

# 中華紙漿股份有限公司

## 資通安全管控指引

### 第一章 總則

- 第一條、 為強化公司資通安全防護及管理機制，並符合「公開發行公司建立內部控制制度處理準則」第九條使用電腦化資訊系統處理者相關控制作業，特擬定本資通安全管控指引。
- 第二條、 名詞定義
- 一、資通系統：指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統。
  - 二、資通服務：指與資訊之蒐集、控制、傳輸、儲存、流通、刪除、其他處理、使用或分享相關之服務。
  - 三、核心業務：公司維持營運與發展必要之業務。
  - 四、核心資通系統：支持核心業務持續運作必要之資通系統。
  - 五、機敏性資料：依公司業務考量，評估需保密或具敏感性之重要資料，如涉及營業秘密資料或個人資料等。

### 第二章 資通安全政策及推動組織

- 第三條、 成立資通安全推動組織，組織配置適當之人力、物力與財力資源，並指派適當人員擔任資安專責主管及資安專責人員，以負責推動、協調監督及審查資通安全管理事項。
- 第四條、 訂定資通安全政策及目標，由副總經理以上主管核定，並定期檢視政策及目標且有效傳達員工其重要性。
- 第五條、 訂定資通安全作業程序，包含核心業務及其重要性、資通系統盤點及風險評估、資通系統發展及維護安全、資通安全防護及控制措施、資通系統或資通服務委外辦理之管理措施、資通安全事件通報應變及情資評估因應、資通安全之持續精進及績效管理機制等。
- 第六條、 所有使用資訊系統之人員，每年接受資訊安全宣導課程，另負責資訊安全之主管及人員，每年接受資訊安全專業課程訓練。

### 第三章 核心業務及其重要性

- 第七條、 鑑別並定期檢視公司之核心業務及應保護之機敏性資料。
- 第八條、 鑑別應遵守之法令及契約要求。
- 第九條、 鑑別可能造成營運中斷事件之發生機率及影響程度，並明確訂定核心業務之復原時間目標(RTO)及資料復原時間點目標(RPO)，設置適當之備份機制及備援計

畫。

第十條、制定核心業務持續運作計畫，定期辦理核心業務持續運作演練，演練內容包含核心業務備援措施、人員職責、應變作業程序、資源調配及演練結果檢討改善。

#### 第四章 資通系統盤點及風險評估

第十一條、定期盤點資通系統，並建立核心系統資訊資產清冊，以鑑別其資訊資產價值。

第十二條、定期辦理資安風險評估，就核心業務及核心資通系統鑑別其可能遭遇之資安風險，分析其喪失機密性、完整性及可用性之衝擊，並執行對應之資通安全管理面或技術面控制措施等。

#### 第五章 資通系統發展及維護安全

第十三條、將資安要求納入資通系統開發及維護需求規格，包含機敏資料存取控制、用戶登入身分驗證及用戶輸入輸出之檢查過濾等。

第十四條、定期執行資通系統安全性要求測試，包含機敏資料存取控制、用戶登入身分驗證及用戶輸入輸出之檢查過濾測試等。

第十五條、妥善儲存及管理資通系統開發及維護相關文件。

第十六條、對核心資通系統辦理下列資安檢測作業，並完成系統弱點修補。

- 一、定期辦理弱點掃描。
- 二、定期辦理滲透測試。
- 三、系統上線前執行源碼掃描安全檢測。

#### 第六章 資通安全防護及控制措施

第十七條、依網路服務需要區隔獨立的邏輯網域(如：DMZ、內部或外部網路等)，並將開發、測試及正式作業環境區隔，且針對不同作業環境建立適當之資安防護控制措施。

第十八條、具備下列資安防護控制措施：

- 一、防毒軟體。
- 二、網路防火牆。
- 三、如有郵件伺服器者，具備電子郵件過濾機制。
- 四、入侵偵測及防禦機制。
- 五、如有對外服務之核心資通系統者，具備應用程式防火牆。
- 六、進階持續性威脅攻擊防禦措施。
- 七、資通安全威脅偵測管理機制(SOC)。

第十九條、針對機敏性資料之處理及儲存建立適當之防護措施，如：實體隔離、專用電腦作業環境、存取權限、資料加密、傳輸加密、資料遮蔽、人員管理及處理規範

等。

- 第二十條、 訂定到職、在職及離職管理程序，並簽署保密協議明確告知保密事項。
- 第二十一條、 建立使用者通行碼管理之作業規定，如：預設密碼、密碼長度、密碼複雜度、密碼歷程記錄、密碼最短及最長之效期限限制、登入失敗鎖定機制，並評估於核心資通系統採取多重認證技術。
- 第二十二條、 定期審查特權帳號、使用者帳號及權限，停用久未使用之帳號。
- 第二十三條、 建立資通系統及相關設備適當之監控措施，如：身分驗證失敗、存取資源失敗、重要行為、重要資料異動、功能錯誤及管理行為等，並針對日誌建立適當之保護機制。
- 第二十四條、 針對電腦機房及重要區域之安全控制、人員進出管控、環境維護(如溫度控制)等項目建立適當之管理措施。
- 第二十五條、 留意安全漏洞通告，即時修補高風險漏洞，定期評估辦理設備、系統元件、資料庫系統及軟體安全性漏洞修補。
- 第二十六條、 訂定資通設備回收再使用及汰除之安全控制作業程序，以確保機敏性資料確實刪除。
- 第二十七條、 訂定人員裝置使用管理規範，如：軟體安裝、電子郵件、即時通訊軟體、個人行動裝置及可攜式媒體等管控使用規則。
- 第二十八條、 每年定期辦理電子郵件社交工程演練，並對誤開啟信件或連結之人員進行教育訓練，並留存相關紀錄。

## 第七章 資通系統或資通服務委外辦理之管理措施

- 第二十九條、 訂定資訊作業委外安全管理程序，包含委外選商、監督管理(如：對供應商與合作夥伴進行稽核)及委外關係終止之相關規定，確保委外廠商執行委外作業時，具備完善之資通安全管理措施。
- 第三十條、 訂定委外廠商之資通安全責任及保密規定，於採購文件中載明服務水準協議(SLA)、資安要求及對委外廠商資安稽核權。
- 第三十一條、 公司於委外關係終止或解除時，確認委外廠商返還、移交、刪除或銷毀履行契約而持有之資料。

## 第八章 資通安全事件通報應變及情資評估因應

- 第三十二條、 訂定資安事件應變處置及通報作業程序，包含判定事件影響及損害評估、內外部通報流程、通知其他受影響機關之方式、通報窗口及聯繫方式。
- 第三十三條、 加入資安情資分享組織，取得資安預警情資、資安威脅與弱點資訊，如：所屬產業資安資訊分享與分析中心(ISAC)、臺灣電腦網路危機處理暨協調中心(TWCERT/CC)。
- 第三十四條、 如發生符合「臺灣證券交易所股份有限公司對有價證券上市公司重大訊

息之查證暨公開處理程序」規範之重大資安事件，應依相關規定辦理。

## 第九章 資通安全之持續精進及績效管理機制

- 第三十五條、 資通安全推動組織定期向董事會或管理階層報告資通安全執行情形，確保運作之適切性及有效性。
- 第三十六條、 定期辦理內部及委外廠商之資安稽核，並就發現事項擬訂改善措施，且定期追蹤改善情形。

## 第十章 附則

- 第三十七條、 除法令、臺灣證券交易所股份有限公司相關章則另有規定外，本指引條文屬於中華紙漿股份有限公司之資通安全最高指導原則，本公司所轄各廠及分公司可衡諸業務相關特性、規模大小及資安風險適度採行之。