# 佳穎精密企業股份有限公司

# 資訊安全管理辦法

1. 目的：

   規範電子郵件及網際網路的正確使用方法，並對公司之各相關電子媒體形式之管制文件、程式、圖檔、記錄等做有效保護，減少公司頻寬資源的浪費及避免資料外洩，確保資料作業內容保護，不受惡意程式與病毒破壞。

2. 依據：

   資訊管理安全政策。

3. 適用範圍：

   凡屬本公司之所有電子文件、電子郵件信箱、電腦主機設備，以及相關延伸之作業活動，皆在適用範圍內。

4. 定義：

   4.1. 主機：指網路上以各種方式提供服務給終端使用者的任一電腦設備。

   4.2. Proxy Server：代理伺服主機，可讓公司內部人員共同使用 Internet 網路資源及加快瀏覽速度。

   4.3. POP3：Post Office Protocol 為接收電子郵件之通訊協定。

   4.4. SMTP：Simple Mail Transfer Protocol 為發送電子郵件之通訊協定。

   4.5. Web Mail：使用者透過瀏覽器連到電子郵件伺服器，進行寄收電子郵件等操作。

   4.6. FTP：File Transfer Protocol 為檔案傳送之通訊協定。

   4.7. Terminal Service：提供類似 Thin Client 之操作，完全相同於公司環境之電腦桌面及速度，安全性高，無法下載任何資料於遠端設備。

   4.8. Anti-Virus Server：提供 Server 與 Client 端防毒服務的主機。

   4.9. IM：包括但不限於以下軟體 Line、WeChar、Skype、MSN、Google Talk、Yahoo!奇摩即時通、ICQ 及 QQ 等等，可即時線上傳送訊息的軟體統稱。

5. 作業權責與控制重點：

   5.1. 資訊部門：

   **應負責郵件伺服主機與 Proxy server 的運作正常。**

   **所有信件進出與網頁瀏覽，均應有紀錄可稽查。**

   **制定 Intranet 與 Internet 間的收發信件通訊規範。**

   **應有權利及義務將 Client 端電腦安裝控管軟體，並隨使用者權限與主機異動，進行資料更新，以控管公司電腦設備。**

   **應定期全面檢討資訊安全相關權限開放與回收。**

5.2. 員工：應遵守公司所制定之郵件收發與上網之政策規範，且不得擅自安裝資訊部門未授權之軟體與非法軟體。

6. 作業內容及流程：

6.1. 電子郵件：

**電子郵件信箱分為公司內部及對外的網路郵件信箱，公司員工依工作之需求可申請郵件信箱。**

**發信規範：**

6.1.1.1. 嚴禁員工使用電子郵件傳遞非公司業務相關之郵件，例如：垃圾郵件、廣告、成人郵件、執行檔(*.exe)、Media 郵件等。

6.1.1.2. 禁止員工將公司重要資料與檔案寄出，造成公司洩密事件發生，若查經屬實，依人事規章予以議處外，並需自負法律上應有之責任。

6.1.1.3. 禁止於公司內部使用 POP3 與 SMTP 的通訊協定來收發非公司提供之外部郵件信箱，以避免資訊稽核之漏洞。

6.1.1.4. 郵件的傳遞若有過大之附件時，應改以 FTP 之檔案傳輸或適當的採取壓縮檔案方式進行，以避免有塞爆對方郵件的困擾，及郵件傳輸過久時的封包遺失。

6.1.1.5. 為使線路頻寬資源與信件的佇列得以有效分配利用，資訊單位應配置合理的容量。

**收信規範：**

6.1.1.6. 嚴禁員工透過電子郵件訂閱非業務需要之郵件，例如：成人郵件、笑話等，若有同一網址連續三天郵寄非相關業務內容之郵件，則視為員工訂閱不當郵件頻道，則應依人事規章，就郵件內容予以議處。

6.1.1.7. 若員工有收到非公司業務之外部郵件，可認定為垃圾郵件者，可告知資訊部門主動預先防範過濾，以便減少不當的資訊再流傳於公司內部。

6.1.1.8. 員工有閱讀郵件，並處理歸檔之義務，分門別類將信件轉存到不同的『個人資料夾』。以避免將過多的信件留置在郵件主機信箱或同一個『個人信箱資料夾』時，而影響信件收發的效能。

**為避免增加郵件主機之資料儲存負擔，員工依以下原則設定使用權限：**

**（如有特殊需求，申請後經總經理核准後，提交資訊單位更改其設定）**

| 使用人員 | E-MAIL 空間容量 | E-MAIL 上傳單封大小 |
|---|---|---|
| 部門主管 | 20G | 20M |
| 單位主管 | 10G | 10M |
| 一般員工 | 5G | 5M |

**員工於公司內部應避免使用外部網站所提供之 Web-Mail，降低網路安全控管不完全而造成不良之後果（例如：垃圾郵件、詐騙郵件、勒索病毒。。。等等）。**

6.2. 上網規範：

**網際網路視業務需求申請開放，需經各部門主管核准後，轉至資訊部門辦理。**

**嚴禁員工上班時間使用網際網路瀏覽非工作上之業務性質的網站：**

| | | |
|---|---|---|
| **色情網站** | **政治新聞** | **賭博網站** |
| **購物網站** | 股票交易 | 交友網站 |
| **外部 WebMail** | 外部儲存空間 | |
| | | |

**員工使用網際網路時若有破壞公司商譽之行為並經查屬實，概依人事規章予以議處外，並需自負法律上應有之責任。**

6.3. 資訊系統管理：

**資訊部門應建立可分析對外收發郵件流量與紀錄內容附件之機制。此辦法於瀏覽網際網路之相關 Download 與 Upload 資料時應比照建置。**

**資訊部門應主機上統計並定期或不定期公告大郵件流量與員工上網之分析報告。如有不當使用之情形經查屬實，概依人事規章予以議處。**

**電子郵件已成商業往來之主要溝通方式，爲避免收件者以轉寄、複製等方式散佈予第三者或意圖不法之使用時，公司應在每封對外寄出之郵件上加註『保密警語』，以主動告知方式降低機密外洩之風險，保障公司之權益。**

6.4. 防毒管理：

**個人電腦硬碟資料防毒：**

6.4.1.1. 每一台電腦設備非實際工作需求時，禁止安裝可讀取外部資料之磁碟機等週邊設備。

6.4.1.2. 公司內部每一台電腦設備皆應安裝防毒軟體，並須定期更新病毒碼版本。

6.4.1.3. 非經資訊部門許可，個人電腦設備禁止使用目錄的檔案分享，以免成為防毒的缺口。

**電子郵件伺服器主機防毒：**

6.4.1.4. 包括郵件本體、共用目錄及附件檔案等皆應可偵測並清除或隔離。

6.4.1.5. 應建置可管制特定內容的垃圾郵件進出郵件伺服器主機，以免影響主機容量及頻寬。

**檔案伺服器主機防毒：**

6.4.1.6. 供使用者存放資料的儲存設備之伺服器主機，應安裝即時掃描病毒軟體，以提高資料安全性。

6.4.1.7. 每一台檔案伺服器主機都應定期更新病毒碼版本。

**網際網路閘道器防毒：提供使用者上網之 Proxy Server 應安裝可有效的過濾 HTTP 資料、攔截惡性的 JAVA 或 ACTIVE 物件、偵測和清除已知或未知的巨集病毒之防毒設備。**

**中央控管病毒碼版本的更新：為有效掌握 Client 端及 Server 端的病毒碼版本及中毒狀況，資訊單位應建置可回報狀態之機制及病毒碼版本更新自動派送功能，以期降低維護成本。**

**中毒時處理：**

6.4.1.8. 機房主機端 ： 應立即與病毒防護中心聯絡,必要時得斷絕對外網際網路等，待及下載最新病毒碼清除所有中毒主機。

6.5. 主機異常與異動：

6.6. IM 使用規範：

**IM 軟體視業務需求申請開放，申請經各部門主管核准後，轉至資訊部門辦理。**

**資訊部門應建立可分析員工上班時間使用 IM 軟體對外收發訊息內容之記錄機制。**

**員工使用 IM 軟體時若有破壞公司商譽之行為並經查屬實，概依人事規章予以議處外，並需自負法律上應有之責任。**

6.7. 保密合約簽訂：若合作廠商因討論、評估、實施或履行雙方「業務關係」而知悉取得公司文書、媒體或資料等，皆需於合作前簽訂保密合約。

7. 核決權限：

本辦法經總經理核准後公佈實施，修正時亦同。