

東柏資訊科技股份有限公司  
「資訊安全管理系統」  
資訊安全政策  
機密等級：公開

發行單位：資訊安全組織之 ISMS 小組  
修訂日期：2025.06.16  
版 次：1.3

使用本程序書前，請先與文件管理者確認版次。

本文件歷次變更紀錄：

版次	發行日	撰擬者或單位	說 明	核准者
1.0	2013.09.01	資訊安全組織之 ISMS 小組	核准	總經理
1.0	2013.09.01	資訊安全組織之 ISMS 小組	發行	資訊安全組織之 ISMS 小組
1.1	2013.09.26	資訊安全組織之 ISMS 小組	核准	總經理
1.1	2013.09.26	資訊安全組織之 ISMS 小組	發行	資訊安全組織之 ISMS 小組
1.2	2023.07.21	資訊安全組織之 ISMS 小組	核准	總經理
1.2	2023.07.21	資訊安全組織之 ISMS 小組	發行	資訊安全組織之 ISMS 小組
1.3	2025.06.16	資訊安全組織之 ISMS 小組	發行	資訊安全組織之 ISMS 小組

本程序書由資訊安全組織之 ISMS 小組負責維護。

本資料為東柏資訊科技股份有限公司專有之財產，非經書面許可，不准洩露或變更使用，亦不准複印、複製或轉成其他形式使用。

## 目 錄

壹、 目的 .....	1
貳、 依據 .....	1
參、 適用範圍 .....	1
肆、 資訊安全政策 (§7.3(A), A.5.1.1) .....	1
伍、 資訊安全定義 .....	1
陸、 資訊安全目標有效性量測 .....	2
柒、 風險評鑑 .....	2
捌、 權責分工 .....	2
玖、 資訊安全政策之審查及修訂 (A.5.1.2) .....	3

## 壹、目的

東柏資訊科技股份有限公司(以下簡稱本公司)為推動資訊安全管理系統(以下簡稱本系統)，建立安全及可信賴之資訊環境，確保資料、系統、設備及網路安全，特訂定本資訊安全政策(以下簡稱本政策)，以為遵循。

## 貳、依據

本政策係依據 ISO 27001:2022 國際標準資訊安全管系統之要求，並參酌 ISO 27002:2022 國際標準資訊安全管理統之作業規範及相關法令及規定而訂定之。

## 參、適用範圍

依本公司之營業特性，相關法令規範、利害關係人包含本公司各單位及相關公司外部合作廠商及客戶，為滿足各方之期待，本系統適用以上各內外部單位，客戶的資訊安全需求，並參照實際契約或 RFP 規範及氣候變遷議題相關要求。

## 肆、資訊安全政策 (§5.2, A.5.1)

防範資安事件，確保資訊安全  
維繫業務運作，維護公司信譽

## 伍、資訊安全定義

應用管理程序及安全防護技術於各項資訊作業，包含作業執行時所使用之各項資訊系統軟、硬體設備、存放各種資訊及資料之檔案媒體及經由

本資料為東柏資訊科技股份有限公司專有之財產，非經書面許可，不准洩露或變更使用，亦不准複印、複製或轉成其他形式使用。

列表機所列印之各式報表，俾能在資訊蒐集、處理、傳送、儲存及流通之過程中，確保資訊資產之完整性、可用性與機密性。

#### 陸、資訊安全目標有效性量測

相關資訊安全目標達成有效性之測量項目與方法，需經本公司 ISMS 或資訊安全相關會議討論訂定，測量結果應記錄於「資訊安全目標有效性測量結果記錄表」，每年至少隨機抽查一測試環境，進行系統異機還原之演練，並記錄其作業過程、時間及需之各項資源，將其演練結果紀錄於「T-04-14-009 備份資料還原測試紀錄單」，驗證整體結果是否符合所議定之服務等級協議(SLA)。另外，為求於資訊安全事故發生後迅速提供客戶災難復原，使其作業恢復運作，本公司將依據受委託之機關專案執行需求，配合於機關指定環境場所進行系統異機還原之演練，並記錄其作業過程、時間及需之各項資源，將其演練結果依照契約規定完整記錄後提交機關查核。

#### 柒、風險評鑑

為識別本公司各項資訊資產的潛在風險，並選擇必要之安全控制措施並持續改善，進而達到避免、轉移、降低及達到可接受風險，預防資通安全事件之威脅發生；本公司資訊資產之風險評鑑及管理方法依本系統所制訂「風險評鑑與管理程序」規範辦理。

#### 捌、權責分工

為落實執行本政策，本公司應建立資訊安全管理系統，權責劃分如下：

- 一、本公司資訊安全政策由總經理核准後發行。(A.5.1)

本資料為東柏資訊科技股份有限公司專有之財產，非經書面許可，不准洩露或變更使用，亦不准複印、複製或轉成其他形式使用。

- 二、本公司資訊推動小組統籌資訊安全政策、計畫、資源調度等事項之協調審議，由總經理指定協理 1 名為小組召集人，並擔任本公司資訊安全全長。
- 三、本公司應成立資訊安全組織，配合資訊安全需求研擬並制訂管理程序及安全防护準則，負責維持本公司資訊安全管理系統之有效運作，並將執行成果呈報本公司總經理。
- 四、本公司各部門需依資訊安全組織制定之規定，辦理相關資訊系統所使用資源之安全需求研議、使用管理及保護等事項。
- 五、資訊機密之維護及稽核等使用管理事項，由本公司具備 ISO 27001 Leader Auditor 主導稽核員資格之同仁會同相關組室負責辦理。
- 六、本公司員工、本公司辦公場所以外之系統連線使用者及承接本公司業務之廠商，應遵循本公司資訊安全管理規定。
- 七、本公司所建立之資訊安全管理制度，須依 PDCA 之管理方式進行變更，藉以有效控制一切可能由變更導致之風險。

#### 玖、資訊安全政策之審查及修訂 (A.5.1)

- 一、本政策應至少每年審查評估一次，以符合政府法令之要求，並反映資訊科技發展趨勢，確保本公司資訊安全管理作業之有效性。
- 二、如公司組織或企業流程發生重大變更或發生重大資安事故時，應審查並即時修訂本政策，以確保其持續的合宜性、適切性及有效性。

#### 壹拾、持續改善資訊安全管理制度

依本政策，每年至少一次內部稽核，藉以持續改善本公司資訊安全管理制度之適切性、充分性及有效性。

本資料為東柏資訊科技股份有限公司專有之財產，非經書面許可，不准洩露或變更使用，亦不准複印、複製或轉成其他形式使用。