# 香港航空發動機維修服務有限公司

# 資訊保安政策

版本: 2.2

發布日期: 2021 年 4 月 01 日

*本政策內容由 香港航空發動機維修服務有限公司 - 資訊科技部門 編寫。*

*如果您對本手冊有任何疑問或建議，請隨時與該負責人聯繫。*

封面
2021 年 4 月

內容目錄

## 1. 資訊保安角色及責任

### 背景

資訊保安具綜合功能，需要有效的組織及協調。角色及責任在港發皆屬重要。

### 內容

a. 財務及行政總經理(GMFA)負責在資訊保安、為公司制訂資訊保安標準及程序與及監察有否遵守政策及指引各方面提供領導。

b. 資訊持有人(通常指部門主管)負責確保有關的資訊資產受到正當保護。

c. 資訊科技(IT)部門負責提供及維持一個安全的資訊科技環境，以便用作儲存公司的資訊系統及數碼資訊。

d. 所有公司員工有責任做足預防措施，保護會接觸到的資訊，包括但不限於

- 採取措施去限制只在有需要時才取用資訊；
- 密碼要保密及定時更改；
- 不要將公司或客戶的敏感資料放上社交媒體、即時通訊網站、公司以外的電郵系統或其他同類網站；
- 確保敏感資料不要胡亂放在辦公桌上無人理會；
- 利用加密來防止披露機密的電子資料；
- 立即報告保安事故；
- 為個人電腦及流動裝置做好保安措施；及
- 妥善保存已打印的敏感文件。

e. 人力資源部負責確保所有新僱員在入職時已知悉資訊保安政策及指引，與及提供持續培訓。

f. 資訊科技部門要確保當僱員離職時不能再使用資訊科技系統(例如電子郵件及流動裝置管理)。

g. 所有員工必須立即將前僱員由所有與公司業務有關的通訊群組中移除 (例如 WhatsApp 及 WeChat)。

## 2. 資訊生命週期管理

### 背景

所有員工應該能夠分辨敏感資料，評估對公司的潛在風險，及實施適當的分類及保護。

### 內容

1. 資訊持有人

   - 資訊持有人在其管理範圍內有責任確保正確實施資料分類計劃及相關的監控。
   - 資訊持有人需要分辨、分析風險、分類及保護用於公司業務上的敏感資料及數據，不論其所儲存的媒體及格式。
   - 資訊持有人需要在其管理範圍內監察有否遵守政策及確保資訊受到保護。

2. 保護

   a. 所有資訊的保護依照保密、完整性及可用性為根據。

3. 保密

   a. 資訊只供有關員工及授權的非僱員在有需要時使用。

   b. 有需要時，在僱員、客戶及供應商合約內加入保密協議條款。

   c. 與商業拍檔的保密協議生效後才可以進行交換內部及敏感資料。

   d. 在傳送敏感資料前必須進行加密，例如出糧數據的儲存應利用軟件加密。

4. 完整性

   a. 所有對港發政策及程序的改動需要記錄下來(例如修改工程程序指引手冊) 。最低限度要記下由誰人及何時改動。

   b. 至於公開及敏感的資料，要以適當的手段偵測到未經批准的改動，包括程序及/或技術上的方法。

5. 可用性

保存

保存期間的資訊(例如引擎檔案文件)只可向授權人士提供。

備份及復原

資訊應根據資訊持有人定義的業務需要進行備份。備份由資訊科技部協調，不容許獨自進行的備份(例如可攜式硬碟)。

6. 分類

資訊最少應該有四種分類:

a. 公開 – 向公眾披露的非敏感資料。

b. 只限內部使用 – 屬於業務單位不向公眾及外人披露的資料，但可供員工及授權的非員工使用。

c. 敏感 – 業務單位內敏感或機密的資料，只提供給有需要知道的人士業務上使用，在使用或完整性上不需要作不合理的妥協。

d. 高度敏感 – 業務單位內具有最高價值，極度敏感或機密的資料，只提供給指定人士使用，在使用或完整性上不需要作不合理的妥協。

## 3. 保安意識及培訓

### 背景

應定期提醒管理層及員工他們的資料保安責任，每年最少提供一次保安意識培訓，可以幫助公司穩固資產及促使員工履行資料保安的責任。

### 內容

a. 人力資源部為所有新員工入職時提供的行為守則入職培訓會包括資訊保安政策。

b. 就政策上的任何更新，部門主管有責任在部門簡報會上傳達改動。

c. 行動守則的複習培訓(包括本政策)會定期舉行。

## 4. 與公司以外人士溝通

### 背景

敏感資料只可以向公司以外獲授權接收該等資訊的人士披露。

### 內容

a. 與公司以外人士溝通時員工要小心那些資料可以披露。 考慮的地方包括可以披露到什麼程度及對公司潛在影響的風險。

b. 得到有關資訊持有人的批准後才可以向外界傳達內部及敏感資料。

c. 由於合約關係要與第三方交換內部及敏感資料的情況下一定要簽訂保密協議。與供應商討論合作計劃中而未有合約的情況下亦應考慮使用保密協議。

d. 在送出敏感資料前應該加密或加上密碼。

## 5. 實際取用

### 背景

員工及公司訪客實際取用時應受管理及監控，以便減低敏感資料被未獲授權人士取用及刪除的風險。

### 內容

a. 所有訪客要登記；登記程序要能夠證明訪客的身份、所屬機構、探訪原因與及被探訪者的詳細資料。

b. 部門主管有責任為存放敏感資料的範圍設立保安。有更高風險的範圍可以考慮增加實際保安措施。

c. 部門主管負責在其管轄範圍內批准所有正常及臨時員工適當的實際取用，而取用應只限於適合日常工作安排的範圍及時間。

d. 如果可行的話，在工作時間儘可能在枱面放最少的紙張及電子媒體；不使用時及放工後將所有含敏感資料的紙張及媒體鎖好。

## 6. 手提電話及其他便攜流動裝置

### 背景

藏有公司敏感資料及/或可以存取公司網絡的流動裝置要正確保護以防在未經批准下洩露資訊。

### 內容

a. 流動裝置在提取及使用公司資料時與其他非流動裝置一樣受制於同樣的資訊保安限制。

b. 公司提供的流動裝置，及個人流動裝置當取用公司網絡或儲存公司敏感資料時

- 應設定為根據公司保安標準可以保護避免未經批准情況下披露資料;
- 應設定不易破解密碼;
- 應設定流動裝置管理軟件(MDM)；
- 啟動遙控銷毀資料。

c. 員工不要在藏有公司數據的裝置上嘗試繞過或移除公司的保安政策設定。

d. 員工有責任當敏感資料已根據預期目的閱讀或使用後，及在棄置該裝置前，從流動裝置移除任何公司的敏感資料，或將這些資料重新交放置到一個更安全的儲存地方。

e. 員工一旦發現任何未經批准使用或取用存有公司敏感資料的流動裝置事件或懷疑事件應立即通知資訊科技部，然後向該流動裝置發出遙控銷毀資料指令(如果該裝置有的話)以便移除公司數據。

## 7. 電子郵件及即時通訊

### 背景

敏感資料只可以經由公司批准的電子通訊系統發出。

### 內容

a. 禁止使用任何公司批准用作交換公司資訊的電子系統以外的其他電子通訊系統。

b. 員工不能:

- 向大型群組發出訊息，除非是業務上有特定需要。
- 轉發非正式的連鎖訊息。
- 容許其他使用者使用自己的帳戶。
- 將公司電郵系統的電子郵件自動轉發至一個私人電子郵件帳戶。
- 將郵件自動轉發至另一員工的帳戶，除非有特定的業務原因。

c. 製造或發佈任何滋擾或令人反感的訊息或使用不適當語言，破壞公司形象。

d. 開啟檔案附件前一定要使用公司的防毒/惡意程式軟件掃瞄。

e. 公司通訊系統受到監察以便偵測可疑活動，保持記錄檔案以作可能調查之用。

## 8. 使用互聯網

### 背景

為了避免資訊保安的相關風險或未獲批准而披露敏感資料，當使用互聯網設施時要額外小心。

### 內容

a. 進入互聯網的人員禁止從事不適當活動，包括但不只限於以下所述：

- 未得到批准及透過未經批准的渠道發放任何敏感資料；
- 在互聯網對敏感資料發表個人意見；
- 製作、發佈或發出非法及惹人反感的訊息或材料，包括任何有可能誹謗、令人尷尬、恐嚇、騷擾、冒犯或傷害到員工、服務供應商、客戶或任何人士；
- 進入惡意網站，有可能對公司的保安構成威脅；
- 下載一些侵犯其他公司知識產權、版權或是不道德或惡意的材料；
- 發動及延續“連鎖”形式文件；及
- 下載未經批准的電腦軟件或應用程式。

b. 公司保留權利限制個人或團體進入任何有需要限制的網站。

c. 公司已啟用互聯網取用記錄，以作日後調查之用。

## 9. 電腦及資訊科技設備

### 背景

所有電腦(包括桌上電腦、手提電腦及/或其他電腦設備)應妥善保存，避免未經批准使用或不正當使用資料。

### 內容

a. 在未經資訊科技部批准前，使用者不得在公司網絡內安裝網絡設備。該等設備包括但不限於數據機、無線存取點、互聯網存取或其他可以容許公司以外人士進入公司系統及/或網絡及資料的外部網絡連接。

b. 使用者不得在公司電腦及網絡設施上安裝任何類型的軟件(不論軟件為有版權、無版權、共享或免費，來自外置裝置、互聯網、電郵或其他軟件運送媒介) 。

c. 一定要安裝螢幕保護密碼、防止當離開座位時電腦被非法使用。

d. 應用程式應提供加密軟件或密碼保護以便保護敏感資料。

e. 手提電腦當無人看管時要做好保安措施。

f. 對應用程式設定、應用程式、作業系統及網絡的更改要正確記錄，包括保安要求的改變，要得到所屬的“系統持有人”批准才可付諸實行，另外在移往生產前亦要經適當人員進行正式測試。資訊科技部有責任為應用程式及基礎設施的開發、實施及保養設立正確的保安機制及程序。

g. 檢討進入系統的申請有否遵守公司有關政策，確保存取權限是根據職責批出亦有正確分工，得到授權人士批准，準確地記錄在系統，及每年會檢討有否持續遵守。

## 10. Internet of Things (IoT) 的規定做法

### 背景

IoT 即接駁至網絡的感應器或設備，例如感應儀表、閉路電視及大型屏幕。它們的保安比一般電腦設備差。下例方法可以改善保安問題:

### 內容

a. 設立網絡可見性及控制;

b. 更改預設賬戶及密碼;

c. 連按至業務單位正常電腦網絡以外的網絡;

d. 調整設定及關閉不必要的功能(例如大型屏幕的聲音控制);

e. IoT 的專屬軟件開發要根據Open Web Application Security Project (OWASP) IoT保安指引進行;及

f. 定期測試及應用保安修補程式。

IoT得出的數據要可以主動地管理。

## 11. 個人資料的規定做法

### 內容

- 請參考人力資源工程程序指引手冊第(04-11-07-01)冊。

## 12. 外判服務的規定做法

### 內容

- 請參考物料管理工程程序指引手冊 40 冊 10 節。

## 13. 社交媒體

### 概論

1. 香港航空發動機維修服務有限公司(“港發”)認識到社交媒體改變了分享資訊的方法，如果適當使用的話可以是一個有效及快捷的溝通工具。本社交媒體政策(“政策”)為適當使用社交媒體提供指引。港發支持公開對話與及知悉社交媒體可以提供的機會。港發不想阻止人們使用社交媒體。但是社交媒體可以在財政上及聲譽上損害港發及其僱員。特別是當使用者被發現是港發僱員或與港發有任何聯繫。本政策的宗旨是要保護港發及僱員免受損害。

2. 政策適用於港發所有僱員與及臨時員工、顧問及其他與港發業務有聯繫的人士(“使用者”)。所有香港的使用者都要遵守政策。香港以外的使用者經考慮當地的法律要求及政策後亦要酌量遵行。

3. 使用者在工作場所不得違反行為守則中有關舉報、個人資料、多元共融、資訊及網絡安全與及其他政策。使用者使用社交媒體時要尊重別人。

4. 政策適用於個人或業務上使用社交媒體，在辦公時間以內或之外，及使用個人及港發的裝置及設備。它適用於所有社交媒體，不論現在及將來，包括 Yammer, Twitter, Facebook, LinkedIn, TikTok, Instagram, Snapchat, WhatsApp, WeChat, Wikipedia, TripAdvisor, YouTube, Flickr 及 LIHKG。

### 部門主管

5. 部門主管要確保其部門的使用者知悉本政策及得到適當的支援及資訊，包括任何適用於該部門的額外指引。

### 使用者

6. 所有使用者應該:

   a. 瞭解及遵守政策;
   b. 在社交媒體只准發表準確及合法的資訊; 及
   c. 向部門主管舉報不正當使用社交媒體。

## 使用社交媒體

7. 代表港發使用社交媒體前要先得到公司書面批准。這包括維持港發帳戶、代港發發表訊息及評論、上傳內容及回應其他人士。
8. 個人使用社交媒體應該遵守政策。使用者要為放上社交媒體的事物負責。使用者不要發表不專業及不恰當的內容及利用違背對港發負責的方法去使用社交媒體。
9. 當使用者表露身份為港發僱員或發表有關工作上的資料時應表明僅屬個人意見而並非代表公司。一定要使用如後的免責聲明: “本網站發佈的訊息僅屬個人意見，並不代表本人僱主的看法及立場。”)

## 具體規則

10. 使用者要注意社交媒體帳戶的安全(例如定期更改密碼及使用足夠複雜的密碼)，以便防止未經批准的存取。

11. 使用者不要發表:

    a. 任何可能損害港發聲譽、對港發失去信任或與港發利益有衝突的消息；

    b. 關於任何人的誹謗或負面的聲明或評論(包括港發的其他僱員及港發的客戶及供應商，及包括冒犯、貶低、歧視、騷擾、欺凌及恐嚇的聲明及評論);

    c. 不恰當的圖像或含不恰當內容的連結;

    d. 港發商標或標誌或提及港發品牌，除非得到批准;

    e. 私人或機密資訊，商業秘密或專有資訊(不論是否屬於或與港發的工作上有關，及包括有關港發業務非公開的資訊及財務表現)。

## 舉報負面消息

12. 如果你在社交媒體發現一些關於港發或其業務的負面或貶損的內容不要自行回應。將內容轉達部門主管以便作出決定。

## 投訴及調查

13. 使用者如果希望舉報不正當使用社交媒體(包括其他使用者違反政策)或覺得自己在社交媒體受到欺凌或騷擾可以利用港發舉報政策中的機制向部門主管投訴。
14. 當收到投訴或有人舉報疑似違反政策個案，該部門的主管會召開初步聆訊以便判斷是否有足夠理據作進一步調查。如果有足夠理據，部門主管會通知人力資源部經理。人力資源部經理在諮詢過其他人後有需要會委任調查員作進一步調查。
15. 調查員會將結果及建議向人力資源部經理及相關部門主管報告，之後經過諮詢其他人後決定所需行動，包括紀律處分。

## 紀律處分

16. 違反政策人士可能會受到紀律處分。使用者可能需要移走社交媒體內容。如未能做到已可導致紀律處分。嚴重違反政策(例如發表在財政上或聲譽上嚴重損害港發或任何員工的消息)足以構成嚴重不當行為可以即時解僱。港發亦可能採取行動追討任何損失或損害。

## 修改權利

17. 港發保留隨時修改本政策條文的權利。

## 14. 保安事件的發現、引起關注及回應

### 背景

一旦發現，所有公司機密資料違規事件應該立即報告、回應及引起關注。

### 內容

a. 員工有責任儘快向資訊持有人報告任何關乎敏感資料的保安違規事件。所有事件亦應該向資訊科技部報告。
b. 在未得管理高層同意前員工不得向第三者透露任何保安事件詳情。

## 15. 調查

### 內容

資訊科技部負責為所有報告的事件進行調查，確定成因與及找出及執行糾正行動，以便保安得以持續完善及增強。當有需要調查時，謹記收集、保存及呈上證據時依足搜集證據的規則。

## 16. 檢討、審查及監察

### 內容

資訊科技部負責確保每年會檢討本文件。並由品質部門負責審查及監察。

## 17. 運送敏感資料的規定做法

### 內容

請參考物料管理工程程序指引手冊40冊10節。

## 18. 棄置保密資料的規定做法

### 內容

請參考物料管理工程程序指引手冊40冊10節。

## 19. 遙距存取

### 內容

只有授權人士可以用遙距方式讀取公司的網絡。遙距存取提供給有正當商業上需要去交換資訊、抄寫檔案或程式、存取電腦應用程式或提供遙距支援服務的公司僱員、承辦商及商業伙伴。

使用者透過遙距存取讀取存放在辦公室網絡的資源時應該遵守遙距存取政策:

a. 雙重認證登入

b. 建議使用公司提供的設備

c. 如使用自己的設備，要確保已安裝最新的防毒軟件及修補程式

d. 遠程連接公司的網絡經過公司規定的一段靜止時間後(例如15分鐘)要暫停

e. 使用RemotePC電腦軟件或應用程式連接

## 20. 在公司以外工作的人士

### 內容

使用者當離開辦公室，包括但不只限於海外公幹，應當安全地處理內部、敏感及高度敏感的資訊。於海外公幹時，使用者應該:

a. 當不是隨身攜帶時要鎖好所有內部、敏感及高度敏感的資訊(文件抑或儲存在電子設備);
b. 不要將內部、敏感及高度敏感的資訊(文件抑或儲存在電子設備)放在無人看管的車輛或酒店房間;
c. 避免在公眾地方談論敏感及高度敏感的資訊。如果不能避免，僱員應該小心使用字眼及隨非有必要時禁止提到敏感內容;
d. 擺好設備的屏幕，防止未經授權人士偷看;
e. 如果未能在外面安全地銷毀內部、敏感及高度敏感的資訊可以回到公司時處理;
f. 儘量使用RemotePC電腦軟件或應用程式存取存放在公司網絡的資源

## 21. 可移動存儲設備

### 背景

可移動存儲設備 - 例如，外置硬碟，移動固態硬碟，USB手指，帶有存儲卡或內置記憶體的移動設備，如數碼相機，IOT設備或移動電話等。

### 內容

連接移動存儲設備到公司IT網絡會帶來網絡安全風險，如數據洩漏和惡意軟件感染。公司禁止透過移動存儲設備共享公司文件和數據，尤其是敏感和高度敏感類別，並且在可行的情況下以技術手段強制執行。

所有連接到公司IT網絡的設備（即公司提供的筆記本電腦，PC），在可行的情況下必須禁用其可連接移動存儲設備的端口（例如USB或Firewire）。 用戶應使用更安全的替代方案和公司存儲與內部和外部共享公司文件。

替代方案常見案例：

| 場景 | 業務用例 | 替代方案 |
|---|---|---|
| #1 | 內部工作文件保存/複製/傳輸/共享 | 使用公司存儲解決方案，例如微軟公司的 OneDrive / Teams Storage / SharePoint 或網絡共享文件夾。 |
| #2 | 外部工作文件共享 | 使用更安全的替代方法。（例如，加密的電子郵件，受密碼保護的附件，SFTP，OneDrive 公司等）。 |