策、標準、指引和程序須定期覆檢。覆檢的結果和建議的變更須由有關各方評估和批准，以確保已納入所需的要求。決策局／部門宜考慮外聘合資格的資訊科技保安審計師或顧問覆檢或協助制訂資訊保安文件，以提高文件的質素和全面性。

在得不到持續支持的情況下制訂的資訊保安文件，最終會無人理會甚至過時。事實上，隨着時間的流轉，有些問題可能不復重要，而新的問題又會不斷湧現。因此，經常覆檢資訊保安文件有助確保相關政策符合部門的最新要求，並能隨着科技發展與時並進。

(c) 與用戶溝通

決策局／部門須發布本身的資訊科技保安政策，並須建立一套政策發布機制，以確保所有人員、功能組別及管理層均能輕易得知有關政策。決策局／部門須確保他們充分認識資訊科技保安政策，以便履行職務及切合政府的保安要求。

除非用戶或有關各方均作出承擔和進行溝通，否則不得將政策視為已落實推行。因此，決策局／部門應確保用戶和有關各方：

- 在新加入時已通過簡介或入職培訓獲悉相關政策。
- 獲邀參與制訂政策建議。
- 已接受遵行政策所需的技能培訓。
- 定期獲知會及認識保安威脅或問題。
- 已獲發分為小篇幅單元的政策指引。

為協助電腦終端用戶了解其資訊科技保安職責，決策局／部門應以簡單易明的實際操作指示形式，制訂部門終端用戶資訊科技保安操作指示文件，概述有關終端用戶的保安要求。附錄 A 載有一份終端用戶資訊科技保安操作指示樣本，以供參考。

9. 人力資源保安

積極培養深厚的保安文化，對於提升決策局／部門的保安態勢、降低風險、遵行法規，以及在整個政府內建立一個具復原能力和可信賴的環境，是至關重要的。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

(a) 資訊科技保安職責

須在所有人員獲派任新職位時，告知他們其資訊科技保安職務和職責，並須在他們受僱期內，定期提醒他們有關職務和職責。決策局／部門須確保所有人員：

- 在新加入時已通過簡介或入職培訓獲悉部門資訊科技保安政策；以及
- 了解他們的資訊科技保安職責及政府保安要求，並定期獲提醒有關職責及要求。

(b) 資訊發布

須設立有效的資訊發布機制，以確保全體有關人員充分了解規管其在資訊系統使用權限和應用範圍方面的相關政策和程序。

(c) 培訓

決策局／部門須定期向所有人員（包括參與政府工作的用戶、開發人員、系統管理員及保安管理員）提供適當保安培訓，以及有關資訊保安政策的最新資料，加強他們的資訊保安意識。培訓可以任何形式進行，例如課堂講授、電腦授課或自學形式（按自己步伐學習）。應提醒用戶留意公務員學院公務員易學網（「易學網」）向參加者提供的培訓資源，包括與一般資訊科技保安有關的教材和自我評核套件。決策局／部門根據其業務及運作需要為轄下人員或承辦商提供特定的培訓計劃及教材時宜參考這些培訓資源。有關「易學網」的詳情，可瀏覽 https://www.clcplus.csc.gov.hk。

人員亦可以通過參與保安演習和參加研討會、展示會或瀏覽載有保安情報資訊和一般保安資訊（例如網絡安全資訊站、資訊安全網）的專頁來提高保安意識。決策局／部門須參與數字政策辦公室指定的資訊科技保安意識活動。

應為系統管理員提供有關推行資訊科技保安程序的適當指導和培訓。系統管理員應懂得如何保護系統免受攻擊及被未獲授權人士擅用。系統管理員須有一套匯報保安問題的既定程序。

決策局／部門應考慮制訂資訊科技保安培訓計劃，以便為其員工提供適切和有系統的資訊科技保安意識活動。

資訊科技保安培訓計劃應包括但不限於以下內容：

(i) 計劃目標

決策局／部門應就資訊科技保安意識計劃制訂目標。這些目標應與決策局／部門的整體資訊科技保安策略一致。

(ii) 對象

決策局／部門應識別需要參與培訓活動的對象或角色。決策局／部門應根據不同的技術專業水平、工作職能和需求來制訂培訓內容。

(iii) 培訓方式

培訓材料和內容的設計應配合目標和對象。培訓主題的例子包括網絡釣魚意識、事故應變、監管遵行、數據私隱、社交媒體平台意識等。此外，應根據決策局／部門的規模、風險、資源和對象的需要，採用適當的培訓方法。培訓方式可包括演示、影片、互動模組、實踐練習和案例研究。

(iv) 評估培訓活動成效

決策局／部門應檢視培訓活動的成效。可進行評估以確保人員了解資訊保安要求和責任，例如透過培訓後測試、意見調查、模擬練習、觀察行為變化或保安事故數目等方法，來評估知識增長、行為變化和參與者滿意度。

(v) 定期覆檢及更新

決策局／部門應持續覆檢及更新培訓計劃，以反映不斷變化的威脅形勢、新技術，以及法規和遵行要求的改變。此外，決策局／部門應參考意見調查結果，找出需要改善的地方，並調整或微調培訓計劃。

(d) 人事保安

保密資料須受到保護，以免在未獲授權的情況下被接達或披露。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」原則適用於所有保密資料，這類資料只可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。

決策局／部門須確保人事保安風險已獲妥善管理。決策局／部門須評估准許個別人員接達保密資料所涉及的風險。

只限曾接受適當操守審查的公務員才可接達限閱類別以上的保密資料。決策局／部門應就《操守審查訓令》諮詢部門的人事部。至於非公務員的人員，決策局／部門應根據業務要求、有關人員所處理資料的類別及表面所知的風險，對該等人員進行適當的背景審查。在顧及個人私隱的情況下，背景審查宜包括以下事項：

- 獨立查核身分（香港身份證或護照）
- 確認所申報的學歷及專業資格
- 檢查履歷表所載資料是否完整和準確
- 是否有提供工作證明
- 如有需要，詳細檢查信用或犯罪記錄等資料

(e) 清晰的政策及程序

管理人員須就資訊系統的使用制訂清晰的政策和配套程序，清楚訂明資訊系統所容許及禁止的用戶行為。這些行為一般應在部門的資訊科技保安政策訂明。部門資訊科技保安政策須規定，任何人員如違反政策的任何條文規定，可能受到不同程度的紀律處分或懲罰，但須視乎違反保安事件的嚴重性而定。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，以及其在資訊系統方面的職責和職務。

(f) 終止或更改僱用後的資訊科技保安職責

須於僱用條款及條件中界定離職後的職責和職務。向人員發出有關終止僱用後職責的通訊須包括延續的資訊保安要求和法律責任，以及任何保密協議和僱用條款及條件中所訂明離職後特定時間內的職責。職責或職位上的變動，須作為終止現有職責或僱用，然後開展新職責或僱用的安排。

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，並確保有關資料得到適當程度的保護。

10.1 對資產的責任

(a) 資產清單

資產清單有助作出有效的保護及識別遺失的資產。無論資訊系統的資金來源為何，均須為所有資訊系統包括基礎設施及部門共享資訊科技服務（及其系統等級）、硬件資產、軟件資產、有效保用證、服務協議和法律／合約文件（例如公共域名註冊和相關互聯網規約地址、數據儲存的實體位置等）制訂一份清單。清單須定期予以覆檢，以確保能妥善持有、保管及維護有關資產。為了更好地管理軟件供應鏈，決策局／部門應盡可能收集有關軟件資產相關組件的資訊（例如供應商、組件名稱、版本、依賴關係等）。

部門資訊科技保安主任尤其須備存其決策局／部門所有與互聯網連接的服務的最新清單。清單必須詳盡，且至少包括各項服務在互聯網上公開的描述、互聯網規約地址、域名及開放的網絡埠。

在設立資產或從其他各方轉移資產時，須編配資產擁有權。資產擁有人須妥善管理資產，以確保：

- 資產被列入清單。
- 資產得到適當分類及保護。
- 資產的接達限制有清楚訂明，並獲定期覆檢。
- 資產的棄置或重用事宜獲妥善處理。

(b) 政府資訊系統的資料保護

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。除非按「有需要知道」原則，以及在獲部門資訊科技保安主任授權的情況下，否則不得披露可能損害資訊系統保安的資訊系統資料，例如寫有互聯網規約地址的網絡圖和保安審計報告。此類資料亦須按保密級別分類及得到保護。

此類資料可能因外聘服務供應商的資訊保安管理不足而受到威脅。如需向外聘服務供應商披露此類資料，則須通過不可向外披露資料的協議或同等的措施保護有關資料。不可向外披露資料的協議須界定不能披露的資料，以及有關各方處理此類資料的方法。如決策局／部門與外聘服務供

應機構簽訂不可向外披露資料的協議，該協議應規定有關外聘服務供應商約束其員工、董事、代理人、相聯者或承辦商等負上相同的保密責任。

(c) 交還資產

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。決策局／部門須制訂一套終止程序，確保之前發出並屬其所有的全部資產均已交還。

如離職人員或外聘機構人員擁有關於決策局／部門運作的重要知識，該等知識應予以記錄並移交有關決策局／部門。

10.2 資料分類

(a) 資料分類及標籤

在訂立保安措施前，首先應確定需要保護的數據並進行分類，例如有金錢價值的數據，或一旦遺失可導致日常操作受阻的數據。數據的保密級別應按其敏感度劃分。

決策局／部門應按照資料的保密類別制訂保密資料標籤及資料處理的程序。決策局／部門須遵守及遵從有關資料分類和標籤的要求，例如保密類別的標記、重新劃分文件的保密等級及降低文件的級別。此外，決策局／部門須遵守以下有關資訊系統處理保密資料的要求：

- 資訊系統的用戶在使用或準備使用資訊系統內提供的保密資料時，須獲得提示所使用資料的保密類別。
- 保密電郵文件的主題欄必須包括文件的保密類別。
- 存有保密資料的抽取式媒體和盛載媒體的保護盒必須穩固地貼上標籤，展示清晰可讀的識別記號和顯而易見的保密類別標記。
- 存有密碼匙的抽取式媒體，若不是用作備份用途，則無須貼上附有保密類別標記的標籤。

(b) 整體數據機密性

不論使用何種儲存媒體，所有限閱或以上類別的資料必須加密儲存。關於加密方法，決策局／部門應採用風險為本的方法評估保安風險，並根據本身的業務需要為資訊系統決定合適的保安措施和配置。如系統內有限閱及非保密資料，則不論是以應用系統或其他方式在欄位、數據庫、檔案或硬碟層次為限閱資料加密，亦能符合有關要求。

部分系統，如網絡設備（例如防火牆、路由器）及專屬設備未必能為其配置、規則集和日誌記錄此類可能被列為保密資料的數據加密。如沒有可行的解決方法，決策局／部門應採取輔助措施，例如加強接達控制，並考慮以此項限制作為理據，取得決策局局長／部門首長批准。

沒有列入任何保密類別的資料亦應予以保護，以維持資料的機密性及完整性。向外界公開資料事宜，應由與資料相關的指定工作範疇的負責人員按照《公開資料守則》的原則加以管制。決策局／部門應緊記須確保資料的機密性、完整性和可用性，並應在適當時考慮和推行保安措施，以保障資料在處理、傳輸和儲存時的機密性、完整性和可用性。

類似的保護亦適用於臨時資料和在處理過程中產生的資料。在不再使用電腦設備時，必須移除所有政府數據和系統磁碟。

根據數據處理的一般原則，任何形式的保密訊息／數據／文件，其保密級別須與書面文件相同，並須按照政府保安要求獲得相應的保護。

決策局／部門須建議其業務伙伴、承辦商或外判人員在儲存、處理及傳遞政府擁有的數據時，必須遵行政府保安要求，並設立機制以檢查他們的遵行情況。

10.3 儲存媒體的處理

(a) 設備及媒體控制

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。為確保資料在運送時得到保護，決策局／部門應：

- 提供足夠包裝，以免儲存媒體在運送途中受到實體損壞。
- 保存記錄，以識別儲存媒體的內容、所採取的保護措施、送交運輸託管人和在目的地接收媒體的時間。

由於流動裝置及抽取式媒體體積細小及容易遺失或被竊，如用作儲存資料，將存在風險，故應避免把保密資料儲存在這些裝置內。有關人員應有充分的理據才可使用這類裝置儲存保密資料，並必須使用由決策局／部門提供的流動裝置及抽取式媒體。有關人員應事先得到正式授權，方可把最少所需的保密資料儲存在流動裝置及抽取式媒體內。為盡量減低資料外泄的風險，應只使用具備適合保護保密資料的加密功能的裝置。當無須使用流動裝置及抽取式媒體儲存保密資料時，所有人員須盡快刪除該等裝置所儲存的保密資料，以盡量減低資料曝光的機會。所有人員亦須確保在棄置或重用該等流動裝置及抽取式媒體前，其內所有保密資料均已徹底清除或銷毀。

用戶未必清楚知悉，一些電子辦公室設備（包括多功能打印機及影印機）可能內置儲存媒體作為輔助裝置。決策局／部門應覆檢裝置清單，並作出適當安排，確保根據《保安規例》的要求及相關政策、程序與作業模式處理資料。這些設備如有可能用作儲存或處理保密資料，使用及管理時須加倍小心。如有需要，應關掉這些設備的檔案儲存功能，以避免儲存任何保密資料。

必須嚴格按照《保安規例》所訂的程序，處理儲存保密資料的所有儲存媒體。遇有問題，可向部門保安事務主任或政府保安事務主任尋求意見。

(b) 刪除資料

在棄置或重用媒體前，須通過(a)淨化程序或 (b)實體銷毀，把媒體內的所有保密資料徹底清除或銷毀，以確保該等資料無法復原：

(a) 淨化程序：指徹底刪除媒體上的資料，以確保無法讀取原有資料的程序。淨化程序可通過蓋寫或消磁完成：

(i) 蓋寫

對於曾用作儲存保密資料的媒體，在棄置或重用前，須通過蓋寫以刪除媒體上的資料。有關程序涉及先以一個字符及其補碼蓋寫所有可尋位址，然後再以一個隨機字符蓋寫和加以核實。刪除資料時，媒體儲存空間的每一個數元均須進行蓋寫，這點是至為重要的。就閃存記憶裝置（例如固態硬碟或閃存盤）而言，生產商一般會提供內置指令[3]，以有效淨化裝置，銷毀整個磁碟的資料，而非僅蓋寫或刪除加密密碼匙。決策局／部門應使用該等功能。儘管如此，如未能核實媒體已獲有效淨化，以及確保不能再讀取原有資料，則須使用其他淨化或實體銷毀方法。這些方法須能核實媒體已獲淨化和原有資料不能再被讀取。

(ii) 消磁

消磁如使用得宜，不失為銷毀硬磁碟、軟磁碟及磁帶等磁性媒體上的保密資料的有效技術解決方案。為硬磁碟進行消磁時，必須先移除硬磁碟上所有可能干預消磁器磁場的保護物料（例如鑄件、機殼及托架）。在消磁過程中，硬碟盤必須保持消磁器指定的某位置或方向。

[3] 建議決策局／部門在採購閃存記憶裝置（尤其是固態硬碟）時，考慮是否已具備數據淨化功能。

須實施足夠的制衡機制，例如要求進行消磁的個別人士證明消磁工作已完成。此外，須由另一人抽樣檢查已消磁的媒體，確保消磁工作已辦妥。

(b) 實體銷毀：不能淨化的儲存媒體須以切碎、解體或研磨等方法作實體銷毀。

對於閃存記憶裝置，媒體須被切碎或解體成標稱邊緣尺寸不超逾 2 毫米的碎片／顆粒。

至於光學儲存媒體（光碟、數碼影像光碟、藍光光碟和磁光碟），則須切碎或解體成碎片／顆粒：

- 如媒體曾用作儲存機密類別以上的保密資料，則碎片／顆粒的標稱邊緣尺寸不得超逾 0.5 毫米，表面面積不得超逾 0.25 平方毫米；或
- 如媒體曾用作儲存機密或限閱資料，則碎片／顆粒的標稱邊緣尺寸不得超逾 2 毫米。

光碟媒體亦可以通過研磨銷毀，以磨掉存有資料的光碟表面。

對於曾用作儲存機密類別以上保密資料的媒體，除採用上述程序進行淨化外，亦應在棄置有關媒體前作實體銷毀。

為遵行有關要求，須使用適當的工具蓋寫媒體上原本儲存了保密資料的儲存區。市面上有具備安全刪除資料功能的商業軟件，這些軟件符合在儲存區多次蓋寫的業界良好作業模式，包括以不同形式蓋寫，以確保徹底刪除資料。由於將閃存式固態硬碟或通用串列匯流排閃存盤內的個別檔案完全蓋寫未必可行，因此應淨化整隻硬碟而非個別檔案，以確保完全刪除資料。

可考慮進行加密刪除，作為數據淨化以外的另一種方法。這種方法會蓋寫用作加密數據的加密密碼匙，但這種方法也容易帶來風險，例如加密算法被破解、備份匙未被刪除和不能保證數據已被淨化。決策局／部門在進行加密刪除前，須評估有關風險及潛在影響。在銷毀保密資料時，加密刪除可與其他淨化和實體銷毀方法同時使用，而不可只單獨以加密刪除方式淨化資料。

須實施制衡機制，以核實是否已順利完成安全刪除程序。儲存媒體應由其他人員抽樣檢查，以確保所有保密資料已妥為清除或銷毀。

用戶如認為將要棄置或重用的電腦或儲存媒體上存有會引致資料私隱問題的資料，則應採取與刪除限閱資料類似的步驟。

如欲獲取更多有關銷毀及棄置儲存媒體的資料，可參考以下文件：

- **銷毀及棄置儲存媒體實務指引**
  可在政府資訊科技情報網下載
  (https://itginfo.ccgo.hksarg/content/itsecure/techcorner/practices.shtml)

11. 接達控制

決策局／部門須防止資訊系統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

(a) 最小權限原則

決策局／部門在向用戶及技術支援人員分配資訊系統的資源及權限時，須確保能遵從最小權限原則。這項原則將用戶可接達的資訊系統資源（例如數據檔案、資訊科技服務及設施或電腦設備）或接達的種類（例如讀、寫、執行、刪除），限制在履行其職責所需的最低限度。

(b) 資料接達

決策局／部門須確保除非獲相關資料擁有人授權，否則不得授予資料接達權限。資料擁有人應訂立適當的接達控制規則，以及個別用戶職務需要的資料接達權限。接達控制的詳細程度和限制應能反映有關資訊保安風險。

(c) 保密資料接達控制

任何人士在未經適當認證前，不得接達保密資料。可使用的認證方法有多種，包括密碼、智能卡、權標、生物特徵和一次性密碼。接達儲存機密類別或以上保密資料的資訊系統，須使用多重認證。

邏輯接達控制是指除實體接達控制（例如限制出入放置系統的地方）以外對資訊科技資源的控制。一般來說，邏輯接達控制包括四大元素：用戶／用戶群組、資源、認證和授權。

- 用戶／用戶群組是指已登記及經確定可接達資訊科技資源的人員。
- 人員將獲授權接達系統資源，例如網絡、檔案、目錄、程式和數據庫。
- 認證是指核實用戶身分。認證通常基於三個要素進行：用戶所知的資料（例如個人辨認號碼或用戶名稱／密碼）、用戶擁有的憑證（例如權標或智能卡）或用戶的特徵或行為的資料（例如指紋、面部特徵、視網膜和聲音等生物特徵），如採用至少其中兩個要素（一般稱為多重認證），可加強認證控制。
- 用戶／用戶群組經過認證後，便會獲授權接達系統資源。

11.2 用戶接達管理

(a) 數據接達控制

須按照「有需要知道」原則授予資料接達權限，並須明確界定、記錄和定期覆檢。所有行政權限和數據接達權限（包括暫時的接達）均須定期覆檢（例如至少每年一次，最好每年兩次），以識別和註銷不需要或過度的權限。對於部分高權限系統帳戶使用情況的定期檢查／審計應由獨立方進行，以確保這些帳戶是為合法目的而使用。此外，亦須備存有關批准和覆檢接達權限的記錄，以確保各方遵守適當的審批程序，並確保能因應人事變動更新有關人員的接達權限。

資料處理設施（例如放置資訊系統的實際場地）的使用權，亦應根據相同的原則管理。

須設立正式的程序，以管制分配資訊系統及服務接達權限的事宜。該等程序須涵蓋用戶接達周期所涉及的各個階段，由最初的新用戶登記、密碼提供和密碼重設，以至最後的用戶取消登記（用戶不需再接達有關資訊系統及服務）。

(b) 控制特別權限的使用

對於擁有特別接達權限的帳戶或用戶（例如管理員或系統帳戶），以下為限制和控制使用有關權限的規定：

- 須確定每個系統或應用系統所涉及的特別權限和數據接達權限，以及需獲分配有關權限的用戶。
- 須根據最小權限原則及職務分工向用戶授予特別權限和數據接達權限。
- 須將特別權限和數據接達權限授予有別於常規業務活動所使用的用戶名稱。
- 不得以高權限帳戶進行常規業務活動，包括但不限於閱讀電郵、瀏覽互聯網和下載檔案。
- 應制訂特定程序，以防預設的管理員用戶名稱被未獲授權人士擅用。
- 高風險接達應採用多重認證。

(c) 移除接達權限

所有用戶權限和數據接達權限(包括暫時及緊急的接達)如在一段預定時間內無任何操作,必須註銷。這項要求須由決策局／部門通過系統／應用系統的自動保安檢查,或定期的人手覆檢(例如檢查對上一次登入的時間),確實執行。

此外,須註銷不再需要的用戶權限和數據接達權限,例如在終止或更改僱用某人員後。確定用戶權限和數據接達權限的文件須予以更新,以反映接達權限已被移除或調整。如離職人員知悉用戶名稱的密碼,而這些名稱將需繼續使用,則須在終止或更改僱用該人員時更改這些密碼。

用戶權限和數據接達權限宜授予群組而非個人(例如群組接達清單)。在此情況下,決策局／部門須從相關群組接達清單中移除離職人員,並通知各方不要與離職人員分享任何資料。

(d) 用戶識別

應建立個人問責制,使相關人員為其行動承擔責任。就資訊系統而言,可通過使用能識別個別人士的用戶名稱,當發生事故或發現違反資訊科技保安政策事件時,便能夠追蹤用戶在系統的活動,藉此識別及鑑定系統用戶,以達到問責的目的。

除非因業務需要(例如示範系統)而無可避免,或無法在資訊系統實行,否則不得使用共用或群組用戶名稱。任何關於這項要求的豁免必須有充分的理據,並須得到部門資訊科技保安主任明確的批准。決策局／部門須權衡系統可能遭受的保安風險,提出支持使用共用帳戶的理據。決策局／部門須定期覆檢共用或群組帳戶的需要,並於理據不復存在時移除帳戶。

11.3 用戶責任

(a) 用戶問責制

用戶須為以其用戶名稱進行的一切操作承擔責任。用戶只可使用其用戶名稱執行獲授權的工作和功能。須禁止未經批准的共用用戶名稱。有關用戶名稱的詳情,請參閱第 11.2(d)節—用戶識別。

(b) 共用密碼的風險

共用密碼會有違用戶問責制及接達控制的不容否認原則。除非有一套能確認用戶身分以確實執行用戶問責制的措施，否則密碼不得共用或外泄。如有需要共用密碼（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），不能確實執行用戶問責制，則須給予充分的理由以事先得到部門資訊科技保安主任明確的批准。決策局／部門須就系統可能遭受的保安風險說明使用共用密碼的理據。共用密碼無需使用時應立即重設，需長期共用的密碼則應經常更改，以盡量減低違反保安事項的風險。

(c) 密碼保護

須時刻妥善保護密碼。當儲存密碼時，須採用接達控制及加密等保安控制措施以保護密碼。由於密碼是登入系統的關鍵憑證，因此在不可信任的通訊網絡傳輸時，必須加密處理。如無法進行密碼加密，決策局／部門須推行輔助控制措施，例如經常更改密碼。

11.4 系統及應用系統接達控制

(a) 資料接達限制

決策局／部門須確保資訊系統採取適當及與其保安要求和所接達資料的敏感度相稱的認證機制和措施。政府已發布《電子認證風險評估參考架構》，旨在提供一致的方式，作為決策局／部門就電子政府服務制訂合適的認證方法時的參考。該架構務求令市民／有關人員在使用有類似認證要求的電子政府服務時有一致的體驗及界面。決策局／部門在制訂和推行其電子政府服務的電子認證要求時，應盡可能遵從該架構。有關該架構的詳情，請參閱：

- **「電子認證架構」專頁：**
  可在政府資訊科技情報網下載
  (https://itginfo.ccgo.hksarg/content/eauth/index.html)

視乎所需的保安控制程度，使用密碼是一個簡單的認證方法。應考慮在認證系統使用密碼檢查程序，以確實執行密碼組合準則，並協助用戶揀選較可靠的密碼，例如避免選取低強度密碼或懷疑已外泄的密碼。另一種認證方法是使用多重認證（例如智能卡或權標），充當保安容器以識別用戶及儲存其他保安相關資料（例如加密匙），或一次性密碼以提供額外的認證。舉例來說，除非用戶出示權標（已擁有）及有效密碼（已知），否則不能啓動受保護的系統。高風險接達（例如遠程接達內部網絡）應採用多重認證，並應考慮以此作為所有新推行或升級的系統須遵守的標準。對於部分應用系統，可選用質疑／應答方案向用戶發出一些資料或問題，要求用戶準確應答後才能成功登入。

為減低密碼因受到如暴力攻擊等密碼猜測活動而外泄的可能性，須控制連續嘗試登入失敗的情況，亦須訂立及執行嘗試登入次數、封鎖帳戶時限及封鎖計時器重設時限。在達到嘗試登入次數的上限後，帳戶便會自動失效。此外，亦可考慮採用增長每次連續登入嘗試的間隔時間的機制，以防範密碼猜測活動。可同時使用用戶接達記錄分析工具及中央記錄伺服器，以維持記錄的完整性，亦能監察用戶接達活動及協助事故調查。

(b) 密碼政策

密碼即保密的字串或符號，是用作防止在未獲授權的情況下接達資料的保安措施。資訊系統可能設有不同類別的電腦帳戶，包括為決策局／部門用戶或使用政府服務的市民而設的服務帳戶或用戶帳戶。決策局／部門須審慎地為各類帳戶制訂密碼政策，並記錄有關政策，務求在保安要求和運作效率之間取得平衡。密碼政策須於所有資訊系統上確實執行。

密碼政策須至少訂明最短密碼長度、初次密碼設定、受限制字詞及格式、密碼更改周期的要求，以及一套良好的揀選密碼規則，並混合採用其他控制措施，如密碼記錄、帳戶鎖定，以及定期更改密碼。除非技術上不可行或有真正的實施操作局限，否則最短密碼長度須規定為至少八個字元。這些控制措施可減低密碼因受到如暴力攻擊等密碼猜測活動而外泄的風險，並應盡可能推行。密碼政策應定期進行審計。

所有載有保密數據的資訊系統均須執行以下的嚴謹密碼政策。此外，如任何資訊系統被入侵時可能會影響上述系統的安全（例如資訊系統與載有保密數據的資訊系統共用同一個網絡分段、或能夠對載有保密數據的資訊系統進行管理功能的特定設備），亦須執行以下的嚴謹密碼政策。如以下嚴謹密碼政策的任何控制措施因技術或操作局限而無法推行，須得到部門資訊科技保安主任明確的批准，而相關的密碼政策調整和理據須予記錄。所有其他資訊系統亦應盡可能採用以下嚴謹密碼政策。

嚴謹密碼政策：

控制措施	**設定**
複雜度和長度	• 由至少八個字元組成，包括大寫字母、小寫字母、數字及特殊字符，或 • 由至少十個字元組成，包括至少三個類別的字符 [4]
密碼記錄	至少記錄八個之前使用過的密碼
帳戶鎖定	五次或更少嘗試登入失敗後
定期更改密碼	每六個月或更頻繁

[4] 類別包括 1) 大寫字母、2) 小寫字母、3) 數字、4) 特殊字符（例如鍵盤上顯示的符號）和 5) (1)至(4)未涵蓋的其他字符（例如非英語語言的 Unicode 字符）。

(c) 揀選密碼

決策局／部門應制訂一套良好的揀選密碼規則，並分發予所有用戶。在可行的情況下，應修改設定用戶密碼的軟件，使其能根據部門資訊科技保安政策確實執行密碼規則。

以下是揀選密碼的一些指引：

<u>不應</u>

- 不應使用任何形式的登入名稱（原形、倒寫、大寫、重複等）。
- 不應使用任何形式的本人姓氏或名字。
- 不應使用配偶或子女的姓名。
- 不應使用他人容易取得的其他個人資料，包括身份證號碼、車牌號碼、電話號碼、出生年月日、居所街道名稱等。
- 不應使用由相同字母組成的密碼，例如“aaaaaa”。
- 不應使用連貫的字母或數字，例如“abcdefgh”或“23456789”。
- 不應使用在鍵盤上相鄰鍵碼組成的密碼，例如“qwertyui”。
- 不應使用能夠在英語或其他外語詞典中查到的單字。
- 不應使用能夠在英語或其他外語詞典中查到的單字的倒寫。
- 不應使用廣為人知的縮寫，包括決策局／部門名稱、工程名稱等的縮寫。
- 不應使用稍為修改以上第 1 至 10 項所述例子後組成的密碼。稍為修改的形式包括附加或加插數字或符號，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。
- 不應使用少於八個字符組成的密碼。
- 不應重用近期使用過的密碼。

<u>應</u>

- 應使用由一組冗長且易於記憶的單字組成的密碼短句，例如 1Apple&2orange&3banana，以大大增加透過暴力破解密碼的難度。
- 應根據不同的保安要求及所需保護的資訊資產的價值，於不同的系統使用不同的密碼。
- 應使用不容易猜到但方便用戶本人記憶的密碼，這樣便無須將密碼寫下。
- 應使用無須眼看鍵盤即能快速輸入的密碼，以避免行經的人看到所輸入的內容。

不當密碼示例：

“password”	最容易猜到的密碼
“administrator”	用戶登入名稱
“cisco”	供應商名稱
“peter chan”	個人姓名
“aaaaaaaa”	重複同一個字母
“abcdefgh”	連貫字母
“23456789”	連貫數字
“111111”	重複同一個數字
“1q2w3e4r5t”	鍵盤上相鄰鍵碼組成的密碼
“qwertyui”	鍵盤上相鄰鍵碼組成的密碼
“computer”	在詞典中查到的單字
“computer12”	稍為修改過在詞典中查到的單字
“c0mput3r”	稍為修改過在詞典中查到的單字，例如以“0”替代“o”，以及以“3”替代“e”
“superman”	虛構人物的名字

(d) 密碼外泄

決策局／部門應提醒有關人員禁止下列可導致在未獲授權的情況下接達資訊系統或削弱資訊系統保安的活動：

- 互動式登入嘗試，包括猜測密碼及以暴力攻擊。
- 通過社交工程或仿冒詐騙獲得密碼。
- 經監看、觀察及使用相機等途徑得知密碼。
- 以竊聽網絡通訊破解密碼。

(e) 系統／保安管理員對密碼的處理

<u>不應</u>

- 除非可驗證用戶的身分，否則不應代用戶透露或重設密碼。
- 不應將密碼儲存在可供公開閱讀的檔案內。
- 不應在未經加密的情況下傳輸密碼予用戶，尤其是經電郵寄出密碼。

應

- 應根據部門密碼政策，揀選適當的帳戶初始密碼。
- 不同的帳戶應選用不同的初始密碼。
- 在用戶收到新密碼後，應在技術上強制或要求他們立即更改初始密碼。
- 應更改所有系統或由供應商提供的預設密碼，包括安裝新系統後的服務帳戶密碼。
- 應在技術上強制或要求用戶定期更改密碼，或在密碼外泄的情況下立即更改密碼。
- 在不可信任的網絡傳遞訊息時應加密密碼。
- 應使用單向功能拼湊密碼。在可行的情況下，以「加鹽」方式拼湊密碼，使同一密碼產生不同的拼湊輸出。
- 如多次連續登入失敗，則應關閉用戶帳戶。
- 應提醒用戶保護其密碼的責任。

系統保安功能

以下是一些操作及應用系統所提供較理想的保安功能，這些功能有助執行以上建議的部分揀選密碼準則。決策局／部門應盡可能啓動這些功能。

- 在嘗試登入失敗次數達到預設上限後自動暫停用戶帳戶。
- 在帳戶操作暫停後，規定有關帳戶必須經系統／保安管理員人手處置後才能重新啓動。
- 禁止用戶使用短於預設長度的密碼，或重用先前使用的密碼。
- 系統／應用系統進行自動保安檢查，或資訊科技保安管理員定期進行人手覆檢時（例如檢查對上一次登入的時間），如發現任何帳戶在一段預定時間內無任何操作，帳戶須註銷或失效。

(f) 終端用戶對密碼的處理

密碼機制與操作系統一樣，也存在相同的保安漏洞，即用戶揀選不當密碼、密碼外泄及密碼猜測程式。

不應

- 除非備有足夠的保護措施，否則不應寫下密碼。
- 即使有極為充分的理由，也不應透露或出示密碼。
- 不應在顯示器展示密碼。
- 不應（尤其是通過互聯網電郵系統）寄出未加密的密碼。

- 如網站儲存了用戶的個人資料(例如身份證號碼),用戶不應揀選這些網站提供的「記憶密碼」功能,而應取消瀏覽器軟件的有關功能,因為可實體接達用戶系統的人可接達這些網站所儲存的資料。
- 除非有關媒體可阻止未獲授權人士接達(例如設有接達控制或加密密碼以作保護),否則不應將密碼儲存在任何媒體。
- 不應將用作加密的接達密碼(例如密碼、密碼短句、個人辨認號碼)儲存在流動裝置。

應

- 應定期更改密碼,例如每九十天更改密碼一次。
- 在首次登入時應更改預設或初始密碼。
- 如懷疑密碼已外泄,應立即更改密碼。更改密碼後,應通知系統／保安管理員,以便進一步採取跟進行動。
- 如因維修及支援服務的需要而向供應商透露密碼,則應在維修及支援工作完成後立即更改密碼。

11.5 流動資訊處理及遠程接達

(a) 流動資訊處理及通訊

須制訂正式的使用政策及程序,並針對使用流動資訊處理及通訊設施的風險採取適當的保安措施。有關的使用政策及程序須顧及在沒有保護的環境中使用流動資訊處理設備的風險。

有關的使用政策及程序應訂明實體保護、接達控制、加密技術、備份和抗惡意軟件等方面的要求,亦應訂定把流動設施連接至網絡的規則和建議,以及在公眾場所使用這些設施的指引。

須制訂及推行有關遠程接達的政策、操作計劃和程序,並只在以下情況授權用戶使用遠程接達:已有適當的保安安排和控制措施,以及這些安排和措施均符合保安要求。同時,須就遠程接達提供適當的保護措施,例如防止設備和資料被竊的實體保護、防止未獲授權人士披露資料的適當接達控制措施、對通過遠程接達進入決策局／部門內部系統的用戶進行多重認證。此外,應向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。

(b) 遠程接達／家庭辦公

遠程接達或家庭辦公用戶可隨時遠離辦公地點工作。雖然提高了工作效率,但因用戶在非政府處所工作,因此存在保安風險。

決策局／部門不應使用遠程接達軟件直接連接至部門伺服器或用戶的工作站。這樣使用遠程接達軟件相當於為攻擊者開啓了資訊系統的後門，讓他們能夠避開防火牆／路由器的保護。為維護政府基礎設施和資訊資產的保安，各決策局／部門應制訂政策，建議用戶如何安全地進行遠程工作。如因業務需要而使用遠程接達軟件，須設有適當的保安控制措施，包括但不限於：

- 提供設有嚴謹端對端保安（例如虛擬私有網絡連接、使用個人證書／密碼匙作加密保護）的安全網絡連接通道
- 限制網絡接達控制
- 推行適當的網絡管理、分段和監察
- 開啓閒置超時控制功能，以避免未獲授權的接達
- 開啓記錄功能
- 監控接達記錄以進行暴力攻擊分析
- 時刻應用最新的修補程式
- 為有適當認證的登記用戶和端點設置白名單
- 維持第 15.1(c)節所訂明與其他網絡通訊的要求
- 定期檢視使用者對遠程接達的需求，並移除不再需要的接達權限

儘管有上述規定，決策局／部門不得允許遠程接達軟件（例如遠程桌面軟件）透過互聯網直接接達政府資源。

對於通過虛擬私有網絡連接遠程接達決策局／部門內部網絡，或經互聯網遠程接達決策局／部門內部電郵系統，須使用多重認證。

應妥善保護遠程電腦，例如安裝個人防火牆、抗惡意程式軟件及惡意軟件偵測及修復措施。所有這些保安功能任何時候均應處於啓動狀態，並具有最新的惡意軟件識別碼及定義。此外，亦須為這些遠程電腦安裝最新的保安修補程式。在這些遠程電腦連接至政府內部網絡前，應為系統進行全面掃描，以偵測任何惡意軟件。

為避免資料外泄，用戶應盡量避免在遠程或便攜式電腦上儲存政府資料。保密資料不得在任何私人擁有的電腦、物聯網裝置、流動裝置或抽取式媒體中儲存或處理。在一般情況下，不得使用私人擁有的資訊科技設備透過虛擬桌面基礎設施查看或與限閱資料互動，因為這些裝置並不受制於政府的要求。決策局／部門須就此類特殊接達要求評估保安風險和獲得決策局局長／部門首長的批准，並定期覆檢接達權限，以撤銷或限制無真正需求和合法目的的接達。決策局／部門須在技術上或行政上確保對此類私人擁有的裝置有效實施完善的控制措施，包括安裝有效的防毒軟件以防範惡意威脅、啟用自動系統更新以確保及時應用最新的保

安修補程式，以及實施嚴謹密碼政策以加強接達控制。虛擬桌面基礎設施須置於決策局／部門內部網絡以外的不同網絡分段，並透過多重認證進行接達。應限制從虛擬桌面基礎設施進行熒幕擷取和貼上。可以考慮透過使用條款及條件來防止終端用戶在裝置上對虛擬桌面基礎設施進行熒幕截圖或拍照。決策局／部門應為接達虛擬桌面基礎設施提供設有嚴謹端對端保安（例如虛擬私有網絡連接、使用個人證書／密碼匙作加密保護）的安全網絡連接通道，並在可行的情況下採用流動裝置管理工具來管理裝置，以降低中間人攻擊和未獲授權接達裝置的風險。

在公共場所工作時，用戶應避免處理敏感文件，以減低把資料外泄予未獲授權人士的風險。用戶亦應避免使用公共打印機，如需打印，應迅速取回打印文件。此外，用戶應使用已設密碼的屏幕保護程式，以保護遠程電腦，切勿讓電腦無人看管。

如遠程接達的資訊系統載有保密資料，決策局／部門應記錄資訊系統上的接達活動，並定期覆檢，以找出是否有人可能在未獲授權的情況下接達系統。

用戶在遠程辦公室使用流動裝置時，應參考第 13.2 節—設備的相關指引。

有關在在家工作安排下加強個人資料保障的實用建議，可查閱個人資料私隱專員公署網站。有關實用建議亦適用於其他敏感資料。

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

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

11.6 物聯網裝置

(a) 使用

使用物聯網裝置須全面檢視端對端保安，採取風險為本的方法為物聯網裝置識別保安風險、訂定風險的緩急次序和應對有關風險，包括但不限於資產管理、認證和授權、通訊網絡、軟件和應用系統、後端基礎設施、裝置保安、實體保安等。決策局／部門尤其須備存和覆檢那些處理敏感數據或連接至內部／外部網絡的物聯網裝置清單，並作出適當安排以確保按照政府保安要求處理數據。

(b) 使用政策及程序

須設有正式的使用政策及程序，並採取適當的保安措施以防範物聯網裝置的風險。有關使用政策及程序應包括但不限於實體保護、接達控制、網絡分段、加密保護、記錄管理、裝置管理（例如使用保安修補程式和固件升級、惡意軟件偵測和預防），以及數據保護（尤其是個人資料）方面的要求。使用政策及程序亦應包括如何安全地將物聯網裝置連接至政府網絡，以及避免被惡意攻擊者控制的規則和建議。

(c) 部署

除非在推行方面在技術上不可行，物聯網裝置應同樣遵從本文件所載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。此外，物聯網裝置上不需要的功能應予關閉，以避免收集敏感資訊和連接至未獲授權的裝置或網絡。

在接達和管理物聯網裝置時，應考慮適當的保安控制措施，包括但不限於：

- 推行適當的邏輯接達控制機制，例如更改預設使用者名稱和密碼、使用嚴謹的密碼和定期更改密碼
- 關閉不需要的連接或網絡埠，並按需要限制裝置連接
- 啟用多重認證（如有）
- 加密靜止和傳遞中的保密數據
- 適當管理密碼匙，例如避免於多個端點共用加密匙
- 按照產品供應商的建議安裝最新的保安修補程式，以進行保安漏洞管理
- 根據最小權限原則和職務分工向用戶授予接達權限
- 在物聯網裝置執行保安啟動

對於使用中的物聯網裝置，決策局／部門應避免在這些物聯網裝置收集和儲存保密資料。如因為業務需要處理保密資料，須將數據加密並傳遞至保安控制措施符合相關政府保安要求的安全後端儲存。如因業務需要而無可避免須將保密資料儲存在沒有人員看管的物聯網裝置，則在偵測到並確認實體保護遭到嘗試入侵時，須實施適當的實體保護和輔助措施（如刪除數據和中斷網絡連接）。

12. 加密方法

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

12.1 加密控制措施

(a) 數據加密

在傳遞及儲存時，使用加密技術可保護數據並加強機密性。檔案加密的模式很多，例如使用程式自備的加密功能、外置硬件設備、保密匙加密和公開密碼匙加密等。

應用系統的密碼保護功能，主要用於保護檔案，防止他人在未獲授權的情況下取閱資料。在保護資料機密性時，用戶應把檔案妥為加密，而非單靠密碼保護。使用密碼時，須遵行第 11.4(b)節—密碼政策及第 11.4(c)節—揀選密碼所載有關選擇及處理密碼的作業模式。

決策局／部門須遵行有關使用加密保護保密數據的政府保安要求。

用作認證或管理的用戶密碼亦應在儲存時進行雜湊或加密。對於雜湊函數算法，應至少使用安全雜湊函數算法 2 (SHA-2)或同級別算法。視乎操作需要，SM3 也可用作雜湊函數算法。除非是舊有系統，否則不得使用安全雜湊函數算法 1 (SHA-1)。如進行加密，用作加密（只限對稱密碼匙）或解密的密碼匙須保密，而且不得向未獲授權用戶披露。

決策局／部門應進行內部研究及評估，選擇最適合其業務需要的解決方案。《資訊科技保安解決方案目錄》專題網頁提供數個加密方案，作為決策局／部門的參考，用戶尋找相關保安方案時亦可以此作為初步的參考。決策局／部門可通過以下連結連接《資訊科技保安解決方案目錄》專頁。

- **《資訊科技保安解決方案目錄》**
  可在政府資訊科技情報網下載
  (https://itginfo.ccgo.hksarg/content/coss/)

(b) 密碼匙管理

「密碼匙」一詞是指用於保密資料認證、解密或產生數碼簽署的代碼。該代碼通常以數學算法產生。這些算法常稱為「密碼算法」，產生的匙稱為「密碼匙」。

對於機密或以上保密類別的資料，對稱密碼匙的長度，起碼須有 AES 加密法 128 個數元，或相對應的長度。視乎操作需要，SM4 也可符合此要求。而非對稱密碼匙的長度，則須至少有 RSA 加密法 2048 個數元。此外，根據操作需要，亦可使用密碼匙長度最少達 224 個數元或同級的橢圓曲線加密技術，以及 SM2，以符合有關要求。至於限閱資料，亦應採用上文建議的密碼匙長度。決策局／部門應為存有限閱資料的系統制訂升級計劃，以符合密碼匙長度要求，並定期覆檢計劃以確保升級過程按預定安排進行。

用作處理機密或以上資料的密碼匙必須與所處理的資料分開儲存。密碼匙可儲存在智能卡晶片、權標或磁碟等，並用作認證及／或為資料解密。確保密碼匙得到保護和管理至為重要。此外，在分發檔案時將解密匙與加密檔案一併分發十分危險，因為一旦有人取得解密匙，便很容易開啓檔案。

應根據以下各點妥善記錄和執行密碼匙管理：

(i) 密碼匙產生
- 產生密碼匙的設備應得到實體保護。

(ii) 密碼匙儲存
- 應妥善存放主密碼匙，例如將之存放在硬件保安模組或可信任的平台模組，不應把有效的主密碼匙帶離安全的儲存位置。

(iii) 密碼匙復原
- 評估是否需要可復原的密碼匙。如需要，應只限由獲授權人員為密碼匙進行復原。
- 密碼匙復原密碼應受到至少兩重獨立接達控制作保護，並只限由獲授權人員進行資料復原。

(iv) 密碼匙備份
- 應為密碼匙備份，並採取妥善的保護措施。
- 應明文訂立有關接達備份密碼匙的程序。

(v) 密碼匙傳送
- 密碼匙不應與數據或載有加密數據的媒體一併傳送。

(vi) 密碼匙退役

- 應訂定密碼匙的啓用及停用日期，減低因保安威脅(如暴力攻擊、職位變動、開放式辦公室環境等)而導致密碼匙資料外泄的機會。
- 應制訂註銷及更換密碼匙的程序。

(vii) 交易活動記錄

- 應以審計追蹤記錄所有接達密碼匙復原密碼的活動。
- 應以審計追蹤記錄所有接達備份密碼匙的活動。

在不同加密技術的推行方法中，密碼匙可用作加密及解密數據(有時稱為數據密碼匙)，並由另一條密碼匙保護(亦稱為密碼匙加密密碼匙)。在這情況下，應根據相關政府保安要求保護最終的密碼匙加密密碼匙。

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

(a) 場地準備

由於大部分關鍵資訊科技設備一般放置在數據中心或電腦室內，因此數據中心或電腦室的場地準備工作必須慎重進行。場地準備工作須包括以下幾方面：

- 選址及場地規劃
- 供電及電力需求
- 空氣調節及通風
- 防火、火警探測及滅火
- 水患及水浸控制
- 實體出入控制

首先，決策局／部門應參考有關一般要求和良好作業模式的現行選址和場地準備工程指引。這些指引包括但不限於：

- **數據中心設計及場地準備實務指引**
  可在政府資訊科技情報網下載
  (https://itginfo.ccgo.hksarg/content/itop/itm_site_preparation.htm)

決策局／部門須根據放置在數據中心或電腦室內的資訊系統的保密類別遵行實體保安要求[5]。如辦公場地未能符合實體保安要求，決策局／部門須按個別情況尋求政府保安事務主任的意見。

如要設置無線通訊網絡，須先進行場地勘察，確保無線訊號能覆蓋預期範圍，並決定無線設備的適當擺放位置。

[5] 對於在政府物業進行涉及建造或改建房間，以為保密數據提供安全儲存的任何建築或裝修工程，決策局／部門須參考政府保安要求，並向建築署說明所需的保安級別，而建築署須按照訂明指引所訂的保安級別進行所需工程。決策局／部門無需取得指引的詳細規格，而且由於保安原因，這些規格通常不會披露。

(b) 防火措施

每更當值操作人員都應組織防火小組，並明確編配各小組成員的職責。必須定期進行火警演習，以便各人員演練發生火警時的程序。

不屬防火小組的操作人員須學會使用火警偵測、防火及滅火系統和手提滅火器。

危險或易燃物品應放置在遠離辦公室的安全位置。文具等大量採購物品不應存放在數據中心或電腦室。在數據中心或電腦室存放的文具用品不應超過一更當值工作所需的數量。

手提滅火器應放在電腦區域的當眼或適當位置，並貼上檢驗標籤及至少每年檢測一次。

應安裝煙霧偵測器以輔助滅火系統，安裝位置應在整個電腦區域較高的位置並處於天花板的下方及／或高架地板的下方。此外，宜安裝熱能探測器，安裝位置應在電腦區域天花板的下方。當發生火警時，熱能偵測器應發出警報聲。

應優先考慮使用氣體滅火系統。如使用液體滅火系統，則宜選擇乾喉花灑系統而非一般灑水系統。所有滅火系統應每年進行檢測。滅火系統應分開處理，以免一個電腦區域內的火警會啓動辦公室內的所有滅火系統。

(c) 實體接達控制

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。應教導人員避免在未獲授權人士面前輸入密碼，並在辭職或離職時交還卡匙或接達器件。只有獲授權人員才可獲知密碼及獲發磁卡匙，而密碼記錄必須存放在安全的地方。不應向任何未獲授權人士透露卡匙或入口處密碼。

所有人員須確保其辦公室的保安。如辦公室可從公共地方直接進入，則在無人使用時，不論時間長短，均應鎖上，以保護其內的資訊系統或資訊資產。

須備存、保持更新並定期覆檢一份獲授權進入數據中心、電腦室或其他支援關鍵作業地方的人士的名單。如情況許可，要求清潔承辦商指定專人清潔數據中心或電腦室，並向清潔承辦商索取有關員工的個人資料。在維修資訊系統期間，必須由負責的人員監督外聘人士施工。

如沒有獲授權人員陪同，供應商支援人員、維修人員、工作小組或其他外聘人員等訪客均不得進入數據中心或電腦室。獲准進入數據中心或電腦室的人士須適當地展示身分證明文件，以便識別擅自闖入的人士。同時，須保存及妥善備存訪客出入記錄以作審計之用。出入記錄宜包括訪客姓名及其所屬的機構、訪客簽名、到訪日期、進入及離開時間、到訪目的等。

在電腦區域範圍內的所有受監控保護及保安地帶須展示清晰顯眼的警告，以阻止陌生人闖入。另一方面，數據中心／電腦室與資料控制室之間的走廊（如有）不應對外開放，以免有人暗中從數據中心／電腦室擅取資料。

在電腦區域範圍內的所有受監控保護及保安地帶應鎖上並定期檢查，以免未獲授權用戶輕易進入電腦室。適用的鎖包括（但不限於）插銷鎖、密碼鎖、電子鎖及生物特徵鎖。

決策局／部門應考慮安裝攝錄機（或閉路電視）以監控放置關鍵／敏感系統的電腦區域並記錄影像。攝錄機的視線範圍應覆蓋整個電腦區域。攝像記錄應保留至少一個月，以便日後在有需要時回放。此外，應考慮在已放置關鍵／敏感系統的區域安裝入侵者偵測系統。

13.2 設備

(a) 設備選址及保護

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。在物聯網裝置方面，須根據物聯網裝置儲存、處理和傳遞資料的保密類別來執行保安控制措施，以防裝置遺失、被盜和遭受破壞。

應適當控制任何人士將資訊科技設備帶離場地。處理流動裝置及抽取式媒體時，決策局／部門須備存一份獲授權設備清單，並定期進行盤點，以檢查這些設備的狀況。另外，決策局／部門須採取出入檢查程序或盤點記錄措施，以識別被帶走的流動裝置及抽取式媒體。雖然如此，將資訊科技設備帶離場地的人員亦不應在公眾場所隨意放置這些設備，並應在無人看管時將設備鎖好，以防遺失及被盜。人員須保管因業務需要而獲准使用的物品（如流動裝置及抽取式媒體），不應在欠缺妥善保安措施的情況下隨意放置業務物品。

為慎防他人非法接達系統，任何人員如需離開工作崗位，須啓動工作站的重新認證功能（例如設有密碼的屏幕保護程式），或須登出系統或中斷連線。工作站如長時間閒置，則須關掉，以防他人在未獲授權的情況下接達系統。

須小心放置顯示資訊系統所載保密資料的屏幕，以防被未獲授權人士窺看保密資料。人員應考慮安裝屏幕防窺片，以限制屏幕可視角度。

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

(a) 最小功能原則

應把資訊系統的配置設定為只提供所需的功能，並且明確地禁止或限制功能、埠、規約及／或服務的使用。同時，應審慎覆檢所提供的功能及服務，以確定哪些功能及服務可刪除。管理員應考慮關閉資訊系統內不使用或不需要的實體及邏輯埠和規約（例如通用串列匯流排埠、檔案傳送規約、保密外殼），以防止他人在未獲授權的情況下連接裝置、傳送資料或採用隧道技術。

當進行系統強化、分配資源和權限，以及接達網絡或網絡服務時，須採取最小功能和最小權限兩項原則。有關最小權限原則的詳情，請參閱第11.1(a)節－最小權限原則。

(b) 變更管理

須慎重考慮會影響現行保安保護機制的變更。應控制對資訊系統作出的任何變更。操作系統及應用軟件應受到嚴格的變更管理控制，和應考慮以下各點：

- 識別及記錄重大變更
- 策劃及測試變更
- 評估有關變更的潛在影響，包括保安方面的影響
- 建議變更的正式審批程序
- 向有關各方傳達變更的詳情
- 針對變更失敗和不可預知情況的復原程序，包括終止變更及系統復原的程序和責任
- 提供一套緊急更改程序，以便迅速及在監控下執行變更以應對事故

(c) 操作及行政程序

須妥善記錄、遵從、維持和定期覆檢操作及管理程序，並提供給有需要的用戶參閱。此外，應備妥與資訊處理及通訊設施有關的系統活動的文件記錄，例如電腦啓動及關機、備份、設備維護、媒體處理、電腦室管理等。決策局／部門應建立、維持及定期覆檢資訊系統的基本配置。

(d) 容量管理

應監察資源的運用以實行容量管理，並應就有關系統的業務需要訂定容量要求。

應為資訊系統制訂容量管理計劃，以概述決策局／部門監察、分析和調整資訊系統容量的方法和程序。這有助於確保資訊科技基礎設施有足夠的容量來處理目前和規劃中的業務工作負載。負責預算的人員應顧及容量管理計劃的需求。

14.2 防範惡意軟件

(a) 用戶的保護措施

為了防範惡意軟件的威脅，用戶應確保其工作站及流動裝置已安裝及採取惡意軟件的偵測及修復保護措施。此外，有些產品亦可在一定程度上防範間諜軟件／廣告軟件。

但是，如沒有更新惡意軟件定義，保護軟件將無法偵測及防範最新型的惡意軟件攻擊。用戶須定期更新惡意軟件定義和偵測及修復保護引擎。更新功能應設定為自動更新，而更新頻率至少須為每天一次。如無法進行自動更新（例如不常接達網絡的流動裝置），至少須每周以人手更新一次。用戶亦應注意，一些嚴重的惡意軟件也可能不時爆發。如發生上述情況，用戶須遵從有關指示，並即時更新最新惡意軟件定義，以防惡意軟件爆發。

以下是防範惡意軟件的保安指引：

- 啓動即時偵測以掃描現行程式、執行程式及正在處理的檔案是否附帶惡意軟件。此外，根據操作需要定期對系統進行全面掃描。
- 在使用前，檢查儲存媒體上的任何檔案及經網絡收到的檔案是否附帶惡意軟件。
- 避免開啓可疑的電子訊息，不要點擊來源不可信任的劃一資源定位址連結，以免被引導至惡意網站。

- 在使用前，檢查附件及下載檔案是否附帶惡意軟件。
- 在安裝任何軟件前，先驗證軟件的完整性（例如比較校驗和值）及確保軟件並無附帶惡意軟件。在安裝任何執行程式／軟件（包括經電子訊息收到或自互聯網下載的執行程式／軟件）前，應先得到決策局／部門指定人員的批准。
- 應通過主硬磁碟啓動工作站。未經允許不得通過抽取式裝置啓動工作站。
- 切勿使用來源或源頭不明的儲存媒體和檔案，除非已檢查並清除儲存媒體和檔案上的惡意軟件。
- 遵從第 14.3(a)節—數據備份及復原的指引，以備份數據。

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，亦應採取適當的措施防範惡意軟件，以保護其工作站及流動裝置。

(b) 局部區域網絡／系統管理員的保護措施

為了防範惡意軟件，局部區域網絡／系統管理員須確保伺服器、工作站和流動裝置均採取惡意軟件偵測及修復保護措施。惡意軟件定義應設定為自動更新，而更新頻率至少須為每天一次。如無法進行自動更新，局部區域網絡／系統管理員應至少每周及在有需要時以人手更新一次。

惡意軟件偵測及修復保護措施應支援企業管理，從而有助進行中央管理。有關企業管理的更多詳情，請參閱第 15.1(b)節—網絡保安控制措施。

局部區域網絡／系統管理員亦應推行以下技術控制措施：

- 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。
- 啓動抗惡意軟件保護程式，以掃描所有經互聯網輸入的網絡通訊。通訊閘的配置應設定為可阻截、隔離及刪除含有惡意內容的網絡通訊，以及建立審計記錄以供日後參考。
- 就發展中或用作測試的電腦設備及軟件，均應考慮資訊保安事項及推行相關程序。除非已推行妥善的控制措施，否則網絡環境愈不穩健，便愈容易遭受攻擊。
- 有關人員、承辦商或外判員工的所有電腦須進行全面掃描後，方可接達政府網絡。
- 要求外聘供應商於安裝新電腦、維修服務或安裝軟件後，以最新的惡意軟件識別碼為用戶的硬磁碟進行惡意軟件掃描。

在管理伺服器時，局部區域網絡／系統管理員應遵守以下保安指引：

- 通過主硬磁碟啓動伺服器。如電腦應通過抽取式媒體（例如軟磁碟、通用串列匯流排閃存盤或硬磁碟、光碟等）啓動，在啓動前必須掃描抽取式媒體是否附帶惡意軟件，這樣可防止伺服器受開機磁區電腦病毒感染。
- 通過使用接達控制功能保護伺服器的應用程式，例如儲存應用程式的目錄應設定為「唯讀」。此外，應按照「有需要賦予」原則賦予最小權限，尤其是「寫入」及「修改」權限。
- 考慮運用文件管理解決方案共用文件，並推行適當的接達控制和保護措施。
- 在供用戶使用前，應先對所有新安裝的軟件進行病毒掃描。
- 宜預設檔案伺服器在開機後自動執行一次全面病毒掃描。
- 遵從第 14.3(a)節－數據備份及復原的指引，以備份數據。

此外，局部區域網絡／系統管理員應取得最新的安全警告訊息，並教導用戶防範惡意軟件的良好作業模式：

- 登記接收保安通知／警告訊息，以便盡早取得重要的惡意軟件警報。
- 立即向全體終端用戶轉達由數字政策辦公室所發出的保安警報，並採取必要的應變措施。
- 教導用戶以令其明白大規模惡意軟件攻擊的影響和了解感染惡意軟件的各種途徑以免感染惡意軟件，例如教導用戶一些含有惡意軟件的電子訊息，可能是仿冒其朋友或同事發出的。

(c) 偵測及復原

以下是一些電腦感染惡意軟件的徵狀：

- 執行程式的時間比正常情況長。
- 可供使用的系統記憶體或磁碟容量銳減。
- 電腦出現來歷不明／新建立的檔案、程式或程序。
- 彈出新窗口或瀏覽器廣告。
- 電腦出現異常重啓／關機的情況。
- 網絡負擔增加。

如用戶懷疑電腦感染惡意軟件，應終止一切活動，因為繼續使用懷疑受感染的電腦可能會讓惡意軟件進一步傳播。用戶應立即向管理人員及局部區域網絡／系統管理員匯報任何懷疑惡意軟件事故。如有需要，應通知部門資訊科技保安主任，並由資訊科技保安主任決定是否保安事故。數字政策辦公室中央電腦中心求助台（ccc_hd@digitalpolicy.gov.hk）可為懷疑電腦感染惡意軟件事故調查工作提供技術支援。用戶亦可在局部區域網絡／系統管理員的協助或建議下，使用市面上抗惡意軟件的軟件，自行清除惡意軟件。

移除惡意軟件並不代表能夠復原或取回受感染或被刪除的檔案。復原已損壞檔案的最有效方法是以原來的檔案取代已損壞的檔案。因此，檔案應定期備份，而且應備存足夠備份複本，以便在有需要時復原檔案。

將電腦中的惡意軟件清除後，用戶應對電腦及其他儲存媒體進行全面掃描，以確保沒有任何惡意軟件。忽略重新掃描電腦這一步驟可能導致電腦再次受惡意軟件感染。

(d) 使用內容過濾軟件

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。即使資訊系統用戶能夠連接某個網站，也不代表他們已獲准瀏覽該網站。決策局／部門應考慮使用網頁內容過濾軟件防止人員濫用資源，例如從互聯網下載大量檔案或瀏覽有害網站。這些活動不僅消耗頻寬和浪費資源，亦會增加感染惡意軟件的風險。

建立及強制執行一份網站許可名單是一種強效的內容過濾方法。只容許接達有業務需要的網站可減低系統受到攻擊的機會。決策局／部門亦可通過建立網站黑名單，防止用戶瀏覽那些網站。部分內容過濾工具已裝有網頁分類數據庫，數據庫會根據網站內容將網頁分類及評分，決定網頁是否適合閱覽，供應商亦會定期覆檢及更新數據庫。決策局／部門應進行研究，根據本身業務需要決定合適的內容過濾方案。

14.3 備份

(a) 數據備份及復原

決策局／部門須定期進行備份工作，並須為本身的資訊系統制訂及推行備份和復原政策。用戶應定期為儲存在工作站、流動裝置及抽取式儲存媒體內的數據進行備份。備份頻率應視乎失去數據可用性所帶來的影響而定。備份復原測試亦須定期進行。須訂定並記錄備份審查和復原測試的頻率。決策局／部門在制訂備份及復原政策時，應遵從有關的良好作業模式：

- 應為所有操作數據備存備份複本，以便在這些數據無意中受損或遺失時可以重組。
- 須定期備份，以便將檔案復原至最新狀態。
- 須定期覆檢備份活動。須制訂完善的數據備份及復原程序，並設法徹底測試這些程序在實際操作環境的效用。
- 備份復原測試應結合測試備份媒體和相關工具，以及復原程序，並測試復原時間是否符合要求。
- 伺服器備份軟件應安裝在伺服器內，以加快數據傳送速度，並避免加重網絡的傳送負荷。此外，軟件應可編排在無人操作的情況下工作，以便在非辦公時間進行備份。
- 備份複本宜存放在安全及穩妥的地方，並遠離系統的所在地。即使發生災難並摧毀了系統，仍可在其他地方將系統重組。
- 除數據的備份複本外，如還需要軟件更新版本才可復原應用系統，軟件更新版本（或軟件更新的備份複本）及數據備份便應存放在一起。
- 應備存多代備份複本，使復原程序有更大靈活性和彈性。備存備份複本時應考慮實施一套「三代」計劃，以確保兩份備份複本（即上一代及再上一代的備份複本）總與最新數據及程式操作複本存放在一起。根據最新操作狀態備份的更新複本，必須與備份複本一併備存及存放。
- 應至少備存三代備份。然而，如每天備份，則在行政上可能較容易保存六至七代備份。舉例來說，星期一的每天備份應保留至下一個星期一，才被蓋寫。如有需要，檔案的月底及年底備份可保留更長時間。
- 應定期測試作備份用途的磁帶、磁碟／光碟或盒式磁帶，以確保在有需要時可復原數據。
- 如使用自動換帶機，應注意往返場外存放地點可能需要較長的運送時間，因為磁帶不一定會立即移往別處。在操作便利與備份數據的可用性（尤其是重要資料）之間，應設法取得平衡。

在一些不能預計的情況下，如數據在進行備份前被意外刪除，或數據所在的硬磁碟因破損而無法利用系統接達，則可能需要硬磁碟數據復原服務。如需要外聘數據復原服務，決策局／部門應遵從有關的良好作業模式，以減低數據外泄的風險：

- 盡可能即場進行數據復原服務，並確保承辦商在復原過程中留意保密資料的保護要求。
- 陪同承辦商人員，並小心留意，確保保密資料不會外泄。
- 淨化用作數據復原的裝備工具及有關媒體內剩餘的用戶數據。
- 與承辦商簽訂不可向外披露資料的協議。
- 遵守政府保安要求，尤其是有關外判保安的要求。

(b) 數據備份設備及媒體

須制訂適當程序儲存及處理備份媒體。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。在不能實體中斷連接的情況下，決策局／部門應考慮以邏輯方式中斷連接，例如關掉網絡裝置的連接埠，使用配備自動磁帶更換裝置的磁帶庫，以機械方式加載及卸除磁帶，或備存一份無法被惡意軟件（例如勒索軟件）接達和更新的備份副本，以確保即使生產系統被入侵，最後一個備份副本也是安全的。

備份媒體的接達須只可通過獲授權人士按既定機制進行。未獲授權人士不得進入媒體儲存庫或場外儲存室。

須適當記錄移入／移出數據庫或場外儲存室的媒體。除非得到批准，否則任何人員不得將任何媒體帶離數據中心或電腦室。為方便偵測遺失的媒體，儲存架可在空置的槽位附上標記／標籤。另須定期進行盤點以偵測備份媒體是否已遺失或遭破壞。

須妥善處理將備份媒體／手冊運出及運入場地的工作。放置媒體的運載箱應具備抗震、隔熱、防水功能，而且應能抵受磁性干擾。決策局／部門應考慮加密儲存媒體內的數據，並將媒體分成多個部分及由不同人士運送，以防止媒體被盜。

現時有許多設備，例如磁碟、光碟及數碼數據儲存磁帶等，均具備數據備份及復原功能。

磁帶是最常用的伺服器備份媒體，因應容量而言，磁帶的成本相對較低。如數據容量龐大，一次備份需要使用多套磁帶，則可使用加載磁帶機或自動加載磁帶機。為了有效使用換帶機，備份軟件必須具備支援換帶機的功能選項。

由於工作站須備份的數據量一般比伺服器的為少，不少設備均可供工作站備份。如要備份的數據量龐大，磁帶仍然是成本相對最低的設備。大部分工作站備份軟件既支援磁帶備份，亦支援抽取式光學儲存媒體。

磁帶機的磁頭應定期清洗。清洗磁頭的次數視乎操作環境及操作（備份、回復、掃描磁帶等）頻率等因素而定。部分磁帶機設有顯示器，可在使用若干次後提醒用戶清洗磁頭。有關詳情應參閱磁帶機的說明書。

應妥善儲存及維護備份媒體。應為備份媒體加上適當標籤，並存放在保護盒內及把附有的防寫標籤（如有）撥到防寫的位置。備份媒體應存放在遠

離磁場／電磁場及熱源的地方，在選擇存放地方時應依照製造商所訂的存放環境規格。

14.4 記錄

(a) 記錄的收集及保留

審計追蹤顯示日常使用系統的情況。視乎審計記錄系統的配置，審計記錄檔案或會顯示一連串的嘗試接達記錄，以得知不正常使用系統的情況。

較複雜的應用系統應具備本身的審計或追蹤功能，以便提供更多有關個人使用或濫用應用系統的資料。這種機制實際上是高度保安應用系統必不可少的，因為操作系統的追蹤功能不一定有足夠的敏感度記錄應用系統的關鍵功能。

雖然審計追蹤功能實際上可無限制地記錄個人用戶接達數據的情況和實際更新次數，但使用記錄例程會浪費系統資源，而所產生的記錄過多甚至會遮蓋不當使用的情況。因此，自行發展的審計追蹤應重點記錄用戶未能成功處理事項及接達未獲授權項目的情況。

事項記錄可包括但不限於以下資料：

- 在未獲授權的情況下的更新／接達
- 啓動／終止日期及操作時間
- 用戶識別（非法登入）
- 登入及退出操作（非法登入）
- 連接對話或終端機
- 電腦服務，例如複製檔案和搜尋

決策局／部門須根據業務需要和數據的保密類別，制訂並記錄與資訊系統工作記錄（包括保存期）有關的政策。有關政策的要求須包括但不限於記錄：

- 登入的嘗試
- 更改密碼的嘗試
- 接達關鍵檔案（例如軟件配置檔案、密碼和密碼匙檔案等）的嘗試
- 特別權限的運用（例如新增和刪除用戶帳戶）
- 用戶接達權限的變更
- 對審計政策的修改

- 啓用或停用保護系統，例如抗惡意軟件系統和入侵偵側系統

如未能記錄以上活動，須提供理據並予以記錄。

已記錄的資料最低限度應符合上述要求，以便在發現違反資訊科技保安政策事件（例如嘗試在未獲授權的情況下接達資源）時，審計有關保安措施（例如邏輯接達控制）的成效。記錄的詳細程度應與業務需要和數據的保密類別相稱。除非得到首長級人員的批准，作為審計工作或事故處理所需，否則記錄不得用作剖析個別用戶的操作情況。

由數字政策辦公室或決策局／部門在中央所提供的核准電郵系統和互聯網接達服務記錄須予記錄。在電郵記錄方面，欄位須包括但不限於發送日期／時間、客戶端的互聯網規約位址、寄件者和收件者電郵地址，以及電郵大小總值。其他有用的欄位（如電郵主旨、電郵附件的名稱和大小）和事件（如接達電郵包括閱讀、刪除、未獲授權的接達）亦應予記錄。在互聯網接達記錄方面，欄位須包括但不限於接達日期／時間、客戶端的互聯網規約位址、接達網站或劃一資源定位址。

抽取式媒體和打印機如不妥善控制其使用，會構成數據外泄的風險。決策局／部門應防止未獲授權而可以通過打印機或抽取式媒體傳輸保密數據。應採取保安控制措施，包括但不限於堵截未獲授權的抽取式媒體（如通用串列匯流排儲存裝置）的連接、記錄列印活動和把檔案傳送至抽取式媒體的活動。如果現有系統未能推行該等保安控制措施，決策局／部門須視乎系統關鍵程度、數據敏感度和如發生事故其後的影響，制訂推行端點保護解決方案的升級計劃，以加強保安保護，以及支援對伺服器、工作站和流動裝置，特別是重要資訊系統，在使用抽取式媒體和打印機以進行事故評估。

記錄保存期須與其作為有效審計工具的日期長短相稱。所記錄的資料及保存期須足夠支援違反保安事項的調查工作。由數字政策辦公室或決策局／部門在中央所提供的核准電郵系統和互聯網接達服務的記錄保存期須不少於六個月。在保存期內，記錄須妥為保存以防被竄改，並只可供獲授權人士閱讀。決策局／部門應考慮以中央記錄管理方式管理有關記錄。決策局／部門須定期覆檢記錄保存期及儲存容量，以確保記錄數據適當保留，並有足夠的儲存空間。

決策局／部門在制訂和覆檢內部的記錄政策時，應考慮以下各點：

(i) 產生記錄

- 需要產生記錄的資訊科技設備的類別和組件（例如應用系統和數據庫等）

- 記錄的事件類別
- 每類記錄事件的詳細資料（例如用戶名稱、發送的互聯網規約地址和時間標示等）
- 時鐘同步要求（例如可信任的時間來源、日期和時間的格式、同步方法和頻率等）

(ii) 傳送記錄

- 需要傳送記錄至中央記錄管理基礎設施的資訊科技設備的類別和組件
- 記錄的傳送要求（例如網絡規約等）
- 傳送記錄的頻率（例如實時、每小時等）

(iii) 儲存及清除記錄

- 記錄的保護要求（例如接達控制等）
- 記錄的儲存空間
- 記錄覆寫的準則
- 根據資訊系統風險水平訂定的記錄保存期

(iv) 分析記錄

- 職務和職責
- 需要發出警報給負責各方的事件類別
- 需要分析的事件類別
- 記錄的覆檢頻率
- 對可疑及異常活動的處理程序

如決策局／部門使用共用帳戶，系統／保安管理員應備存及定期更新共用／群組帳戶的帳戶清單。清單內的資料包括但不限於系統名稱、可共用帳戶的用戶名稱（個人姓名）、共用的用戶名稱、批准的權限、帳戶有效期及共用帳戶的理由。如有需要，在進行調查時，帳戶清單可用作追蹤在特定時間內個別用戶利用共用帳戶接達特定系統的活動。

載有機密類別或以上資料的系統須啓用審計追蹤所有數據共用接達。

如在獨立個人電腦或工作站的硬碟機儲存保密資料，則必須啓動審計追蹤及記錄功能。須根據部門記錄政策訂定的記錄保存期，預留足夠硬碟空間保存記錄。

應定期（至少每月一次）根據可信賴的時間伺服器的時間校準資訊系統的時鐘。決策局／部門應使用政府主幹網絡的時鐘同步服務或通過網絡時間規約使用香港天文台的時間伺服器。網絡時間規約的認證可加強時鐘同步程序的保安。所有設備的系統時間未必完全相同。視乎資訊系統的類

別和系統對精確度的要求，應將時間的差異控制在合理範圍內。具備同步時鐘，可使審計追蹤能夠有可信任的時間標示及更方便地記錄事件之間的聯繫。此外，在調查事件時，審計追蹤將會更加可靠。

有關政府主幹網絡時鐘同步服務的資料，可查閱政府資訊科技情報網(https://itginfo.ccgo.hksarg/content/gnet/servicevas.htm#ntp)

有關香港天文台時間同步服務的資料，可查閱天文台網站(https://www.hko.gov.hk/en/nts/ntime.htm)

14.5 操作環境的控制

(a) 安裝電腦設備及軟件

安裝電腦設備及軟件前，須先得到系統擁有人或負責的管理人員的批准，然後由獲授權人員執行。有關設備或軟件的安裝及連接工作須在不影響現行保安控制措施的情況下進行。有關設備或軟件的任何變更，均應作詳細記錄及經過測試，並應就所有安裝和提升項目備存審計追蹤記錄。

(b) 變更控制

如設施、資訊系統，以及業務和保安程序出現會影響資訊科技保安的變更，這些變更均須受到控制。須制訂更改控制程序及制訂相關的職務和職責，以確保變更得到適當控制，並須備存變更記錄，以追蹤曾作出的變更。除操作環境外，供發展、測試及運作復原的環境亦應有適當的變更控制。變更管理控制詳情可參閱第 14.1(b)節—變更管理。

14.6 技術性保安漏洞管理

(a) 漏洞管理程序

決策局／部門須進行漏洞管理程序，包括識別、評估、緩解和追蹤漏洞。將這些程序整合到常規例程中有助確保任何新漏洞在被利用前得以及時識別和修復。有效的漏洞管理亦有助決策局／部門有效管理資訊科技保安風險。

(i) 漏洞識別

決策局／部門須進行漏洞識別程序，以持續找出其資訊系統內的潛在漏洞。此程序應涉及不同的漏洞識別活動，包括漏洞掃描、滲透測試、源碼掃描、手動程式碼審查、配置審查、模擬攻擊等，以識別潛在的保安

漏洞。另一方面，漏洞識別程序還應包括監控發出保安新聞、警報、報告和其他刊物的來源（例如政府電腦保安事故協調中心），以便及時識別新的攻擊方法和未修補的漏洞。此程序中使用的漏洞識別活動也可用於保安風險評估期間的風險識別程序，以識別可能導致資訊科技保安風險的漏洞。

(ii) 漏洞評估

決策局／部門一旦發現漏洞，須進行漏洞評估程序，以評估漏洞的潛在影響和嚴重性。此評估應考慮不同數據或系統的敏感性、成功利用漏洞所造成的潛在損害或中斷，以及利用漏洞的複雜性等因素。

(iii) 漏洞緩解

決策局／部門在評估漏洞後須進行漏洞緩解程序，採取行動及時解決和緩解漏洞。此程序涉及進行完善的修補程式管理程序以安裝必要的更新，並調整配置設定以保護資訊系統。推行額外的保安控制以防止漏洞被利用，並確保使用授權軟件，也是此緩解程序的重要一環。如果無法立即採取緩解措施，決策局／部門應推行臨時應變方案或輔助控制措施。

(iv) 漏洞追蹤

決策局／部門須進行漏洞追蹤程序，以確保持續追蹤和監控已識別的漏洞及其相應的緩解工作。這包括備存漏洞清單、定期更新漏洞狀態，以及向部門資訊科技保安主任提供定期更新資料。

(b) 漏洞掃描

漏洞掃描是漏洞識別活動的一部分，應在漏洞管理程序中採用。漏洞掃描使用專門的工具有系統地檢查資訊系統是否存在已知漏洞，目的是在惡意者利用漏洞之前識別漏洞。

決策局／部門須備存漏洞掃描結果和所採取的補救措施的記錄。記錄有助日後進行保安審計和風險評估。此外，決策局／部門應定期審查和更新其漏洞掃描計劃和工具，以確保它們能夠有效應對不斷變化的威脅和漏洞。

參與漏洞掃描程序的所有人員都應接受適當的培訓和支援，以便有效地執行其工作。這包括了解如何配置和使用掃描工具、解釋結果，以及修復已識別的漏洞。政府電腦保安事故協調中心的技術中心會為決策局／部門提供漏洞掃描設施，以協助決策局／部門對其與互聯網連接的網站進行漏洞掃描。

(c) 滲透測試

滲透測試是漏洞識別活動的一部分，應在漏洞管理程序中採用。漏洞掃描試圖在不利用漏洞的情況下發現漏洞，而滲透測試則使用自動和手動技術來發現漏洞並模擬網絡攻擊以利用漏洞。滲透測試是確保資訊系統保安措施有效實施的必要方法，讓決策局／部門更了解其系統的弱點，並採取積極措施來解決這些弱點。在對資訊系統進行保安風險評估時，還可將滲透測試納入相應的風險識別程序中，以發現資訊系統中的漏洞。

在進行滲透測試前，決策局／部門應明確制訂測試的範圍和目標，其中包括與滲透測試人員就所使用的方法以及如何報告結果達成協議。滲透測試須從外部潛在攻擊者的角度進行，並可涉及主動利用可能有的漏洞。滲透測試須涵蓋網絡保安、系統軟件保安、客戶端應用系統保安，以及伺服器端應用系統保安。滲透測試人員還應了解測試的範圍和潛在的操作影響。決策局／部門可考慮聘請專門從事滲透測試的外聘承辦商來進行這些測試。

可以使用威脅情報以提供對威脅者使用的最新策略、技術和程序的見解，從而提高滲透測試的有效性。這些資訊可以指導測試的設計和執行，使測試能夠更好地模擬真實世界的攻擊，並識別當前和新興的威脅可能利用的漏洞。

與漏洞掃描的做法相若，決策局／部門須記錄所有滲透測試結果和跟進行動。記錄對於日後進行保安審計至關重要，可以為決策局／部門的持續安全態勢提供寶貴的見解。

有關滲透測試的指引，請參閱《滲透測試實務指引》。

(d) 配置審查

配置審查是漏洞識別活動的一部分，應在漏洞管理程序中採用。配置審查旨在識別可能引入漏洞並危及資訊系統保安的潛在錯誤配置。配置審查可利用自動掃描工具或透過手動審查工作，來確保資訊系統的配置正確設定並符合保安良好作業模式。

(e) 源碼掃描

源碼掃描是漏洞識別活動的一部分，應在漏洞管理程序中採用。源碼掃描是指使用自動掃描工具或透過手動程序檢查代碼，以識別資訊系統中的漏洞、錯誤和保安缺陷的程序。決策局／部門應利用源碼掃描來識別、分類和訂定修復資訊系統源碼中存在的錯誤的緩急次序。程式碼修改、應用保安編碼作業模式和推行保安控制是已識別源碼問題的常見緩解措施。

(f) 模擬攻擊

由情報驅動和威脅主導的模擬攻擊演習，是技術漏洞管理的關鍵。模擬攻擊是漏洞識別活動的一部分，可在漏洞管理程序中採用。模擬攻擊演習亦稱為紅隊演習，旨在模仿真實的攻擊，以驗證決策局／部門在保安控制上的整體實力及其抵禦實際攻擊的能力。演習利用各種方法來測試不同的漏洞點，從社交工程到精密的技術利用不等。滲透測試旨在嘗試盡可能發現更多的漏洞，而模擬攻擊則是以外部威脅者的角度進行，並有特定的議定目標（例如接達第 2 級資訊系統的特定資料庫）。

在進行模擬攻擊演習前，應先明確界定演習的目標、範圍和參與規則。應分析模擬攻擊的結果，以評估決策局／部門偵測、應對和從攻擊中恢復的能力。分析應是全面的，要同時考慮應對的技術和部門層面。應記錄調查結果，並提出補救建議。最終報告應詳細提供可行的見解，以協助決策局／部門加強保安態勢。在採取補救措施後，應重新進行測試，以驗證已識別的漏洞是否已有效解決。

決策局／部門可在模擬攻擊中利用威脅情報，例如可以透過威脅情報來改善偵察階段，因為它有助於根據潛在威脅者的已知策略、技術和程序來識別可能的攻擊媒介。這使模擬攻擊能夠更準確地反映真實世界的威脅，測試決策局／部門對最有可能遇到的攻擊的防禦能力。

另一方面，還有另一種攻擊模擬演習，即紫隊演習，在模擬攻擊過程中還涉及藍（防守）隊。藍隊參與演習旨在了解紅隊所發現的保安漏洞，並提升決策局／部門的整體防禦能力。

(g) 修補程式管理

修補程式管理是及時安裝軟件更新和修復的程序，以解決資訊系統中的漏洞和問題。它迅速解決已識別的漏洞，是漏洞緩解的重要一環。

為免有人對已知的保安問題或漏洞作出攻擊，局部區域網絡／系統管理員須在資訊系統（包括操作系統、數據庫軟件、程式庫）及在這些系統上運行的應用系統，安裝由產品供應商提供的最新保安修補程式／修復程式，或採取其他輔助保安措施。決策局／部門應確保其局部區域網絡／系統管理員了解最新推出的保安修補程式／修復程式。

有效的修補程式管理程序在維護資訊系統保安方面至關重要。隨着新發現的漏洞及相應提供的修補程式與日俱增，局部區域網絡／系統管理員有必要以有系統及管制的方式管理修補程序。

成功的修補程式管理需要一套完善的程序，即修補程式管理流程，當中包括以下多個步驟：

- 取得修補程式 — 選擇及下載適當的修補程式，並部署應用。
- 測試 — 進行測試以確定修補程式是否與其他修補程式、主要企業應用系統甚至整個環境「基準」相衝突。
- 風險評估 — 評估與安裝修補程式相關的風險及影響，並確定將採取的措施。考慮以下問題：系統應用程式的功能是否會受影響？安裝修補程式後是否需要重新啓動系統（這會令服務供應受影響）？
- 安裝 — 將修補程式安裝於目標設備，並確保修補程式僅安裝於必需的設備上。
- 遵行要求 — 核實所有設備均運作正常，並符合相關的資訊科技保安政策及指引。

此外，修補程式的安裝及管理應遵從以下指引：

- 建立及備存決策局／部門常用的硬件設備、軟件（包括其修補程式管理系統）及其版本號碼的清單。這清單對修補程式管理程序至關重要，可方便系統管理員監控及識別相關的漏洞及修補程式。
- 界定與修補程式管理相關的職務和職責，包括漏洞監控及修補等。
- 考慮統一資訊系統的配置。統一的配置可簡化修補程式測試及安裝程序。
- 監控與決策局／部門有關的資訊科技保安資源的漏洞及修補程式。
- 訂定與系統技術配置有關的安全警告訊息的應對時間表。
- 一旦確定出現保安漏洞，則應評估相關的風險及制訂將採取的措施。
- 定期覆檢修補程式管理程序，以評估其成效及效率。
- 在軟件供應商的官方網站檢查軟件產品的終止支援日期，並事先擬備可行的遷移計劃。
- 移除已終止支援的軟件產品，或升級至其他有安全更新的軟件產品。
- 教導用戶高度重視資訊科技保安及修補程式管理對日常操作的重要性。
- 定期進行保安漏洞識別，例如使用以主機或網絡為基礎的漏洞掃描工具，以找出修補程式的不足或系統的錯誤配置。
- 考慮購買修補程式管理系統，以支援整個修補程式管理周期，從而減輕人手管理工作及減少修補程式安裝／測試的時間。應為修補程式管理系統採取適當的保安措施。

當保安修補程式發布時，決策局／部門須評估此安裝相關的影響。在此安裝前，須測試及評估修補程式，以確保其成效。須通過既定更改控制程序

安裝保安修補程式。如安裝修補程式不可行，則應計劃為有關產品進行升級以消除保安問題或推行其他保安控制措施並記錄在案。

對於已終止支援的軟件，已識別的風險將不再有安全更新可供修復保安漏洞，這樣會增加成功入侵系統或網絡的機會。如有需要繼續使用已終止支援的軟件，決策局／部門須評估使用有關已終止支援軟件的保安風險，以及採取適當保安措施保護資訊系統和相關數據。為了減低已終止支援的影響，應在終止支援日期前至少六個月推行遷移計劃，而相關保安措施應於不遲於終止支援日期前實施。遷移計劃應包括但不限於使用該等軟件的風險評估、計劃取代該等軟件的日期、使用已終止支援軟件時的保安措施(如從部門網絡實體隔離、應用系統和通用串列匯流排裝置白名單)。

資訊系統的風險水平會因應其性質而有所不同，例如供內部使用的資訊系統所面對的威脅會較供公眾使用並與互聯網連接的資訊系統為少。決策局／部門須根據風險水平，為資訊系統制訂適當的修補程式管理策略，包括修補程式檢測及使用修補程式的頻率。決策局／部門須採用風險為本的方法，考慮每個漏洞的潛在影響和被利用的可能性，以確定每個漏洞的修補計劃。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。所有已知的與互聯網連接的資訊系統的保安漏洞應在保安修補程式發布後一個月內修復。一般應優先處理高風險的資訊系統。決策局／部門須遵從政府電腦保安事故協調中心發出的保安警報中所訂明的建議，以緩解其資訊系統的漏洞。

當評估是否使用保安修補程式時，應將漏洞所導致的風險與安裝修補程式帶來的風險作比較，從而評估與安裝修補程式有關的風險。如決策局／部門因任何理由而決定不安裝修補程式或並無修補程式可用，便應諮詢部門資訊科技保安主任，並須妥善記錄此事。決策局／部門亦應採取其他輔助控制措施，例如：

- 關閉與漏洞相關的服務或功能
- 調整或加強接達控制
- 加強監控，以偵測或防止實際攻擊活動

(h) 使用獲授權軟件

軟件安裝控制措施防止未獲授權的軟件出現潛在漏洞，是漏洞緩解的重要一環。決策局／部門須根據操作需要建立及備存一份獲授權軟件清單（包括免費軟件、開放源碼軟件、流動應用程式、程式庫和相關應用程式）。安裝不在獲授權軟件清單上的軟件前，須得到決策局／部門指定人員的適當批准。

至於從互聯網下載的軟件，決策局／部門必須留意，即使這些軟件是合

法下載的軟件，仍有機會隱藏惡意軟件。決策局／部門須從正式途徑取得軟件，並利用供應商提供的校驗和核實軟件的完整性。此外，決策局／部門在採用軟件前，應考慮以下幾點：

- 使用軟件／產品的需要
- 產品的過往記錄
- 修補頻率及產品供應商處理產品漏洞所需的時間
- 可能對決策局／部門帶來風險的產品特性（例如將數據與雲端服務同步）
- 如軟件／產品被入侵，對決策局／部門帶來的保安風險
- 軟件／產品的技術支援問題

軟件資產管理工具的用途是將軟件清單掃描及軟件計量自動化。軟件資產管理工具有助偵查未獲授權軟件，確保所有軟件均得到特許使用權，而且還可反映未曾使用或使用率不足的軟件特許使用權數目。決策局／部門應考慮配備軟件資產管理工具，協助管理軟件資產。

軟件資產管理有不同的產品和技術。舉例來說，有些桌面操作系統提供備存軟件資產清單的工具，以防止未獲授權軟件載入。決策局／部門應選擇最適合本身資訊科技環境的軟件資產管理工具。決策局／部門亦可委聘服務供應商推行軟件資產管理措施、進行軟件審計及安裝軟件資產管理工具。

14.7 資訊科技保安威脅管理

(a) 威脅管理機制

決策局／部門須建立威脅識別、偵測和監察機制，並定期覆檢機制，以確保其在資訊系統性質和技術進步方面的成效。此機制至少須涵蓋定期監察資訊系統（例如伺服器、虛擬私有網絡通訊閘、防火牆）的日誌記錄，以及決策局／部門相關保安裝置（例如抗惡意軟件系統、入侵偵測系統、端點偵測與回應解決方案等）所檢測到的資訊科技保安威脅的迅速應變計劃。

(b) 威脅識別和情報收集

威脅情報是為了減少威脅對資訊系統造成的危害而收集和分析的威脅相關資訊。威脅情報可以是特定攻擊的操作細節、有關攻擊者策略的資訊（例如方法、工具），以及有關不斷變化的威脅形勢的策略性資訊（例如攻擊和攻擊者的類型）。

決策局／部門須訂閱保安新聞、警報、報告和其他資訊保安刊物，了解與其業務和日常操作有關的新興保安威脅和相關風險。政府電腦保安事

故協調中心是就即將及已經發生的威脅向決策局／部門發出保安警報的來源之一。決策局／部門也可在威脅情報平台取得威脅資訊（例如惡意互聯網規約地址和域名）。

決策局／部門應考慮建立一套獲取威脅情報的機制，從不同來源（例如政府電腦保安事故協調中心）收集威脅相關資訊和分析其對決策局／部門的影響，並將所獲得的威脅情報傳達給決策局／部門內的有關各方。

(c) 威脅監察及偵測

一旦發現潛在威脅，對資訊系統的持續偵測和監控就變得至關重要。須按已訂定的檢查頻率定期檢查記錄（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不當情況或系統及應用系統誤差，均須予以記錄和呈報。如有需要，應展開詳細的調查。

不同裝置內的記錄應互相關聯，以找出潛在保安事故，以及操作和保安問題。除了應用系統記錄外，網絡裝置及伺服器系統記錄（例如防火牆記錄、網頁接達記錄、系統事項記錄）亦須定期覆檢，以偵測異常的情況，包括攻擊／入侵系統軟件，或針對終端用戶的網上應用程式。應就所有在未獲授權的情況下接達資訊系統的事件作出匯報，並稽查（宜每天稽查）違反保安事件報告。此外，對系統軟件亦應制訂嚴格的更改控制程序，以偵測未獲授權擅用的情況。

大部分操作系統均設有記錄檔案。定期檢查這些記錄檔案往往是偵測未獲授權擅用系統的第一道防線。以下情況可為偵測在未獲授權的情況下接達系統的事件提供線索：

- 大部分用戶一般會在每天差不多相同的時間登入及退出。在「正常」時間以外登入的帳戶可能被入侵者擅用。
- 會計記錄（如有）亦可用作判斷系統的使用模式；不正常的會計記錄可能表示系統被人擅用。
- 應檢查系統記錄設備，以找出從系統軟件發出的任何不正常誤差訊息。舉例來說，在短時間內錄得大量登入失敗記錄可能表示有人嘗試猜測密碼。
- 以操作系統指令列出執行中的各個程式，有助偵測未獲授權用戶使用的操作程式，並可偵測入侵者所啓動未獲授權使用的程式。

利用標準操作系統軟件結合多個不相關的程式，亦可製作其他監察工具。舉例來說，可使用此方法建立和以離機形式儲存檔案擁有人及權限設定清單。日後，這些清單可定期重新組合與主清單作比較。如有差異，則顯示系統可能已在未獲授權的情況下被竄改。

主機入侵偵測系統或入侵防禦系統可作多方面的分析，以判斷是否有濫用(網絡內部的惡意或濫用活動)或入侵(外來的違反保安事件)的情況。主機入侵偵測系統／入侵防禦系統會參考多類記錄檔案(核心、系統、伺服器、網絡、防火牆等)，與存有已知攻擊的共用識別碼的內部數據庫作比較。入侵偵測系統／入侵防禦系統還可驗證重要檔案及可執行檔案的數據完整性。入侵偵測系統／入侵防禦系統可檢查由用戶預先選定的保密檔案數據庫，就每個檔案以訊息摘要實用程式(例如 sha2sum)制訂其校驗和。然後，入侵偵測系統／入侵防禦系統以純文本檔案格式儲存校驗和，並定期將檔案校驗和與文本檔案的數值作比較。如有任何檔案校驗和不相符，入侵偵測系統／入侵防禦系統便會以電郵、電話、短訊或傳呼機通知管理員。

外聘供應商及公共軟件下載網站亦有提供其他工具。決策局／部門應根據其目標及具體要求選擇合適的保安監察和檢測工具。

決策局／部門須在技術可行的情況下，在所有伺服器、工作站和流動裝置中部署端點偵測與回應解決方案，以即時識別異常或可疑活動，並就潛在保安事故發出預警。端點偵測與回應解決方案有助即時偵測和應對威脅，減少保安事故的潛在影響。此外，端點偵測與回應解決方案針對網絡內的個別裝置(例如端點)，可供深入了解所採取的每項操作，同時監察流量以識別可疑模式和異常情況。決策局／部門亦可考慮網絡偵測與回應解決方案，該解決方案可以持續監察網絡流量，以發現保安事故的跡象。

(d) 持續改善和適應

決策局／部門應根據保安事故的經驗教訓和風險形勢變化，定期評估和更新其威脅偵測和監察程序。決策局／部門亦應利用漏洞管理程序中常用的漏洞識別活動，包括漏洞掃描、滲透測試和模擬攻擊，以驗證決策局／部門檢測和應對真實攻擊的能力，並將其納入為持續改進和適應策略的一部分。有關漏洞識別活動的更多資料，請參閱第 14.6 節。

如欲獲取更多有關資訊科技威脅管理的資料，可參考以下文件：

- **資訊科技保安威脅管理實務指引**

  可在政府資訊科技情報網下載
  (https://itginfo.ccgo.hksarg/content/itsecure/techcorner/practices.shtml)

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

(a) 一般網絡保護

對於網絡式或分布式應用系統，多重系統的保安與互連網絡的保安同樣重要，尤其有關應用系統使用公眾人士可接達的寬廣區域網絡。

在與外部網絡連接時，必須權衡有關利弊風險，並宜施加限制，只容許沒有儲存敏感資料的主機與外部網絡連接，並隔離主要電腦。

以下是一些網絡保護指引：

- 網絡應盡量簡單（即把「安全」網絡與其他網絡的網絡界面點減至最低）。
- 只容許獲授權的通訊進入「安全」網絡。
- 利用多重機制鑑定用戶身分（例如密碼系統加上預先註冊的互聯網規約地址及／或預先註冊的媒體接達控制地址）。
- 在網絡傳遞數據前，使用經證明有效的加密算法為數據加密。

須備存最新的系統或網絡資料，特別是網絡圖、內部網址和配置，顯示最新的網絡環境，以有效推行保安控制措施。這些資料須適當地分類及穩妥地儲存。如把這些資料外泄予未獲授權各方，可能會導致違反保安事項，所以須按照「有需要知道」原則只向用戶或有關各方披露，並備存適當記錄。決策局／部門須確保未經事先批准不會公開這些資料。

(b) 網絡保安控制措施

除非有運作上的需要並得到部門資訊科技保安主任的批准，否則用戶不得把未獲授權的電腦資源（包括私人擁有及外聘服務供應商擁有的電腦資源）連接至政府內部網絡。即使得到部門資訊科技保安主任的批准，決策局／部門亦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。

如有需要連接寬廣區域網絡，可考慮限制所有局部網絡的接達都要通過指定的通訊閘，即所有進入或來自局部網絡的接達均必須經過指定的通訊閘，這個通訊閘可作為局部網絡與外界之間的防火牆。這個系統必須受到嚴格控制和以密碼作保護，其配置應只容許來自外部用戶的合法網絡通訊接達受其保護的網絡。防火牆受到損害可能導致受其保護的網絡也受到損害。

此外，應考慮設立雙重防火牆，以進一步保護資訊系統。此結構使用兩道防火牆，包括外部及內部防火牆。外部防火牆保護非軍事區不受來自互聯網的入侵，而內部防火牆則進一步保護內部網絡。就此設計而言，即使外部用戶損害非軍事區的伺服器，內部防火牆仍可保護內部網絡的伺服器／工作站。

除防火牆系統外，還應考慮為經網絡傳送的密碼引入加密算法，並推行安全程序識別系統，以便分布在網絡的應用系統可識別對話的「對象」。

為偵測網絡異常活動，決策局／部門須推行入侵偵測策略，在網絡關鍵節點安裝網絡入侵偵測系統或網絡入侵防禦系統。網絡入侵偵測系統監察網絡線路的小包，旨在揭發意圖入侵系統（或發動拒絕服務攻擊）的黑客／電腦破壞者。一旦入侵偵測系統發現系統遭到攻擊，便會向資訊科技管理員發出警報，從而將系統停機時間及對服務的潛在影響減至最低。入侵防禦系統的功能與入侵偵測系統相若，然而該系統會採取額外措施主動阻止攻擊來源或將攻擊的影響減至最低。入侵偵測系統及入侵防禦系統的配置須調校識別碼及識別方式，以減少虛假警報。

決策局／部門須全面承擔保護數據、資訊系統及網絡的責任。決策局／部門須確保資訊／通訊系統已妥善配置及穩妥管理，包括關掉所有無須使用的服務和適當地設定保安配置。配置須定期覆檢，並在有需要時更新。決策局／部門亦應購置保安軟件（如防火牆、惡意軟件偵測及修復軟件等），以便推行企業管理。企業管理是指有關軟件運用中央管理控制台管理機構內所有保安軟件，通常具備遠程更新、政策實施、狀態查詢、報告編製、保安功能等特點，可節省政策／識別碼／更新所需的調配時間、實施統一標準的機構保安政策、協助進行遵行要求評估，以及減輕局部區域網絡／系統管理員及資訊科技保安管理員的工作負擔。

決策局／部門須將其網絡劃分為分隔的網域。可以按可信任的程度選擇網域（例如公眾可接達的網域、桌面網域、伺服器網域），並可採用實體或邏輯（例如使用虛擬私有網絡）的方式分隔網域。此外，跨網絡連接應僅按需要而提供。

每個網域的邊界須清晰界定。網域之間可容許互相接達，但應使用通訊閘（例如防火牆和過濾路由器）在網域邊界作出控制。把網絡分隔為網域和

容許通過通訊閘接達的準則，應根據對各網域保安要求的評估制訂。有關評估應根據第 11 節－接達控制內有關接達要求及所處理資料的價值和保密類別進行，亦應考慮採用合適通訊閘技術所需的相對成本及對效能的影響。

流動裝置通常具備網絡連接功能。這些裝置如在沒有適當保護措施的情況下連接政府內部網絡，可能導致違反保安事項，包括外泄保密資料，以及在政府內部網絡傳播惡意軟件，或者成為被惡意軟件控制的攻擊裝置。除非得到部門資訊科技保安主任的批准，否則用戶不得將其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。

在技術可行的情況下，資訊系統的管理控制台和管理介面不得直接從互聯網接達。

在通過無線通訊接達保密資料時，應考慮把所有無線接達視為不可信任的連接。因此，使用無線通訊接達內部系統須通過指定通訊閘（例如虛擬私有網絡通訊閘）進行，並應推行適當的認證、加密、用戶層網絡接達控制和備存記錄。

(c) 與其他網絡的通訊

與另一個網絡的連接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／部門須在建立網絡連接前，與另一方的決策局／部門或外部機構就保安要求進行溝通。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。有關保安要求應依據的原則是，如雙方的保安保護級別不同，則雙方均採用較嚴格的保安保護。

一些決策局／部門所實施的保安要求可能較其他決策局／部門的嚴格（例如客戶端程式配置／設置、網絡傳遞要求、用戶身分識別及鑑定、對話管理、事項完整性等方面）。有時會出現兩個決策局／部門的保安要求不同，但需要互相通訊的情況。如部門間通訊的保安要求存在差異，應遵守以下原則：

- 資訊系統提供者的保安要求較其他決策局／部門用戶的保安要求嚴格：
  在此情況下，應以資訊系統提供者的保安要求為準，因為作為資訊系統提供者的決策局／部門有合理的業務上考慮因素提高其保安要求，其他決策局／部門的用戶需要遵從。

- 資訊系統提供者的保安要求較其他決策局／部門用戶的保安要求寬鬆：
  在此情況下，資訊系統提供者應進行保安風險評估，以釐定是否需要調整其保安要求。如評估結果顯示沒有需要更改其保安要求，作為資訊系統提供者的決策局／部門應與保安要求較高的其他決策局／部門用戶協調，為其設置其他接達渠道，或要求這些用戶容納較寬鬆的保安要求。

  如評估結果顯示作為資訊系統提供者的決策局／部門需要加強其保安要求，便應相應推行額外的保安控制措施。如在加強保安要求後，仍有其他決策局／部門用戶採用比其更高的保安要求，作為資訊系統提供者的決策局／部門應與這些用戶協調，為其設置其他接達渠道，或者要求這些用戶容納較寬鬆的保安要求。

當決策局／部門推行資訊系統供其他決策局／部門的用戶使用時，該決策局／部門應把有關接入要求視作來自不可信任的網絡，並根據應用系統的特定要求推行足夠的保安控制措施，同時推行額外措施確保用戶的行為恰當（例如自動對話超時），而不應假設其他決策局／部門的用戶會遵從其資訊科技保安政策行事。

(d) 無線通訊

無線通訊是指在沒有連接電線、導線或任何其他形式的電導體的情況下在一段距離上傳遞資料。無線電話、流動電話、全球定位系統裝置及無線電腦等裝置，均使用無線通訊。無線局部區域網絡是政府常用的無線通訊技術，是一種利用高頻無線電波（而非經線路）在裝置之間進行通訊的局部區域網絡。無線局部區域網絡是一種靈活的數據通訊系統，用以作為有線局部區域網絡的替代或延伸。無線資訊通訊使人們可以更容易及自由地互動。隨着科技日新及價格／性能提高，辦公室或公共場所愈來愈廣泛應用無線連接。

無線局部區域網絡是以電機電子工程師學會訂定的 IEEE 802.11 標準為基準。該標準已演化為 802.11a、802.11b、802.11g 及 802.11n 等不同標準，以支援不同頻譜及頻寬。

IEEE 標準 802.1X 及 802.11i 是互相關連的。802.1X 標準是以埠為基礎的網絡接達控制規約，為 IEEE 網絡（包括以太網及無線網絡）提供保安架構。802.11i 標準則針對無線保安功能而制訂，與 IEEE 802.1X 共同運作。

使用無線通訊接駁政府內部網絡時，須採取充分認證及傳遞加密措施，並輔以適當的保安管理程序及作業模式。

(e) 無線局部區域網絡面對的威脅及保安漏洞

無線信號的特點是有關信號普遍在無線局部區域網絡的覆蓋範圍內通過空氣傳輸，並可穿越建築物的牆壁及窗戶。因此，除非已採取保安措施保護無線傳遞不被「竊聽」，否則會帶來任何人也可截取及閱讀這些信號的潛在保安風險。事實上，無線局部區域網絡面對的風險，相等於運作有線網絡的風險，加上無線規約的漏洞所引致的新風險。以下是與無線局部區域網絡相關的一些風險：

- 懷有惡意的人士可通過無線連接，並有可能避開防火牆，在未獲授權的情況下接達政府內部網絡及發動攻擊。
- 電腦惡意軟件可破壞無線裝置內的數據，繼而影響有線網絡的運作。
- 懷有惡意的人士可利用未獲授權設備（例如客戶裝置及無線接駁點）暗中接達或竄改資料。
- 未經加密（或採用較弱的加密技術加密）的保密資料在無線裝置之間傳遞時或會被截取及外泄。
- 拒絕服務攻擊可能會針對無線連接或裝置發動。
- 可能有虛假的無線接駁點被建立，以獲取無線局部區域網絡內傳送的資料。

無線局部區域網絡技術日新月異。決策局／部門須定期覆檢其 Wi-Fi 基礎設施，以評估在 Wi-Fi 通訊標準和規約所發現之保安漏洞的影響。政府應考慮採用較強的無線保安規約如「無線保護接達 3」，以保護無線局部區域網絡。由於日後可能在這些規約發現新的漏洞，故不能只依賴這些無線保安規約作為保護數據機密性及完整性的唯一措施。決策局／部門如需通過無線局部區域網絡傳輸保密數據，應在無線局部區域網絡之上設置虛擬私有網絡。

(f) 保護無線局部區域網絡的保安控制措施

決策局／部門應注意，除使用技術保安措施保護其無線局部區域網絡外，還須採取適當的管理控制措施以有效保護其無線局部區域網絡。以下是一些管理及技術保安控制措施，以供參考：

<u>管理控制措施</u>

- 就無線局部區域網絡的使用及可經無線局部區域網絡傳遞的資料類別制訂無線保安政策。
- 制訂及妥善保存無線局部區域網絡的覆蓋圖，涵蓋相關無線接駁點的位置及服務設定識別碼資料，避免無線信號的覆蓋範圍過大。

- 確保硬件及軟件得到妥善修補及更新。
- 定期搜尋虛假或未獲授權的無線接駁點。
- 定期進行資訊科技保安風險評估及審計，以找出保安漏洞。
- 妥善保存所有配置無線界面的裝置的記錄。某裝置一旦被報失，應考慮更改密碼匙及服務設定識別碼。
- 推行嚴格的實體保安控制措施及鑑定用戶身分，以彌補無線裝置實體保安的不足。
- 在遠離門窗的位置安裝無線接駁點，以防止網絡在可公開進入的地方被竊聽。

技術控制措施

- 在安裝時更改網絡預設名稱。服務設定識別碼不應包含任何決策局／部門的名稱、系統名稱或產品名稱／型號。
- 更改產品預設的無線接駁點配置設定。為方便設置，有關預設配置設定在大部分情況下視為不安全。
- 關閉無線接駁點上所有不安全及未使用的管理規約，並以最小權限配置所需的管理規約。
- 確保所有無線接駁點均有嚴謹而獨立的管理密碼，並定期更改密碼。
- 開啓及配置保安設定，包括服務設定識別碼、密碼匙及簡單網絡管理規約的社群字串。
- 關閉服務設定識別碼廣播功能，以免無線接駁點廣播服務設定識別碼，只有配置與無線接駁點服務設定識別碼相符的獲授權用戶才可與網絡連接。
- 關閉動態主機配置協議伺服器，並向所有無線用戶指派固定的互聯網規約地址，從而將未獲授權用戶取得有效互聯網規約地址的機會減至最低。
- 配置無線接駁點時使用媒體接達控制地址過濾功能，使只有具有特定媒體接達控制地址的客戶才可接達網絡，或只容許接達一系列設定的媒體接達控制地址。
- 切勿直接連接無線局部區域網絡和有線網絡。在無線接駁點與決策局／部門網絡之間安裝防火牆或路由器，並使用接達控制名單，以過濾連接。
- 啓動基本參數，例如靜止暫停。
- 啓動記錄功能，並在可行的情況下把所有記錄轉移至遠程記錄伺服器。有關記錄應定期檢查。
- 安裝無線網絡入侵偵測系統或無線網絡入侵防禦系統，以監察無線局部區域網絡。
- 在無線局部區域網絡之上設置虛擬私有網絡，以連接部門網絡。

- 對於 Wi-Fi 防禦功能有限的流動裝置，應使用客戶端數碼證書，使只有獲授權的裝置才可接達部門網絡或資源。
- 把無線接駁點的覆蓋區域分段，以平衡網絡負荷及減低受到拒絕服務攻擊的可能性／影響。
- 棄置無線組件時，刪除有關裝置所載的所有敏感資料，例如系統配置、共享密碼匙、數碼證書和密碼。
- 關掉無線接駁點的通用即插即用功能，以防止惡意軟件通過連接的裝置繞過防火牆。

終端用戶控制措施

- 在無線客戶端（例如流動裝置）安裝防火牆。
- 關掉無線客戶端的共用或網絡共享功能。
- 已連接第三方無線局部區域網絡的無線客戶端不得同時連接部門網絡。
- 通過虛擬私有網絡連接部門網絡資源。
- 嚴格控制無線界面裝置（例如膝上電腦的通用串列匯流排權標），因為接達憑證（例如服務設定識別碼及／或密碼匙）通常儲存在卡內。
- 只在用戶需要時才開啓無線連接，不需要時則關閉。
- 遵從第 14.2 節—防範惡意軟件和《流動保安實務指引》第 4 節—流動裝置保安的指引。

(g) 通過無線通訊的傳遞

無線局部區域網絡通常被視為不可信任的網絡，如無適當的保安控制措施，不得用於傳遞保密資料。無線局部區域網絡與內部可信賴網絡之間的網絡通訊必須經過加密及認證。採用虛擬私有網絡是達致這種端對端保安的可行方法。

下表簡列各類資料使用無線通訊進行傳遞的適用範圍。

資料類別	使用無線通訊傳遞資料的適用範圍
機密以上	不可使用
機密	可使用，但必須得到決策局局長／部門首長的批准並以指定裝置傳遞資料，以及有足夠的認證和傳遞資料加密保安控制，並達到機密資料必須達到的加密水平。 應使用虛擬私有網絡，以加強無線局部區域網絡連接的認證和加密功能。此外，亦須制訂適當的密碼匙管理及配置政策，以輔助技術方案。 如果無線鍵盤能夠符合在認證及加密方面的行業保安標準，並且經部門資訊科技保安主任確認符合規格，則無需獲得決策局局長／部門首長的批准。
限閱	可使用，但必須有足夠的認證和傳遞資料加密保安控制，並達到限閱資料必須達到的加密水平。 宜使用機密資料必須達到的同一加密水平，並制訂與機密資料相似的適當密碼匙管理及配置政策。
非保密	可使用。在遵從只有獲授權人士才允許接達儲存資料的網絡的原則下，具備足夠及適當的認證和傳遞資料加密措施的無線通訊可視作適合決策局／部門使用。 與機密及限閱資料一樣，亦須制訂適當的密碼匙管理及配置政策，以輔助技術方案。

(h) 互聯網保安

互聯網是由全球電腦網絡互相連接而成的網絡，通常使用傳輸控制規約／聯網規約組進行通訊。連接互聯網使獲取資訊的途徑更為廣泛，從而帶來很多好處，不過，互聯網廣泛存在嚴重的保安問題。

根本問題是互聯網的設計並非十分安全。很多傳輸控制規約／聯網規約服務很容易受到保安威脅，例如被偷聽及仿冒，利用現成的軟件便能夠監察並擷取電子訊息、密碼及檔案傳送。

互聯網服務需要更嚴格的認證和加密機制，而這些機制須做到真正兼容。為落實政府互聯網資源的真確性，政府互聯網網域的資源記錄須受現行的保安控制措施（即域名系統安全擴展）所保護。同樣，就互聯網郵件服務而言，所有發給市民的政府互聯網郵件須受現行的電郵真確性標準保護，包括「發件人策略框架」、「域名密鑰識別郵件」或「網域型郵件驗證、

報告與一致性」規約。此外，所有互聯網服務（包括資訊網站）須推行加密傳遞，例如超文本傳輸安全規約，以加強政府互聯網服務的真確性和內容完整性。互聯網資料查詢或事項處理須鑑定用戶身分，為安全接達起見，可能須採用一次性密碼和進行多重認證，認證資料也須進行審計和備份。

一般來說，互聯網保安涵蓋廣泛的課題，包括識別及認證、防範惡意軟件、軟件特許使用權、遠程接達、撥號接達、實體保安、安裝防火牆，以及與使用互聯網相關的其他範疇。

因此，決策局／部門應通過定期和特設的培訓以提高人員對資訊保安的意識，並着眼於妥善使用互聯網服務。所有人員須知道不當使用互聯網可能會帶來保安風險，這些風險有可能危害政府資訊科技基礎設施和／或對政府聲譽造成負面影響。此外，所有決策局／部門的人員在使用政府提供的互聯網服務時應了解其義務和責任，並嚴格遵從政府所提供互聯網服務的使用條款。

使用個人網絡郵件、公共雲端儲存和網絡版即時通訊服務會帶來重大保安風險，包括在傳輸過程中可能發生未獲授權外泄敏感資料和資料外洩。因此，決策局／部門須定期審慎檢視使用者接達這些服務的必要性。只有當有真正的需要及合理理由，並且獲決策局局長／部門首長或他們明確授權的首長級人員批准時，才可授予接達權限，並在不再有需要時立即撤銷有關權限。決策局／部門應採取技術控制措施，例如網頁內容過濾，以防止未獲授權接達個人網絡郵件、公共雲端儲存和網頁版即時通訊服務。

如果訂閱服務遭受破壞，訂閱線上服務中使用的政府電子郵件地址及政府資訊系統中使用的密碼可能會讓攻擊者獲得接達系統的權限。訂閱中提供的其他資訊也可能外泄，以及被用於網絡釣魚活動和網絡攻擊。雖然訂閱網絡服務可能確實有需要，決策局／部門應不斷提醒用戶相關風險，並提倡採用保安良好作業模式，例如使用嚴謹而獨有的密碼、謹慎處理個人資料、啟用多重認證（若有的話），並對網絡釣魚保持持續警惕，以及在線上服務訂閱使用電子郵件別名。

(i) 通訊閘保護

所有支援互聯網設施的決策局／部門均須保護其資料和資料資源免在未獲授權的情況下被接達或被公眾人士入侵。部門網絡必須通過中央安排的互聯網通訊閘或決策局／部門內部的互聯網通訊閘接達互聯網。通訊閘利用屏蔽路由器、防火牆或其他通訊設施可同時提供保安和認證保護。除特定開啓的功能外，互聯網通訊閘應拒絕其他所有互聯網服務。所有不使用的配置、服務、埠及不必要的通訊，例如不需要的日間服務、傳入或發出的互聯網控制信息規約(ICMP)通訊等，亦應被終止或堵截。不應直接

撥號連接互聯網服務供應商。有關互聯網通訊閘保安的技術指引詳情，請參閱以下文件：

- **《互聯網通訊閘保安實務指引》**
  可在政府資訊科技情報網下載
  (https://itginfo.ccgo.hksarg/content/itsecure/techcorner/practices.shtml)

決策局／部門如決定在獨立電腦（即沒有連接政府或部門網絡的電腦）安裝不經過中央安排的互聯網通訊閘或決策局／部門內部的互聯網通訊閘的寬頻連接，便須在這些獨立電腦推行足夠的保安控制措施，例如防火牆、抗惡意軟件程式、限制用戶權限等，以避免可能發生的違反保安事項和濫用系統事故；同時亦須實施適當的審批及控制機制。除已採取適當的保安保護措施並已得到部門資訊科技保安主任的批准外，任何電腦不得同時以寬頻連接互聯網和接達內部網絡，因為這樣會對政府網絡構成嚴重威脅。

為減低用戶接達釣魚網站或含有惡意內容的網站的風險，決策局／部門須攔截用戶接達任何已知或懷疑有惡意的互聯網規約地址或網站。

(j) 客戶端保護

個人防火牆可有效保護用戶的工作站，以阻截未獲授權的網絡通訊，防禦如網絡蠕蟲入侵或其他形式的惡意軟件攻擊。在用戶工作站安裝的個人防火牆，為工作站與網絡之間提供防火牆服務。個人防火牆在容許網絡通訊進入或輸出用戶工作站前會查詢用戶授權，藉以控制網絡通訊。一些個人防火牆甚至提供應用系統層保護，確保只有獲授權的程序在用戶工作站運行。

局部區域網絡／系統管理員須在有機會直接連接互聯網或第三方網絡等不可信任網絡的電腦安裝個人防火牆。大部分個人防火牆適用於獨立配置或代理配置，上述配置可集中管理及實施個人防火牆政策。

除考慮個人防火牆保護外，應適當配置在用戶工作站運行的互聯網瀏覽器。由於互聯網瀏覽器是連接互聯網的主要界面，互聯網瀏覽器配置不當可能會讓惡意軟件下載至用戶的工作站。決策局／部門在配置互聯網瀏覽器時可參考下列指引：

- 除與可信賴來源通訊外，關閉電子訊息應用系統或瀏覽器的 Java、JavaScript 及 ActiveX 等主動式內容選項。
- 使用最新版本的瀏覽器，並安裝最新的保安修補程式。
- 關閉自動輸入密碼或密碼記憶功能。

- 除與可信任網站通訊外，啓動攔截彈出視窗功能。
- 定期刪除瀏覽器內的快取檔案或臨時檔案，以保障資料私隱。
- 關閉自動安裝外掛程式、附加元件或軟件的功能。

向用戶推行教育及認知培訓亦十分重要，以提醒用戶使用適當配置的互聯網瀏覽器的重要。

15.2 資料傳送

(a) 傳遞保密資料

機密類別以上的保密資料必須經過加密處理，並只限於在已獲數字政策辦公室技術審核和政府保安事務主任批准的獨立有線局部區域網絡內傳遞。獨立的局部區域網絡是指在受監控的單一環境中，沒有與其他網絡（包括其他政府網絡、互聯網和遠程接達）連接的局部區域網絡。

機密／限閱資料在任何通訊網絡上傳遞時應加密，以作保護。機密／限閱資料在不可信任的通訊網絡上傳遞時則必須加密。不可信任的通訊網絡包括：

- 互聯網
- 使用公共電訊線路的網絡（例如租用線路、撥號連線）
- 無線通訊
- 都會以太網

可信任的通訊網絡應具備以下條件：

- 存放地點受到嚴密的實體保護，以免經過網絡傳輸的數據被未獲授權人士接達、竄改或刪除。
- 受到嚴密保護，例如通過鎖上網絡設備及保護局部區域網絡埠，以免被未獲授權人士破壞。
- 制訂清晰明確的資訊科技保安政策，以控制對網絡設備及設定的適當配置和管理。

不符合可信任通訊網絡定義的網絡被視為不可信任的通訊網絡。一般而言，在任何通訊網絡傳遞資料都有保安風險，因為惡意攻擊者可擷取保密資料，甚至利用通訊網絡的保安漏洞入侵政府網絡。決策局／部門應進行保安風險評估，以確定正在使用的通訊網絡是否可信任，並識別相關風險。決策局／部門應考慮在數據、應用系統或網絡層面進行加密，將在未獲授權的情況下被接達的風險減至最低。

(b) 電子訊息保安

電子訊息（例如電郵、即時通訊）是供內部及外部通訊的一項主要應用科技。政府內部網絡有多種電郵產品供內部用戶使用。用戶須提出正式申請才能使用電郵帳戶。互聯網的電郵與內部網絡的電郵一樣，應支援認證、加密及數碼簽署等功能。載有保密資料的電子訊息在傳遞或儲存時必須加密。

除非因業務需要而無可避免，否則應限制使用公共電郵。如傳遞載有保密資料的電子郵件，必須通過已獲政府保安事務主任批准的資訊系統傳遞。在內部通訊方面，「政府內部機密郵件系統」、「機密信息應用系統」、「機密電郵流動服務」和「中央管理通訊系統」中已獲批准的子系統是政府的指定電郵系統，以便在政府網絡內交換機密類別的電郵訊息和文件。在互聯網交換電郵，不論是否已簽署或加密，都不能假設已達到與「政府內部機密郵件系統」或「中央管理通訊系統」相同的保安程度，因為互聯網電子訊息服務未必符合有關處理機密資料的政府保安要求。有關「政府內部機密郵件系統」和「中央管理通訊系統」的配置和操作程序，請分別參閱載於政府內聯網數碼政府合署網站：http://cms.host.ccgo.hksarg/ 和 https://itginfo.ccgo.hksarg/content/cmmp 的相關文件。

(c) 電郵伺服器和客戶端的保安

在連接互聯網前應適當地配置電郵伺服器及客戶軟件。以標準的簡單郵遞傳送規約傳送的電郵不會進行完整性檢查，互聯網電郵地址可輕易被仿冒，以互聯網傳遞電郵一般沒有保障。如技術上和運作上可行，電郵的標題應避免透露內部系統或配置的具體資料，以防止把系統資料外泄予外部機構。

決策局／部門可考慮就接達電郵的任何活動進行審計追蹤，以記錄獲授權及未獲授權用戶嘗試閱讀或更新電郵的每項活動。須訂立有系統的程序，以記錄、保存及刪除電子訊息及備存清晰的記錄。應使用警示報表或警報報告保安事故。此外，獲授權的管理員必須妥善備存和保護用戶電子郵件通訊錄，以免在未獲授權的情況下被接達或竄改。

為加強政府電郵系統的保安，用戶須為其工作站及電郵帳戶設置密碼等認證功能，以免在未獲授權的情況下被接達和使用。

不應讓電郵客戶端自動處理附件，因為附件可能含有惡意手稿程式或惡意軟件。有關詳情請參閱第 15.1(j)節—客戶端保護。

局部區域網絡／系統管理員應為使用政府電郵系統的用戶安排自動更新惡意軟件定義。用戶應確保每當使用系統接達任何檔案或資料時，均已開啓其工作站內的抗惡意軟件自動防護功能。有關詳情請參閱第 14.2 節—防範惡意軟件。

用戶應保護及定期更改其密碼。用戶不應打開或轉寄任何來歷不明或可疑來源的電郵。如用戶懷疑或發現電郵附有任何惡意軟件或可疑內容，應立即向管理人員及局部區域網絡／系統管理員報告有關事故，並遵從相關事故應變計劃。如有疑問，用戶也應透過其他途徑（例如透過電話）驗證電子郵件寄件者的身份。

此外，除非能夠確保外部電郵系統安全，否則用戶不應設定把公務電郵自動轉寄至該系統，因為一些包含保密內容的電郵也可能會一併自動轉寄出去。如在沒有加密的情況下自動轉寄這些包含保密內容的電郵，可能違反有關傳遞保密資料的政府保安要求。此外，不受政府直接控制的電郵系統，會為所儲存的資料帶來額外保安風險。

有關政府電郵系統的電郵管理及電郵保安詳情，請參閱以下文件：

- **《使用電子郵件實務指引》**
  可在政府資訊科技情報網下載
  (https://itginfo.ccgo.hksarg/content/imx/email_practice_guide.asp)

(d) 與外部機構通訊

與外部機構（如非政府機構、政府相關組織、外判人員或外聘服務供應商）的網絡通訊應視為不可信任。各決策局／部門在通訊網絡與外部機構連接或交換資料時，應遵從相關的資訊科技保安政策，並根據應用系統的特定要求推行足夠的保安控制措施。

向外部機構提供資料時必須遵守「有需要知道」原則。決策局／部門須確保有關保護保密資料的安排盡量符合政府內部所採用的標準。

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。與外部機構達成的資料傳送協議應至少包括以下各點：

- 不可向第三方披露保密資料或視乎情況向政府作出彌償的責任。
- 保護保密資料防止在未獲授權的情況下被接達的措施，例如數據加密和接達控制。

- 發生資訊保安事故（例如數據外泄）時的責任和義務。
- 記錄或閱讀保密資料的技術標準。

應制訂及備存相關的政策、程序及標準，以保護在傳輸過程中的資料及實體媒體。這些文件應在資料傳送協議內提及。

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

(a) 設計層面的保安

設計層面保安的概念對識別應用系統的潛在風險，並在發展／購置系統前進行適當補救工作尤為重要。完善的應用系統設計不僅針對用戶的問題提出可行的解決方案，更為用戶提供安全的操作環境。在系統發展初期以至各個階段，均應採取措施加強保安及保障私隱，並善用操作系統所提供的保安設施。此外，應用系統本身應視乎系統的保安漏洞和關鍵性，以及所處理數據的敏感度，內置額外的保安措施。

保安左移方法在整個系統發展生命周期的早期和整個過程中整合了保安考慮因素，以確保適當地識別和納入必要的保安要求。決策局／部門應考慮實施保安左移方法，包括採用安全編碼作業模式，以及在系統設計階段對其資訊系統進行保安審查。

決策局／部門應在新資訊系統或現有資訊系統改善計劃的要求中界定有關資訊科技保安的要求。如能清晰界定保安要求，並於早期階段處理已識別的風險，預計可大大減少重做系統所需的工作。決策局／部門應在資訊系統的設計階段進行保安覆檢作為檢查點，以確保已識別所需的保安要求，並已將之適當地納入於系統設計階段或其他階段。

有關覆檢應根據業務需要、法例和規管要求（例如《個人資料（私隱）條例》），以及政府的保安要求評核有關保安要求，並參照應用系統設計和發展階段的保安考慮，識別可能出現的遵行問題及保安風險，藉此覆檢系統設計。在覆檢後，應適當地記錄及在設計或其他階段處理所識別的風險及建議。覆檢時應在發展小組中加入一項職務，以評估保安風險、提出潛在的保安問題，以及進行系統設計及程式編碼的保安覆檢。為確保所需的保安措施和控制措施均已在系統內妥善推行，投產前的保安風險評估應在正式推出之前核實已完成保安審查的跟進行動和程式編碼的覆檢。

如欲獲取更多有關設計層面的保安的更多信息，可參考以下文件：

- **《設計層面的保安實務指引》**
  可在政府資訊科技情報網下載
  (https://itginfo.ccgo.hksarg/content/itsecure/techcorner/practices.shtml)

(b) 系統規格及設計控制

在系統規格及設計階段，應進行以下檢查：

i) 確保所設計的系統符合可接受的會計政策、會計及應用系統控制措施，以執行足夠的認證、授權及問責，以及符合所有適用的立法措施。

ii) 確保已建立威脅模型，並在所有設計及功能規格中加入可減低威脅的措施。另外，可通過分析應用系統中較高風險的進入點和數據，建立最基本的威脅模型。

iii) 與用戶共同覆檢系統設計，檢查在維持資料的完整性方面是否存在任何漏洞。應鼓勵用戶就所發現的任何漏洞建議修正措施。

iv) 與用戶共同評估數據處理能力損失時對用戶的影響。評估後應制訂應急計劃。有關制訂應急計劃的詳情，請參閱第19.1(a)節—應急管理。

v) 與資料擁有人共同評估數據的敏感度，須探討的資料包括：
- 達到的保安水平
- 數據來源
- 容許用戶部門各級人員接達的數據字段
- 容許用戶部門各級人員處理電腦檔案內數據的方式
- 達到的審計功能程度
- 備存的數據量及在資訊系統備存有關數據的目的
- 需備份的數據檔案
- 備存的備份份數
- 備份及存檔的頻率

vi) 如系統有潛在私隱影響，進行私隱影響評估以審查用於保障個人資料的計劃其保護措施是否足夠、有效和實際。個人資料私隱專員已發出關於私隱影響評估的資料單張，該單張可於個人資料私隱專員公署網站下載。

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

用戶要求可匯集成為某種形式的保安聲明。用戶的保安聲明繼而應作為系統功能規格的一部分，並在設計系統時反映出來。

敏捷開發方法日漸獲得軟件業界採納。然而，鑑於敏捷開發方法的特點，敏捷方法與傳統方法在保安保證方面明顯存在不協調。現提供一些建議，以調整保安保證措施配合敏捷軟件開發工作：

(i) 記錄保安架構。
(ii) 在發展小組中加入一項職務，以評估保安風險、提出潛在的保安問題，以及進行系統設計及程式編碼的保安覆檢。
(iii) 記錄與保安相關的程式編製活動。
(iv) 如有需要，進行程式碼覆檢。

(c) 應用系統設計及發展的保安考慮事項

下文列舉了一些在設計及發展應用系統時應遵守的保安原則：

- ***保安架構、設計和結構***。確保在設計基本系統架構時已顧及保安問題。應覆檢針對潛在保安問題的詳細設計，並設計和制訂減低所有潛在威脅的措施。有關保障個人資料方面，決策局／部門須進一步參考《個人資料（私隱）條例》中保障資料原則[6]所列明的強制要求。
- ***最小權限***。確保應用系統的設計只授予執行工作所需的最小系統權限。
- ***職務分工***。確保遵從職務分工的做法，將關鍵功能分為多個步驟並分別交由不同人員處理，以防止關鍵程序被一人破壞。
- ***有需要知道***。系統文件和應用系統清單的接達權限須設定在最低限度，並須獲得應用系統擁有人授權。
- ***保護最弱鏈路***。應用系統和操作系統的保安取決於最弱鏈路的保安，因此，應確保各方面均已設置足夠的保安保護，以預防攻擊者通過因編碼方面的疏忽而產生的漏洞入侵系統。
- ***適當認證及授權***。確保推行妥善的接達控制措施，以執行用戶的權限及接達權限。對於公共網上服務，應考慮使用全自動區分電腦和人類的公開圖靈測試，以控制提交的輸入資料。
- ***適當對話管理***。確保應用系統有適當及安全的對話管理，以保護對話不會在未獲授權的情況下被接達、竄改或劫持。保護措施包括產生無法預測的對話識別項目、確保通訊渠道安全、限制對話有效期、把敏感對話內容加密、採取適當的登出功能和暫停閒置對話，以及過濾無效對話。
- ***輸入驗證***。確保應用系統對來自可信任範圍以外的所有輸入均施加嚴謹的驗證，使任何預期以外的輸入均獲得妥善處理，不會成為攻擊應用系統的途徑。預期以外的輸入包括過長的輸入、不正確的數

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

據種類、預期以外的負值或日期範圍，以及預期以外的字符，例如那些被應用系統用作分隔所輸入字元串的字符等。

- ***適當誤差處理***。確保應用系統會提供有意義及對用戶或支援人員有幫助的誤差訊息，但同時亦須確保這些誤差訊息不會披露保密資料。確保有關誤差已被偵測、報告和妥善處理。
- ***故障處理***。確保應用系統設有保安機制，在應用系統發生故障時拒絕進一步執行編碼。
- ***適當配置管理***。確保應用系統和系統均具備適當及安全的配置，包括關閉所有不使用的服務及設定適當的保安配置。
- ***移除不需要的項目***。確保關閉不使用或較不常用的服務、規約、埠及功能，以減少受到攻擊的機會。此外，在生產伺服器內不需要的內容，如顯示於伺服器橫幅的平台資料、說明資料庫及聯機軟件手冊，以及預設或示例檔案等亦應移除，以避免系統資料不必要的外泄。
- ***資料機密性***。在儲存或傳遞保密資料時，確保資料已經加密。在展示、列印或使用保密資料作測試時，應遮蔽該等資料（如適用）。
- ***資料真確性及完整性***。在交換資料過程中，確保資料屬真確及完整。
- ***安全使用***。確保備妥使用指引，載列如何安全地使用應用系統的各項功能。
- ***記錄管理***。備存重要事件（如關鍵操作或敏感資料的處理）的審計追蹤，以作恆常管制或調查之用。應禁止竄改或更改任何審計追蹤。對於特殊情況，應提請管理層注意。

(d) 制訂程式編製標準

執行程式編製控制至少須達到以下目的：

- 確保程式符合程式規格，除應有功能外，程式內沒有任何未予記錄的功能。
- 確保程式符合必要的程式編製標準。
- 防止及偵測欺詐行為。

為方便發展及維修程式，應制訂程式編製標準。制訂有關標準後，下一項重要工作是確保嚴格遵守所制訂的標準。

(e) 分工

對風險較大及較敏感的系統來說，可能需要把處理極敏感資料的程式分為不同單元的模組和分段，並指派多位程式編製員處理。這樣做可達到兩個主要目的：

- 把程式編製職責分開可以令不誠實的程式編製員較難在系統內製造程式故障，因為該程式編製員無法控制程式的其他單元，必須與其他程式編製員合謀才能得逞。
- 把程式分為較小單元亦可提高偵測程式編製詐騙的機會，對程式單元可進行更詳盡的分析和覆檢。

(f) 程式／系統測試

首先，用戶部門應進行用戶驗收測試，並負責制訂測試計劃和測試數據。用戶部門亦應詳細檢查所有輸出，以確保產生預期的結果。如發現誤差訊息，用戶部門應有能力明白有關訊息和採取相應行動作出修正。

測試計劃應涵蓋下列個案：

- 有效及無效的數據及個案組合。
- 違反編輯及控制規則的數據及個案。
- 算術運算的捨入、截尾及溢出測試個案。
- 預期以外的輸入測試個案，例如過長的輸入、不正確的數據種類、預期以外的負值或日期範圍，以及預期以外的字符，例如那些被應用系統用作分隔所輸入字元串的字符等。

除用戶驗收測試外，還有其他測試有助驗證系統功能的正確性。單元測試用於測試獨立程式或模組，以確保程式的內部操作符合規格。界面測試是一項硬件或軟件測試，用於評估傳遞資料的兩個或以上組件之間的連接情況。系統測試包括一系列測試，旨在確保改寫後的程式可正確地與其他系統組件互相配合。壓力測試或負荷測試用於測定指定系統的穩定性，方法是為系統加載超過其正常運行容量的負荷量，以觀察其結果。迴歸測試是一項重新進行某測試方案或測試計劃一部分的程序，以確保作出的變更或校正不會導致新的誤差。在測試期間，每項測試均應予記錄，列明記錄的內容及測試目的。事項檔案的記錄還應包括事項完成後預期的結果，以供系統測試之用。每次更改系統後，使用相同的檔案重新進行測試，然後比較前後輸出的內容。任何修改只在沒有發現任何分歧的情況下方可驗收。

由數字政策辦公室揀選的支援大規模面向公眾數碼服務的資訊系統，亦須接受政府資訊科技總監辦公室通告第 5/2023 號「加強大規模面向公眾服務的資訊科技系統投入運作前的準備工作」所規定的額外測試。

16.2 發展及支援程序的保安

(a) 安全的發展環境

決策局／部門應評估個別應用系統發展工作涉及的風險，並為特定的應用系統發展工作建立安全的發展環境。決策局／部門應考慮：

- 需予處理、儲存及傳遞的數據的敏感度。
- 規例或政策中可應用的內部或外部要求。
- 已制訂的應用系統發展保安控制措施。
- 工作人員值得信任的程度。
- 應用系統發展的外判程度。
- 不同發展環境之間的分隔需要。
- 發展環境的接達控制。
- 程式碼與發展環境的變更監察。
- 於場外地方安全儲存備份。
- 數據移出／移入發展環境的控制。

當決定個別發展環境的保護程度後，決策局／部門應記錄安全發展程序的相關過程，並提供予有需要的人員。

(b) 應用系統的文件、程式源碼和清單的控制

須妥善備存及根據既定程序妥善管理應用系統的文件、程式源碼（包括無須編譯而可直接執行的手稿程式）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，並採取嚴格的接達控制措施。應用系統的文件、程式源碼及清單的接達權限須維持在最低程度，並須獲應用系統擁有人授權。這些文件應予以適當分類。

程式源碼可以程式源庫的形式集中儲存，並應遵守以下附加指引以控制程式源庫的接達：

- 程式源庫不應存放在生產系統內。
- 所有程式源庫的接達均應於審計記錄內記錄及備存。
- 維護程式源庫時，應遵從嚴格的更改控制程序。

(c) 保安措施的測試及覆檢

決策局／部門應確保任何全新及更新的應用系統在投產前，均已在發展過程中徹底測試及驗證保安措施，包括擬備有關活動、測試輸入及在一系列不同情況下的預期輸出的詳細列表。測試範圍應與系統的性質及關鍵程度相符。

(d) 應用系統的完整性

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。

應建立版本控制機制，記錄程式源碼在應用系統發展過程中的變更，以便在有需要（例如程式復原）時可獲取指定版本。應制訂、記錄及遵從一套版本慣例，例如以 1.0 表示第一個正式版本，1.1 表示第一個正式版本的第一個修改版本。應備存一份變更記錄，闡述自上一個版本以來所作的變更。決策局／部門可考慮採用版本控制工具，以提升版本控制的效益及減少人為失誤。

應按以下考慮因素，隔離發展、系統測試、驗收測試和實際操作等不同環境，以減少意外更改或在未獲授權的情況下接達操作數據及應用系統的風險：

- 除非得到資料擁有人的批准，以及在測試系統推行相等的保安措施，否則不得複製保密資料至測試環境內。
- 應制訂及記錄將數據及應用系統由發展轉移至操作狀態的規則。
- 發展及操作軟件應在不同的系統和網域內運行。
- 操作系統及應用系統的變更在提供正式服務前，應在系統測試及驗收測試的環境內進行測試。
- 用作測試或發展的系統，應限制未獲授權人士及不必要的網絡連接（如互聯網）的接達。此外，連接互聯網的系統應避免選用一些吸引攻擊者注意的系統名稱，例如會令人聯想到發展或測試環境的名稱。
- 在操作系統方面，編譯器之類的系統工具應受到限制，以免在未獲授權的情況下被接達，除非是技術上或運作上有需要接達這些系統工具，在這情況下應實施控制機制。
- 用戶應在測試及操作系統內使用不同的用戶帳戶，應用系統應顯示適當的識別資料以防止出現誤差。

(e) 程式／系統更改控制

所有資料處理設施的變更均應獲得授權及經過妥善測試。所有建議的程式／系統變更或提升項目應經過檢查，以確保不會削弱系統本身或其操作環境的保安。有關人員應接受適當培訓，確保充分認識其保安職責，以及任何系統配置更改後對保安和資訊系統用途的影響。

維持程式／系統更改控制（包括操作系統、數據庫及中間件平台的變更）的目的是：

- 維持程式或系統的完整性。
- 減低修改程式或系統時發生欺詐及出現誤差的風險。

所有與保安控制相關的變更應經過確定、記錄、測試和覆檢，以確保系統能有效抵禦攻擊或破壞。在推行變更前應及時發出通知，以便有足夠時間進行測試及覆檢。應建立要求及審批程式／系統變更的程序。宜建立不同的授權級別（部分為非計劃推行小組人員）以批准相關變更，並應只在得到正式批准後才可作出變更。授權級別應與變更幅度相稱。在任何情況下，所有變更應由變更統籌員協調。變更統籌員應確保變更要求的資料質素和完整性，以及有關要求已得到相關人士的批准。操作及管理程序、業務持續運作計劃和審計追蹤（如適用）亦應予更新，以反映所作出的變更。

應盡量避免更改由供應商提供的軟件套裝。如確實有需要修改軟件套裝，應考慮以下數點：

- 會否損害內建控制及完整性程序。
- 是否需取得供應商同意。
- 可否從供應商的標準程式更新取得所需的變更。
- 如決策局／部門須負責軟件日後的維修保養，會否帶來影響。
- 有關變更是否與其他使用中的軟件兼容。

(f) 程式編目

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。應推行程式編目，以限制生產系統內的保密資料的接達。

程式編目的基本原則是發展或維修小組人員不得將任何程式來源或物件帶入生產程式庫，或從生產程式庫複製任何程式源碼或物件。有關工作應由控制單位人員進行。

如須作出修改，須在控制單位人員看管下把提供正式服務的程式複製至發展程式庫。在完成修改後，工作小組應要求控制單位將程式編入提供正式服務程式庫的目錄。此外，應推行版本控制，並備存至少兩代軟件產品，以便在有需要時可復原程式。

程式或系統強化應在系統啓用前進行。強化後的程式／系統應作為進一步更改的基礎。

為有效維護應用系統，請參閱以下就組織結構、程序及產品各方面詳述系統維修周期的指引文件：

- **《系統維修周期指引》（G22）**
  可在政府資訊科技情報網下載
  (https://itginfo.ccgo.hksarg/content/sm/docs/G22.doc)

16.3 測試數據

(a) 測試數據的保護

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。正式服務的數據不得用作測試，並應避免使用包含個人或保密資料的操作數據庫作測試用途。如不能避免，則須覆檢及記錄有關過程，而且須得到資料擁有人的正式批准，並採取以下控制措施：

- 使用有關資料前，須移除個人資料的部分。
- 使用有關資料前，須刪除保密資料的部分或更改至不能辨認的程度。
- 所有這些資料在測試後應立即妥善刪除。

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

(a) 外判資訊系統的保安

外判服務是指安排由政府以外的機構提供可由決策局／部門自行承辦的服務。在向外聘服務供應商外判資訊系統時，須制訂適當的保安管理程序，以保護資料和減低與外判資訊科技項目／服務相關的保安風險。外聘服務供應商參與政府工作時，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。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。所處理的全部資料須清晰及妥為分類。傳輸到外聘服務供應商的資料宜根據數據的性質和使用案例採用適當的技術進行數據掩蓋。決策局／部門須記錄及推行根據資料類別和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，並與外聘服務供應商訂明保安職責。接達資料的保安權限必須按照「有需要知道」原則授予。

此外，決策局／部門不得允許其外聘服務供應商享有接達在生產環境中的政府資訊系統和數據的權限。如果認為有需要，例如基於系統維護及支援，接達須由獲授權人員嚴密監管，並且在受控的情況下進行，以保護政府資訊資產。嚴禁外聘服務供應商遠程接達生產系統和數據進行日常管理和操作。

把資訊系統外判時，應清楚界定、商定和記錄外聘服務供應商、有關決策局／部門和終端用戶的保安職務和職責。決策局／部門應注意，雖然資訊系統的發展、推行及／或維護工作可以外判，但管理資訊系統的整體責任仍由決策局／部門承擔。

決策局／部門應確保外聘服務供應商擬備妥善的應急計劃及備份程序，同時亦應確保外聘服務供應商根據政府規例、資訊科技保安政策及指引，採取足夠的保安控制措施。外聘服務供應商應向其人員提供有關保安意識的適當培訓，使他們認識資訊保安方面的職責。

資料或系統擁有人應知道服務供應商存放資料的位置，並確保已推行措施，以符合相關的保安要求及本地法例。

(b) 合約內的保安要求

決策局／部門須制訂控制措施，管理有關外聘顧問、承辦商及臨時人員接達資訊系統事宜。與第三方簽訂的合約或其他形式的協議須訂明有關第三方接達或內部控制的保安要求。

除非已推行適當的控制措施，並已簽署訂明接達系統條款的合約，否則決策局／部門不得容許外聘顧問、承辦商、外判人員及臨時人員接達決策局／部門擁有或保管的資料和資訊系統。

在擬定外判服務合約時，決策局／部門須訂明外判的資訊系統的保安要求。這些要求須成為招標程序的基礎，並用以確定投標者有否遵行要求。

外判合約應規定外聘服務供應商的員工簽署不可向外披露資料的協議，以確保外聘服務供應商人員在需接達保密資料時，承擔保密的責任。合約亦應包括一系列服務水平協議。服務水平協議用於界定各項所需的保安控制措施的預定效能、說明可量度的成效，以及就任何已確定的違約事件定出補救及應變要求。服務水平協議應處理責任問題、服務的可靠程度，以及提供服務的回應時間。外聘服務供應商亦須承諾未經政府事先書面同意，不得向任何第三方傳送或披露政府的保密數據。如果收到第三方的披露保密資料特別請求，而該等請求不能直接拒絕，則外聘服務供應商須立即通知並將請求轉交決策局／部門處理。此外，外聘服務供應商須訂立在其所有平台上安全刪除政府資料的程序，並在資料刪除後通過書面確認。此外，合約應包括一套解決問題及事故應變的升級處理程序，並應要求承辦商遵行，以盡量減低對決策局／部門造成的影響。

(c) 損害或損失彌償

所有外聘服務合約應載有適當和有效的彌償損失條款，以保障政府不會因服務中斷或承辦商人員行為不當而蒙受損害或損失。

17.2 外判服務交付管理

(a) 對外判服務的監察及覆檢

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。

決策局／部門應使用合約方式保留審核及監察遵行保安要求的權利，以確保政府資訊系統、設施及資料已推行足夠的控制措施。合約應容許決策局／部門審核服務水平協議所界定的職責，並安排獨立第三方進行審計，以及列舉審計師的法定權利，否則外聘服務供應商須定期提交令人滿意的保安審計／認證報告，以證明所採取的措施達到滿意程度。

為管理外判服務的交付，決策局／部門應就下列方面制訂程序：

- 根據服務協議監察服務表現。
- 定期舉行進度會議，並覆檢外聘服務供應商的服務活動。
- 覆檢保安事務、操作問題和保安審計報告，並跟進所確定的問題。
- 對外判服務的保安活動（例如變更管理、保安漏洞管理及事故監察和應變）保持足夠的整體控制及了解。

(b) 在合約期滿或終止時的控制

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根據政府的保安要求予以清除或銷毀。有關資料須根據其保密級別及相關的政府保安要求予以銷毀。外聘服務供應商人員須在服務終止時，把其管有的所有政府資產交還政府。須制訂及記錄有關終止程序。有關刪除資料及交還資產的詳情，請分別參閱第 10.3(b)節—刪除資料及第 10.1(c)節—交還資產。

17.3 雲端運算保安

(a) 共同責任

雲端運算中的共同責任是指雲端服務供應商（包括公共雲端或私有雲端服務供應商）與雲端客戶之間在保安和管理責任上的分工。這種共同責任模型確保問責，並有助於界定雙方的角色和責任，以確保雲端環境中數據和資源的保安和保護。

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、記錄及了解雙方的共同責任。決策局／部門應仔細檢視雲端服務供應商的服務條款、數據保護政策和所推行的保安措施。

協議簽署後，決策局／部門應確保合約所訂明的共同責任持續獲得遵行。應進行定期審查，以核證雲端服務提供者遵守其在共同責任模型的責任部分。這種方法讓決策局／部門能夠保護其放在雲端的工作負載，從而確保外判資訊系統的整體保安。

雖然資訊系統的開發、推行和／或維護可以外判，但資訊系統的整體問責仍然歸決策局／部門所屬。

如欲獲取更多有關雲端服務中的共同責任的資料，可參考以下文件：

- **雲端運算保安實務指引**
  可在政府科技情報網獲取
  (https://itginfo.ccgo.hksarg/content/itsecure/techcorner/practices.shtml)

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 資訊保安事故的管理和改進

(a) 事故監察及偵測

須推行足夠的事故監察及偵測保安措施，以便在系統正常操作期間保護系統，同時監察潛在的保安事故。所採取措施的程度和範圍取決於系統、系統處理的資料及系統提供的功能的重要性和敏感度。

下列是一些常用的保安事故監察及偵測措施：

- 安裝防火牆設備，並採取認證和接達控制措施，以保護重要系統和數據資源。
- 安裝入侵偵測工具，主動監察、偵測並就系統入侵或黑客活動作出應變。
- 安裝抗惡意程式工具和惡意軟件偵測及修復工具，以偵測及清除惡意軟件，並防止惡意軟件影響系統操作。
- 利用保安掃描工具定期進行保安檢查，以找出現有的保安漏洞，並進行既定保安政策與實際保安安排之間的差距分析。
- 安裝內容過濾工具，以偵測電子郵件或網絡通訊的惡意內容或程式碼。
- 開啓系統及網絡審計記錄功能，以便偵測和追蹤未獲授權的活動。
- 開發程式和手稿程式協助偵測可疑活動、監察系統和數據的完整性，以及分析審計記錄資料。

(b) 保安事故報告

須制訂及記錄一套報告程序，清楚訂明適時向有關各方報告任何可疑活動的步驟和程序。報告程序應列明詳盡的聯絡資料，例如電話號碼（包括辦公時間及非辦公時間的聯絡電話號碼和流動電話號碼）、電郵地址和傳真號碼，以確保負責人員之間能夠有效溝通。

如果懷疑系統出現任何異常的情況，歡迎決策局／部門向政府資訊保安事故應變辦事處尋求意見，以便及早發現政府的資訊科技保安威脅和事故。此舉有利於政府維護整體保安，並構建具復原能力和安全的環境。

為有效執行報告程序，應注意以下幾點：

- 報告程序應載列清楚標明的聯絡點，並包括簡單但明確的步驟以便遵從。
- 應向所有相關人員發布報告程序，以供參閱和參考。
- 確保所有相關人員熟習報告程序，能夠立即報告保安事故。
- 編製保安事故報告表，以規範所收集的資料。
- 考慮報告程序在辦公時間及非辦公時間是否同樣適用，如有需要，應為非辦公時間制訂一套獨立報告程序，並指定相關人員擔任非辦公時間聯絡人。
- 有關事故的資料應只按照「有需要知道」原則披露，並只有資訊保安事故應變小組組長有權或可授權他人把有關保安事故的資料與他人分享。

為改善資訊科技保安事故處理的效率和效益，當意識到資訊保安事故（即合理確定資訊保安事件已對政府資訊系統或數據資產的機密性、完整性或可用性造成損害，或已損害其運作），部門資訊保安事故應變小組須：

(i) 於 60 分鐘內向政府資訊保安事故應變辦事處常設辦公室作電話匯報，並於 48 小時內提交填妥的資訊保安事故初步報告表；

(ii) 如保安事故牽涉關鍵電子政府服務、對保安有重大影響，或會引起傳媒注意，在取得以下資料後盡快與政府資訊保安事故應變辦事處常設辦公室分享：
   - 事故類別及對事故範圍、破壞及影響的評估；
   - 為遏止破壞及修正問題而正在或將會採取的行動；
   - 如引起傳媒注意時的回應口徑；以及
   - 傳媒的查詢及回應建議（如有）。

(iii) 每天向政府資訊保安事故應變辦事處常設辦公室更新受影響的關鍵電子政府服務的修復狀況，直至服務恢復為止。

(iv) 就任何已向香港警務處、個人資料私隱專員公署[7]報告或向傳媒機構發布的保安事故，通知政府資訊保安事故應變辦事處常設辦公室。

在事故解決後的一星期內，應向政府資訊保安事故應變辦事處常設辦公室提交事故事後報告。對於需要較長時間完成調查的個案，有關部門資訊保安事故應變小組須根據以下指引就最新的修復情況及調查進度，向

[7] 若事故涉及個人資料外泄，須盡快透過個人資料私隱專員公署的資料外泄通報表格向個人資料私隱專員公署報告事故:
https://www.pcpd.org.hk/english/enforcement/data_breach_notification/dbn.html

政府資訊保安事故應變辦事處常設辦公室提交中期報告：

- 於第一次報告事故後不遲於十四天內向政府資訊保安事故應變辦事處常設辦公室提交第一份中期報告；以及
- 為了讓管理層知悉事故的狀況，每三個月向政府資訊保安事故應變辦事處常設辦公室提交事故調查進度，直到結案為止。

(c) 保安事故應變

適當的事先規劃可確保有關人員知悉應採取的事故應變行動，而有關行動可在互相協調及有系統的情況下執行，這亦有助相關決策局／部門在處理保安事故時作出適當和有效的決定，從而把保安事故可能造成的破壞減至最少。

須制訂及記錄保安事故應變計劃。保安事故應變計劃須至少包括以下內容：

- 事故應變小組的結構以及相應的角色和職責；
- 第 18.1 (b) 節所規定的報告程序；
- 緩解事故影響、保留證據、調查事故原因及影響的程序；
- 復原計劃；
- 與持份者和公眾的溝通計劃；以及
- 事故後的審查程序。

保安事故應變計劃須至少每兩年定期覆檢一次，或當決策局／部門的操作環境有任何實質改變時進行。決策局／部門須確保所有相關人員熟悉該計劃，並且全體人員（包括管理層人員）均應知悉該計劃，以作為參考和遵行有關要求。這套計劃應清晰直接而且容易理解，讓全體人員清楚了解他們需採取的行動。應變計劃須定期進行測試和更新，以確保可迅速及有效地就資訊保安事故作出應變。決策局／部門須至少每兩年進行一次演習，最好每年進行一次，以評估計劃的有效性。事故應變小組成員須參加演習，熟悉自己在保安事故應變計劃中的角色，以確保快速及有效地回應保安事故。

所有保安事故、已採取的行動和相關的行動結果須予記錄。這些記錄有助確認和評估事故，為檢控提供證據，並為其後的事故處理階段工作提供其他有用的資料。整個保安事故應變過程都應保留記錄。宜為每宗事故編配事故編號，以便在整個事故處理過程中作出跟進和追蹤。

事故記錄最低限度須包括以下資料：

- 系統事件和其他相關資料，例如審計記錄。
- 已採取的所有行動，包括日期、時間和參與行動人員。
- 所有對外通訊，包括日期、時間、內容及有關各方。

當保安事故在非辦公時間發生，7x24 小時的聯絡點對於即時溝通和快速處理事故至關重要，可以有效減少損害及損失。決策局／部門須安排兩個 7x24 聯絡點，以接聽資訊科技保安問題的緊急電話。聯絡點須能及時處理保安事故或向負責人員轉發緊急保安訊息。

有關事故處理指引及程序的詳情，請參閱：

- **《資訊保安事故處理實務指引》**
  可在政府資訊科技情報網下載
  (https://itginfo.ccgo.hksarg/content/itsecure/techcorner/practices.shtml)

上述文件為決策局／部門提供參考，以便制訂部門保安事故應變計劃，並用作防備、偵測及應對資訊保安事故。為使計劃行之有效，應定期安排及進行演習。

(d) 培訓與教育

決策局／部門須確保全體人員均遵守及遵從相應的資訊系統保安事故應變計劃。各人員應熟習由事故報告、確認，以至採取適當行動恢復系統正常操作的處理事故程序。決策局／部門應定期舉行事故處理演習，讓人員熟習有關程序。決策局／部門亦須參加數字政策辦公室指定的保安演習。

此外，為了加強系統或功能範圍的保安保護措施，並減低發生事故的機會，向系統操作和支援人員提供足夠培訓亦十分重要，使他們掌握有關保安預防的知識。

(e) 披露事故的資料

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。

披露有關事故的資料，包括入侵方法、系統背景資料如實體位置或操作系統等，可能會鼓勵黑客入侵其他有相同保安漏洞的系統，亦可能會影響警方偵查時的鑑證及檢控工作。

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

(a) 應急管理

資訊科技應急規劃指在緊急情況或系統中斷的情況下恢復資訊系統及資訊科技服務的臨時措施。有關臨時措施可包括將資訊系統及運作遷移至另一場地、使用其他設備恢復資訊科技服務，或使用人手操作方式提供資訊科技服務。應完整記錄及定期測試資訊科技應急計劃。決策局／部門亦應評估持續業務場地或替代工作場地的保安風險，以確保已推行足夠的保安控制措施保護政府保密數據。

資訊系統的應急計劃有不同種類，最常見的兩種為業務持續運作計劃及運作復原計劃。業務持續運作計劃着重於機構的關鍵業務程序在服務中斷期間及之後仍可持續運作。在業務持續運作計劃中，業務方面的系統擁有人應評估有關系統及數據的關鍵性、進行業務影響評估、設定復原時間目標、復原點目標及界定最低服務水平。運作復原計劃提供詳細程序以助資訊科技能力的復原，下一節將作進一步闡述。

(b) 運作復原規劃

運作復原規劃是就資訊系統制訂運作復原計劃的程序。運作復原計劃包括一份規劃完善的文件，處理資訊系統及／或主電腦場地因發生災難以致系統無法運作及數據全失的情況。運作復原計劃應包括詳細的資訊系統備份程序，以及在另一電腦場地復原資訊系統的程序。制訂計劃時應考慮資訊系統的主電腦場地在災難後可能有一段長時間不可使用，而另一電腦場地的資訊系統運作不能達到理想水平（如可能需要人手操作輔助以彌補服務水平的下降）。計劃應清楚訂明有關各方的職責、各項功能的負責人員和聯絡資料。

計劃應載有運作復原策略，包括詳細及經過全面測試的數據復原及驗證程序。鑑於測試的目的在於增強對程序準確性及成效的信心，因此制訂測試的範圍、方法及預期結果十分重要。

此外，應編製復原數據所需的一切資料及文件，以及在另一電腦場地預先安排通訊網絡服務。運作復原計劃還應包括在災難後把數據復原至已修復的主電腦場地的程序。

決策局／部門應決定其運作復原計劃是否足以應付可能發生的災難。運作復原計劃應載有最新資料，尤其是在主電腦場地的資訊系統出現變更時。定期的運作復原演習是測試運作復原計劃準確性及成效的好方法，但由於進行運作復原演習可能十分費時及影響正常操作，決策局／部門應根據其業務環境決定進行演習的次數。

(c) 資訊科技保安的連續性

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。決策局／部門應在運作復原計劃中，界定職務和職責、資訊保安要求，以及資訊保安的連續性。在欠缺運作復原計劃及應急計劃的情況下，決策局／部門應假設在任何情況下資訊保安要求均與正常操作情況時相同。

19.2 復原能力

(a) 資訊系統的可用性

決策局／部門應識別在資訊系統可用性方面的業務要求。所有資訊系統均應具備足夠的復原能力，以符合在可用性方面的要求。如現存的系統架構不能確保資訊系統的可用性，應考慮具復原能力的資訊科技服務及設施。應測試具復原能力的資訊系統，以確保組件的故障切換功能能按預期運作。在設計具復原能力的資訊系統時，決策局／部門需考慮及解決相關資料的完整性或機密性的風險。

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

(a) 定出適用的法例及合約要求

為避免違反法例及合約要求，決策局／部門須就每個資訊系統的操作，明確定出、記錄及更新所有適用的相關法定、規管及合約要求。應訂明及記錄符合這些要求所需的具體控制措施及個別職責。應定期覆檢資訊系統的保安狀況，有關覆檢應根據適當的保安政策進行，並應審計資訊系統是否遵行適用的保安實施標準和已記錄的保安控制措施。

(b) 知識產權

任何時候均須尊重版權法的限制。只有獲准使用及已購置特許使用權的軟件和硬件，才可按照所有特許證協議及程序設置及安裝。所有人員必須遵守及遵從有關條款。在未獲授權的情況下，須嚴禁複製、竄改或在未獲特許使用權的情況下使用有關軟件或硬件。應制訂保安控制程序，以確保人員遵行所有軟件特許使用權、採購協議及現行版權法例的規定。

應定期（例如每年一次）根據特許證協議，審計所有已安裝軟件的清單。特許使用權證明、軟件手冊及採購文件應存放在密封式檔案櫃等安全地方，並必須定期更新軟件清單。購入軟件升級版後，可能須根據採購協議棄置舊有版本。

- 所有安裝於電腦或在電腦運行的軟件應向獲授權代理商／供應商正式採購。
- 決策局／部門應注意免費軟件的特許使用權未必涵蓋商業用途。
- 應定期覆檢系統的軟件清單，並須就安裝未經批准的軟件或在未獲授權的情況下修改生產檔案展開調查。

(c) 文件記錄

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。已記錄的資料應得到保護，以防止遺失及在未獲授權的情況下被接達。欠缺有關資料會妨礙保安評估或審計活動，該等活動為決策局／部門及政府內部資訊保安監管及保證工作的一部分。

決策局／部門應考慮根據其部門資訊科技保安政策及指引文件，建立一份資料記錄清單，以作為遵行保安要求的證明。有關用作證明遵行要求的資料記錄清單樣本，請參閱《保安風險評估及審計實務指引》。

(d) 數據保護

決策局／部門有責任了解並遵從所訂明的規例。決策局／部門應找出數據可能外泄的途徑，並考慮推行防止數據外泄方案，以監察及保護在儲存、端點使用或與外部通訊傳輸中的保密數據，從而保護保密數據免在未獲授權的情況下被接達或不慎外泄。

決策局／部門亦應留意其他經濟體的規管框架（例如歐盟的《通用數據保障條例》、內地的《個人信息保護法》）（如適用）可能帶來的影響。

所有個人資料應列為限閱類別或以上的保密資料。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。決策局／部門處理個人資料時，必須確保遵行《個人資料（私隱）條例》，特別是保障資料第 4 原則（有關個人資料的保安）。有關六個保障資料原則的詳情，請於個人資料私隱專員公署網站參閱《個人資料（私隱）條例》
(https://www.pcpd.org.hk/tc_chi/data_privacy_law/6_data_protection_principles/principles.html)。

對於可能涉及個人資料的資訊系統，應在整個資料生命周期內推行適當的措施，以有效地處理以下事宜：

- 將個人資料的收集限制於標明目的的相關和必需的最低水平。
- 將個人資料的處理限制於標明目的的足夠、相關和必需的程度內。
- 採用匿名化技術（例如移除或掩蓋個人身分），以盡量減少個人資料曝光的機會。
- 確保在不再需要時刪除個人資料。

當設計載有個人資料的資訊系統時，應採取適當的技術層面和組織層面的保安措施，以保障個人資料免遭未獲授權或意外的接達、處理、刪除或其他用途，包括但不限於確保遵行所有適用的法律和規例、進行私隱影響評估以識別和管理資料保障風險、確保程序和系統的設計使個人資料的收集和處理僅限於必需的標明目的，並提高人員對個人資料外泄時可能造成的後果（如違反保安政策、破壞政府形象、紀律處分）的意識。

為了更好地保護資訊系統中的個人資料，決策局／部門應遵守個人資料私隱專員公署制訂的以下準則。

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

20.2 保安審查

(a) 保安風險評估

保安風險評估旨在評估資訊系統的資訊科技保安風險，根據風險源頭（例如威脅、漏洞）和事件（例如事故場景）識別風險、根據風險的影響和可能性決定風險的級別，並對風險進行緩急排序以作處理。此外，在保安風險評估過程中，進行漏洞識別活動（例如漏洞掃描、滲透測試），以協助識別資訊科技保安風險。保安風險評估完成後，應將已發現但尚未完全處理的風險記錄在資訊系統風險記錄冊中。

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。為免生疑問，（甲）連續兩次評估工作之間相隔的期間，是指（一）在獲得批准撥款後兩次工作的開始日期，或（二）兩次就已識別的風險作出評估的報告的發布日期之間的期間，而有關相隔的期間不得超過兩年；以及（乙）在計算相隔的期間時，不包括針對已識別的風險而推行保安保障措施的時間。

決策局／部門應根據資料的保密類別、與互聯網連接的資料、涉及的個人資料、外判安排，以及適用於每個資訊系統的可用性要求等準則，識別及記錄其資訊系統的相關資料。

資訊系統或生產應用系統在提供正式服務前，以及在進行大規模升級和變更前，也須進行保安風險評估。由於負責分析所收集資料及權衡保安措施的人員須具備深厚的專業知識和豐富的經驗，因此應委任獨立於覆檢範圍的合資格保安專家進行保安風險評估。當聘請服務供應商進行保安風險評估時，須在展開評估前決定和商定細節（例如評估範圍、方法、報告格式）。保安風險評估須根據業界良好作業模式進行，包括現場審查，當中包括對資訊科技基礎設施的徹底檢查和與關鍵人員的訪談，以全面了解環境，並識別可能無法從場外審查中識別的風險。

決策局／部門須在保安風險評估期間定期與服務供應商舉行檢查點會議，以監察進度、提供回饋，以及迅速解決意想不到的問題。決策局／部門須監督保安風險評估，並確保工作質素符合服務協議。雖然完成自我評估清單可以視為是持續監控的有用工具，但不足以被視為徹底和公正的保安風險評估，亦不得用作全面保安風險評估的替代品。

保安風險評估只能概括地提供資訊系統在某特定時間存在的風險情況。決策局／部門應考慮根據資訊系統的風險等級更頻密地進行保安風險評估。

有關保安風險評估的指引，請參閱《保安風險評估及審計實務指引》。

(b) 保安審計

保安審計是以資訊科技保安政策或標準為基礎，以確定現行保護措施的整體狀況，以及核實現行保護措施是否已妥善執行的程序或事件。保安審計的目的在於了解現有環境是否已根據既定的資訊科技保安政策得到妥善保護。保安審計須至少每兩年進行一次，以確保有關各方已遵行保安政策和採取有效的保安措施。決策局／部門須備存有關保安過程及程序的最新文件，以便促進保安審計過程。

決策局／部門應按照已規劃的保安審計的性質，考慮所委聘的保安審計師是否適當人選。須選擇獨立和可信賴的第三方作為保安審計師，以確保審計觀點正確、公平和客觀。委聘內部或外部保安審計師的工作應慎重計劃，尤其是委聘處理保密資料的保安審計師。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。此外，決策局／部門應避免長期聘請同一保安審計師，以避免獨立性下降。

保安審計須由具備足夠技術和經驗的審計師，在系統管理員的陪同下進行。應清晰界定和分派參與審計各方的職務、職責和責任。

保安審計須由具有相關專業資格的獨立保安審計師（如註冊信息系統審計師（CISA）、註冊信息系統安全專家（CISSP）和註冊信息安全專業人員（CISP））進行。審計師也應具有審計類似系統或行業的相關經驗。

保安審計須評估資訊系統有否遵行政府資訊保安要求和決策局／部門的資訊保安政策和指引。保安審計不得被視為對保安風險評估工作中所建議的修正措施的核證過程。保安審計須包括與不同持份者的訪談，以及就系統設定、記錄、政策、程序和其他相關文件的審查。

當發現任何違規情況時，決策局／部門須：

- 確定違規原因。
- 評估是否有需要採取行動。
- 採取任何需要的行動。
- 覆檢任何修正行動的成效。
- 記錄及備存審計及所採取修正行動的結果。
- 審查類似的問題是否適用於其他資訊系統。

有關保安審計的指引，請參閱《保安風險評估及審計實務指引》。

(c) 技術性遵行覆檢

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。為使用這些軟件及程式而作出的所有資訊系統變更，應受到嚴格的變更管理控制。決策局／部門應根據最小權限原則，分配有適當接達權限的專用帳戶，以進行保安漏洞掃描、滲透測試、配置審查和源碼掃描。在完成有關工作或活動後，應立即刪除有關帳戶，或重設有關帳戶的密碼。

決策局／部門須至少每年一次、在提供正式服務前，以及在進行就與資訊系統相關的大規模升級和變動前，對所有與互聯網連接的資訊系統進行漏洞掃描。漏洞掃描也應納入資訊系統保安風險評估的風險識別程序中。所有與互聯網連接的資訊系統的保安風險評估工作須包括滲透測試。決策局／部門應定期、在提供正式服務前，以及在進行就與資訊系統相關的大規模升級和變動前，對所有與互聯網連接的資訊系統進行配置審查和源碼掃描。應在系統正式服務前評估所確定的保安漏洞及問題，並採取適當修正行動處理。

由於漏洞掃描、滲透測試、配置審查和源碼掃描可能會危及資訊系統的安全，所以應計劃、記錄並小心進行這些活動。保安漏洞掃描、滲透測試和源碼掃描應只由獲授權的合資格人士或在該等人士監督下進行。

有關技術性漏洞管理的詳情，請參閱第 14.6 節《技術性漏洞管理》。

(d) 資訊保安遵行的監察及審計機制

決策局／部門須遵從附錄 D 所規定由政府引入的機制，用以簡化監察及評估決策局／部門關於資訊保安遵行情況的各項程序。

有關上述機制的詳情，請參閱政府資訊科技情報網的資訊科技保安主題專頁 (https://itginfo.ccgo.hksarg/content/itsecure/isc_new/index.asp)。

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 ***

附錄 A 終端用戶資訊科技保安操作指示樣本

本文件旨在協助終端用戶了解他們在資訊科技保安方面的責任。

決策局／部門應採用隨附的終端用戶操作指示樣本，自行編製其終端用戶保安操作指示。決策局／部門應根據其部門資訊科技保安政策和電腦操作環境，特別編製切合需要的終端用戶操作指示。決策局／部門應向所有在職及新入職人員派發相關文件，並定期提醒各人員閱覽文件。

本終端用戶操作指示文件不能取代決策局／部門或政府現行的保安文件。用戶須閱讀所有現行保安文件的要求並遵從行事。

終端用戶
資訊科技保安操作指示

[部門名稱]

[*人員姓名*]已獲委任為部門資訊科技保安主任，負責監督[*決策局／部門名稱*]的資訊科技保安工作。保安是每名人員的個人責任。終端用戶應根據數據類別小心保護資料或資訊系統。每名用戶必須對其在資訊系統上所進行的一切活動負責。

為防止他人在未獲授權的情況下接達或披露保密或個人資料，有關各方均須遵守現行的政府資訊科技保安要求，包括《保安規例》和《基準資訊科技保安政策》。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，這類資料須只提供給有需要和有權接達資料的政府內部及外部人員，以便他們有效執行工作。如對某人員是否有權接達某份文件、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。

用戶須妥善地保管及保護電腦和儲存裝置，以防止他人在未獲授權的情況下接達或披露其所管有的資料。同時，須推行適當的保安措施，以保護政府資訊資產及資訊系統。用戶如察覺任何可疑活動或懷疑發生違反保安事項，須盡快在辦公時間內向[*求助台*]報告。如在辦公時間外發生保安事故，請聯絡以下人員：[*填上姓名及聯絡資料*]。

違反資訊保安要求者可能會受到紀律處分。

以下是處理政府資料或使用資訊系統時應做與不應做的事項。請注意，下文所列事項並非詳盡無遺，故應視乎情況同時參照部門資訊科技保安政策、《保安規例》和《基準資訊科技保安政策》[S17]。

應做的事項

- 保密類別須清楚標明，例如就載有限閱資料的電郵而言，應在標題之前註明[限閱]。
- 所有保密資料必須加密儲存。所有保密資料在任何通訊網絡上傳遞時均應加密。機密或限閱資料在不可信任的通訊網絡上傳遞時必須加密。
- 在政府內部以電郵方式傳遞機密資料時，須使用「政府內部機密郵件系統」、「機密信息應用系統」、「機密電郵流動服務」和「中央管理訊息平台」中已獲批准的子系統。
- 在發送電子郵件之前，尤其是當電子郵件包含保密或個人資料時，小心檢查收件人的電子郵件地址。
- 檢查郵箱中是否有可疑活動，以及電子郵件帳戶設定中是否有不熟悉的變更。例如，在沒有通知的情況下設定了郵件規則的配置、收件匣不再接收電子郵件，或「已傳送」資料夾包含你未撰寫過的外發電子郵件。
- 透過檢查通訊中使用的電子郵件地址、劃一資源定位址和拼寫，驗證收到的訊息和內容的真實性。
- 經常備份關鍵數據，以及保留備份的離線副本，並採取足夠的保護措施。
- 減少在流動電話處理和儲存保密或個人資料。

- 在使用流動電話時，讓其處於持續和直接受到監察的情況，並在不使用時將其存放在與其儲存的資料保密類別相應的實體受保護區域。
- 應採取適當的保安措施，以妥善保護所管有的設備、裝置或用戶身分資料，例如啓動密碼保護、登出或關機、無人看管時把有關設備、裝置或資料鎖於櫃／抽屜內。
- 確保工作環境安全及穩妥，例如使用熒幕防窺片，以防止敏感資料意外泄露及避免遭受竊聽。
- 應按照「有需要知道」原則發放資料及授予資料接達權限。
- 應根據部門密碼管理要求設定密碼，例如採用由至少八個大寫的字母、小寫字母、數字及特殊字符混合組成的密碼，並定期更改密碼。如懷疑密碼已被破解，應立即更改密碼並向上級報告。
- 應就每個系統或服務賬戶使用獨特且足夠複雜的密碼，例如公務電郵帳戶的密碼應與私人電郵帳戶的不同。
- 為線上帳戶啟用多重認證（如有），盡量減低憑證被竊的風險。
- 應安裝最新的保安修補程式，並定期刪除快取檔案或臨時檔案，以保障資料私隱。
- 應推行配備最新惡意軟件識別碼和定義檔案的惡意軟件偵測措施，以便在使用前掃描電郵、已下載檔案、抽取式媒體或流動裝置上的檔案。
- 應不理會或刪除濫發電郵[8]。小心仿冒詐騙電郵[9]可引致感染惡意軟件甚或違反保安事項。
- 應採用加密方法保護無線或流動裝置，以保護所傳遞的數據，並啓動密碼保護功能，以防止他人擅用該等裝置。

[8] 濫發電郵指濫發無用的訊息（例如廣告），使電郵帳戶不勝負荷。
[9] 仿冒詐騙電郵指仿冒收件者認識的人送出電郵，意圖竊取資料。

- 應關閉無需使用的無線及流動服務。
- 關掉不使用的無線連接，如 Wi-Fi、近距離無線通訊、藍牙和紅外線連接。
- 關閉自動連接 Wi-Fi 以避免自動連接不安全的網絡，例如在公共場所。
- 使用政府提供的互聯網服務時，應遵從《使用互聯網服務的指導原則》[10]。

不應做的事項

- 不應在私人擁有的流動裝置、抽取式媒體或物聯網裝置儲存保密資料。
- 不應在無人看管和沒有推行足夠實體接達控制措施（例如房門已打開、物品遺留桌上）的情況下，離開工作站及電腦設備。
- 不應將寫有密碼的紙張放置於工作間附近（例如貼在屏幕上的便條紙），或使用容易猜到的密碼（例如在詞典中查到的單字）或與個人資料相關的密碼（例如姓名、出生日期或職位名稱），或與他人共用密碼。
- 不應向未獲授權人士披露個人、系統或部門資料。
- 不應把私人擁有的裝置連接至政府內部資訊系統或網絡。
- 不應經撥號調解器、無線界面或寬頻鏈路將工作站連接至外部網絡。
- 不應向非應邀和任何可疑的電子訊息（包括但不限於電子郵件、即時訊息和短訊）作出回應、開啓附件或點擊連結。

10 https://itginfo.ccgo.hksarg/content/itsecure/techcorner/practices/Guide_use_of_Internet.htm

- 不應從未經確認可信賴的網站下載和開啟檔案。
- 不應使用政府電子郵件地址註冊與工作無關的線上服務。
- 不應重複使用與政府電子郵件帳戶相同的密碼訂閱其他線上服務。
- 不應使用任何私人電子郵件服務進行官方通訊，尤其是在以官方身分與公眾或外部機構通訊的情況下。
- 未經部門資訊科技保安主任事先批准，不應在工作站安裝軟件。
- 不應關掉政府擁有裝置的現有端點保護功能。
- 不應於工作站接達來自不明抽取式媒體的檔案。
- 未經決策局／部門指定人員事先批准，不應在工作站安裝及執行未獲授權軟件。

附錄 B 評級指引

決策局／部門在為資訊系統評級時，應參考以下考慮因素。

1. 第 2 級資訊系統

第 2 級資訊系統是指對政府或社會運作重要的資訊系統，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。

一般來說，資訊系統故障或中斷對政府造成的影響可分為三個嚴重程度，詳情如下：

影響程度	描述
高 （H）	對政府造成重大損失／嚴重損害或不利
中 （M）	對政府造成中等損失／一些損害
低 （L）	對政府造成輕微損失／少許損害

下表總結一些在判斷影響時的要素，以供考慮。這些要素可以分為四個不同的方面。決策局／部門應慎重考慮系統發生故障或中斷時在不同方面的影響程度。

方面	資訊系統故障或中斷時應考慮可能會導致的影響	影響程度（高／中／低）
防禦／保安風險	(a) 危害人命或財產 (b) 無法維持治安 (c) 無法執行法定責任 (i) 在及時的情況下 (ii) 在信心和／或正確性足夠的情況下 (iii) 在規劃資源受限等情況下 (d) 導致實體／資訊資產損壞或遺失 (i) 實體設施、系統或網絡 (ii) 設備、組件或必需品 (iii) 數據、個人資料、知識產權等 (e) 令保安控制措施鬆弛等	
經濟影響	(a) 直接或可能導致政府財務損失 (i) 直接的財務損失 (ii) 稅款損失或徵收稅款延誤 (iii) 延遲檢討政府收費 (iv) 執行跟進行動（例如清理和／或整理數據）有額外支出 (v) 在付款過程中延遲所產生的額外開支／補償等。	

政府形象	(a) 影響政府聲譽 (b) 影響公眾信心等	
為用戶提供的服務	根據終端用戶的類型及用戶人口，當服務中斷或在效率下降時，影響有多嚴重？ (a) 影響大量用戶還是只影響少數用戶？ (b) 目標終端用戶是公眾，或只在所屬決策局／部門內，還是其他決策局／部門？ (c) 干擾政府高層官員分析資訊與決策過程？等。	
其他	請包括任何適用於其資訊系統的其他考慮範疇。	
	整體影響程度：	

（註：請同時考慮服務中斷對其他相互依賴的資訊系統的影響。）

一般來說，如果有一個或多個方面的影響程度被評估為「高」，你應考慮將系統或服務的整體影響程度視為「高」。如果整體影響程度為「高」，則該資訊系統應視為第 2 級資訊系統。

2. 第 3 級資訊系統

有很多必要服務對社會及其經濟的運作和安全是關鍵的。第 3 級資訊系統是指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。

為識別第 3 級資訊系統，決策局／部門應識別其所提供的必要服務，並隨後根據定義決定第 3 級資訊系統。一般來說，必要服務通常分布在對社會有重大影響的不同行業（例如航空、銀行和金融、廣播、通訊、能源、醫療保健、陸路運輸、海事、媒體、保安和緊急服務、供水和污水處理等）。在識別必要服務時，決策局／部門應根據服務性質以及服務對社會及其經濟的運作和安全的影響，考慮其所提供服務的關鍵性。在識別必要服務後，決策局／部門應隨後識別與提供相關必要服務直接相關的第 2 級資訊系統，所識別的資訊系統被視為第 3 級資訊系統。

上述考量可作為決策局／部門為其資訊系統評級的參考。決策局／部門應參考上述指引作出自行評估。如有疑問，歡迎決策局／部門就系統評級的評估諮詢數字政策辦公室的意見。

附錄 C 資訊系統應有的資訊科技保安等級保護

第 2 級資訊系統與第 3 級資訊系統須根據其系統等級分別採取以下更嚴格的保安控制措施，以達致資訊系統應有的資訊科技保安等級保護。第 3 級資訊系統亦須採用第 2 級資訊系統保安控制措施。

政府資訊保安組織（第 5 節）	
第 3 級資訊系統	a) 設有第 3 級資訊系統的決策局／部門，其資訊科技保安主任須由高層管理人員中的首長級人員擔任。 b) 就設有第 3 級資訊系統的決策局／部門，須成立由高層管理人員及部門資訊科技保安主任參與的資訊保安督導委員會，以確保在資訊保安方面投入足夠的資源和關注。資訊保安督導委員會須定期召開會議。委員會的討論結果須妥為記錄，包括關於資訊保安相關問題的管理層指示，以便作出跟進行動。委員會的結構、職務和職責也須記錄在案。 c) 就設有第 3 級資訊系統的決策局／部門，須最少有一名資訊科技保安管理組的成員持有最少一項業界認可的資訊科技保安認證（例如註冊信息系統審計師（CISA）、註冊信息系統安全專家（CISSP）和註冊信息安全專業人員（CISP）等）。
管理職責（第 7 節）	
第 3 級資訊系統	a) 就設有第 3 級資訊系統的決策局／部門，有關決策局／部門須採用第 7.2(c)節所訂明的資訊科技保安風險管理架構。決策局／部門須為其第 3 級資訊系統備存風險記錄

	冊。風險記錄冊須至少記錄已識別的資訊科技保安風險、其發生的可能性和嚴重性、減低該風險的措施和所需的監測。
人力資源保安（第 9 節）	
第 3 級資訊系統	a) 就設有第 3 級資訊系統的決策局／部門，有關決策局／部門須制訂資訊科技保安培訓計劃，以便為其人員提供適切和有系統的資訊科技保安意識活動。培訓計劃亦須確保參與第 3 級資訊系統支援和操作的所有人員，包括產銷商、承辦商和服務供應商，熟悉資訊科技保安要求及當前的資訊科技保安威脅、影響和緩解措施。若無法為產銷商、承辦商和服務供應商制訂或提供培訓計劃，決策局／部門須與對方訂立合約責任，要求對方向其人員提供相關的資訊科技保安培訓。
接達控制（第 11 節）	
第 2 級資訊系統	a) 須至少每六個月一次定期由獨立方檢查／審計高權限帳戶的使用情況，以確保這些帳戶是為合法目的而使用。 b) 如果沒有技術解決方案限制高權限帳戶接達資訊系統和應用系統中的數據，決策局／部門須採用行政程序以管理有關接達（例如從另一個指定人員保存的密封信封獲取密碼、由兩名員工使用分拆的密碼登入）。 c) 須確實執行第 11.4(b)節規定的嚴謹密碼政策。此外，如果任何資訊系統被入侵時可能會影響第 2 級資訊系統的安全（例如資訊系統與第 2 級資訊系統共用同一個網絡分段、或能夠對第 2 級資訊系統進行管理功能的特定設備），亦須確實執行嚴謹密碼政策。

	d)	在技術上可行的情況下，須對第 2 級資訊系統的高權限帳戶的任何互動式登入實施多重認證。
操作保安（第 14 條）		
第 2 級資訊系統	a)	須備存本地和場外備份。場外資料備份須存放於穩妥及安全的地方，並遠離設備的的所在地。
	b)	須制訂及記錄容量管理計劃。
	c)	為了減低軟件終止支援的影響，須在終止支援日期前至少六個月制定遷移計劃，而相關的保安措施須在終止支援日期前實施。
	d)	所有已知的保安漏洞須盡快修復，通常在保安修補程式發布後一個月內完成。決策局／部門須進行風險評估，考慮漏洞的潛在影響和被利用的可能性，以決定漏洞緩解的方法和時間表。風險評估的結果須妥為記錄。如漏洞未能在一個月內得以緩解，決策局／部門須告知其部門資訊科技保安主任有關理據、相關風險以及緩解方法和時間表，以提高漏洞緩解狀態的可見性。決策局／部門亦須每月向資訊科技保安主任提供有關漏洞緩解狀態的中期更新情況，直至漏洞得以緩解。
第 3 級資訊系統	e)	就設有第 3 級資訊系統的決策局／部門，有關決策局／部門須建立資訊科技保安監察流程，當中包括 24×7 的資訊科技保安監控。資訊科技保安監察流程讓決策局／部門能夠整合來自多個來源的數據（例如防火牆、入侵偵測系統／入侵防禦系統、端點偵測與回應／網絡偵測與回應的解決方案），以提供全面的保安情況，以便對潛在的保安事件作出更快捷有效的應變。此外，保安監察流程須有助監察網絡和系統內的活動，並提供持續的威脅偵測、監察和事故應變能力，包括利用保安資訊和事件管理工具協助全面分析及關聯來自多個來源的保安事件數據。

系統購置、發展及維護（第 16 節）	
第 2 級資訊系統	a) 須採用保安左移方法，包括依照第 16.1(a)節規定在系統設計階段採取保安編碼作業模式和保安審查。在提供正式服務前的保安風險評估須核實保安覆檢的跟進行動，以確保系統在正式投入運作前已推行所需的保安措施及控制措施。 b) 系統強化須在系統投入運作前進行，強化後的系統須作為進一步更改的基礎。
資訊科技保安方面的業務持續運作管理（第 19 節）	
第 2 級資訊系統	a) 須制訂資訊科技應變計劃以確保第 2 級資訊系統在出現極嚴重的服務中斷（例如火災、水浸等天災）或緊急情況（例如恐怖襲擊、大型示威或炸彈威脅而需撤出場地）時仍可持續運作。須完整記錄及定期測試資訊科技應變計劃，並與業務持續運作計劃互相配合。
第 3 級資訊系統	b) 須具備足夠的復原能力，以防止所提供的必要服務中斷。須定期測試復原能力，以確保組件的故障切換功能的運作能夠符合預期目標。
遵行要求（第 20 條）	
第 2 級資訊系統	a) 須每年至少一次對第 2 級資訊系統進行漏洞掃描，並在資訊系統正式投入運作前，以及在進行大規模升級和變更前進行漏洞掃描。 b) 滲透測試須包含在所有第 2 級資訊系統的相應保安風險評估工作中。對於與互聯網連接的第 2 級資訊系統，決策局／部門須確保每年至少進行一次滲透測試。

第 3 級資訊系統	c)	第 3 級資訊系統須至少每年進行一次保安風險評估，並在資訊系統正式投入運作前，以及進行大規模升級和變更前進行。保安風險評估須包括漏洞掃描、滲透測試、配置覆檢和源碼掃描。保安風險評估包含的滲透測試須由具有專業資格或認證（例如，道德黑客認證課程（CEH）、Offensive Security 認證專家（OSCP））的獨立服務供應商進行。保安風險評估完成後的保安風險評估報告，包括系統風險記錄冊、相應的漏洞掃描報告、滲透測試報告、漏洞修正計劃等，須經部門資訊科技保安主任認可。

附錄 D 資訊保安遵行監察與審計機制

政府引入以下資訊保安遵行監察及審計機制，以簡化監察及評估決策局／部門關於資訊保安遵行狀況的各個過程：

1. 就設有第 3 級資訊系統的決策局／部門，有關決策局／部門須向數字政策辦公室提交其資訊科技保安管理組的編制、匯報機制、職務及職責。如有需要，數字政策辦公室可要求決策局／部門澄清相關資料。若資料有任何重大變更，決策局／部門須在三十天內通知數字政策辦公室。
2. 決策局／部門須向數字政策辦公室提交其第 2 級資訊系統、第 3 級資訊系統的清單及系統評級的評估詳情(獲決策局局長／部門首長或他們明確授權的首長級人員同意)。若所提交的清單有任何變動，包括系統評級的變動，決策局／部門亦須在三十天內通知數字政策辦公室。數字政策辦公室可要求各決策局／部門提交進一步資料，以確保各決策局／部門對系統等級的評估符合第 7.2(b)節所訂明的資訊科技保安等級保護。
3. 第 3 級資訊系統的事故應變計劃須在數字政策辦公室要求下提交檢查及覆檢。
4. 決策局／部門須提交一份標準表格《保安遵行狀況表》向數字政策辦公室概括其所有系統的資訊保安風險評估及保安審計的資料。每次完成保安風險評估或保安審計後，應在六個月內向數字政策辦公室提交中期表格，以追蹤保障措施的推行情況。如所有保障措施已在六個月內推行，《保安遵行狀況表（中期）》將視為《保安遵行狀況表（終期）》，否則應在完成保安風險評估或保安審計後一年內，向數字政策辦公室提交《保安遵行狀況表（終期）》。
5. 第 3 級資訊系統保安風險評估報告，包括系統風險記錄冊、相應的漏洞掃描報告、滲透測試報告及漏洞修正計劃，均須於評估完成後三十天內提交予數字政策辦公室，以供進行檢查和覆檢。
6. 第 3 級資訊系統的保安審計報告須在審計完成後三十天內提交予數字政策辦公室，而若出現違規，則須在提交審計報告後三十天內進一步提交修正計劃。
7. 決策局／部門須參與由數字政策辦公室進行的抽樣保安審計，並在議定的時間內優先完成審計。這項工作評估決策局／部門進行保安風險評估及保安審計的質素，以及對政府資訊保安要求的遵行情況。決策局／部門須提交標準表格《遵行審計跟進狀況表》，以報告遵行審計所需的跟進工作的完成情況。每次完成遵行審計後，決策局／部門應在六個月內向數字政策辦公室提交中期表格，以追蹤建議的落實情況。如所有建議均已在六個月內落實，《遵行審計跟進狀況表（中期）》將被視為《遵行審計跟進狀況表（終期）》，否則應在完成遵行審計後一年內，向數字政策辦公室提交《遵行審計跟進狀況表（終期）》。

8. 決策局／部門須完成數字政策辦公室定期進行的保安問卷調查，以收集保安狀況資料。通過問卷調查可了解決策局／部門有關資訊保安的計劃、慣例及行動。這些資料可反映決策局／部門在回應保安政策、保安威脅或其他保安問題方面的就緒程度。