



大統新創股份有限公司		文件編號	IS
文件名稱	資訊安全政策	頁次	2/4
		頁版別	C

第一章 本公司為強化資訊安全管理，確保資訊的機密性、完整性與可用性，資訊設備(包含電腦硬體、軟體、週邊)與網路系統之可靠性以及同仁對資訊安全的認知，並確保資訊資源免受任何因素之干擾、破壞、入侵或任何不利之行為與企圖，特制定本政策。

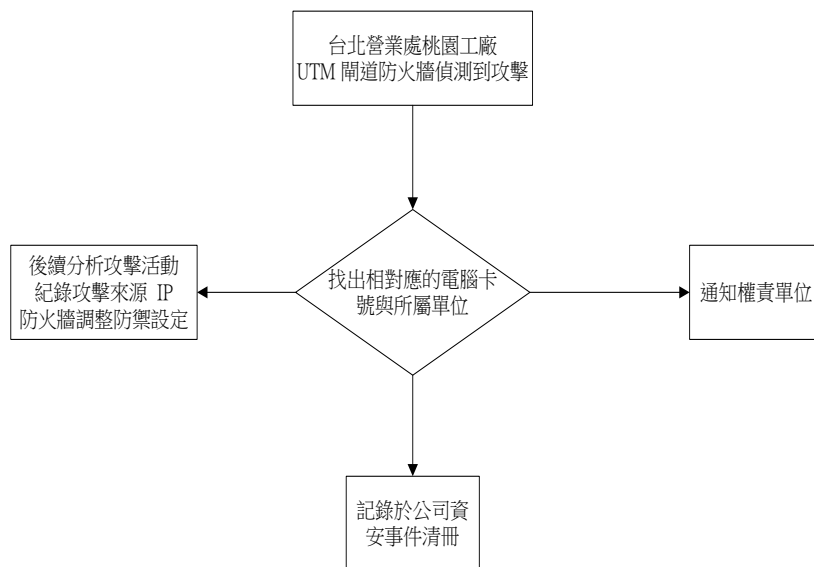
第二條 組織

為統一資訊安全管理等事項之協調、規劃、稽核與推動，由資訊課負責。

第三條 權責與分工

1. 資訊課：系統操作與維護、硬體與網路安全、資料庫與設備帳密管控、資安宣導。
2. 各單位：電腦資料保存與管理、資安認知。
3. 稽核室：公司資訊機密與安全文件稽核。

第四條 內部資安事件處理標準作業程序



內部員工電腦，如發生當機、無法開機、開機無畫面、檔案資料異常情況，當下應先將電腦電源關閉，並通知資訊課，以避免網路病毒(勒索病毒)所造成的危害。

第五條 人員管理與安全規則

1. 本公司在人員進用、工作及任務指派時，謹慎評估人員之適任性，並進行必要的考核，各單位主管人員，應負責督導所屬員工之資訊作業安全，防範不法及不當行為。
2. 針對資訊管理之工作類型需求，定期宣導資訊安全與建立員工對資安的認知，提升資訊安全水準。

第六條 電腦系統安全管理

1. 應依公司標準或權責主管訂定之資訊安全規範，研提資訊安全需求，並列入採購規格。
2. 對內部各種系統變更作業，建立管控制度，並建立紀錄以便考察。
3. 辦理資訊業務委外作業，明訂廠商之資訊安全責任與保密協定列入契約，嚴格要求廠商遵守並定期查核。

大統新創股份有限公司		文件編號	IS
文件名稱	資訊安全政策	頁次	3/4
		頁版別	C

4. 採行必要的事前預防及保護措施，偵測及防制電腦病毒及其他惡意軟體，確保系統正常運作。

#### 第七條 網路安全管理

1. 訂定電子郵件使用規定，機密性資料文件不得以電子郵件或其它電子方式傳送。
2. 與外部網路(Internet)連接之網點，以 UTM 多功能整合式防火牆設備與其它安全設施，管控外部與內部網路資料傳輸與資源的存取。
3. 為避免員工不慎違反本公司相關規定，資訊人員可以考慮以相關技術，以不干擾正常網路使用為原則下，主動管制違反本公司相關網路規定之使用者。
4. 對於開放委外廠商連線作業的資訊系統，以資料的重要性與系統價值，使用防火牆 ACL 管制與連線紀錄管制。
5. 所有員工不得透過網路洩漏公司機密，未經同意之個人隱私及公司資料與文件不得上網公布。

#### 第八條 系統存取控制

1. 離(休)職人員，應立即取消項資源之所有權限，並列入離(休)職之必要手續。人員職務調整及調動，應依系統存取，授權規定，限期調整其權限。
2. 建立使用者存取公司內部網路資源制度，所有單位必要人員如需存取內部資料與共享檔案，一律要登入帳號與密碼，密碼需定期更換。
3. 系統服務廠商以遠端登入方式進行系統維修者，加強安全控管，並記錄其存取程序，以便日後查核與追蹤。

#### 第九條 資料檔案備份管理

1. 資訊人員應定期進行資料備份，以利系統遭不可抗力之災害事故或檔案破壞時，能立即恢復運作。
2. 資訊人員備份後，應填寫【備份記錄表】，載明備份內容及日期，以確保系統資料的安全性。
3. 未經許可，個人不得備份公司資料、軟體。
4. 備份之資料由資訊課集中控管，不得擅自外借他單位。

#### 第十條 資訊資產安全管理

1. 建立公司資訊清冊清單，所有資訊硬體設備與軟體種類皆紀錄於檔案，定期更新。
2. 電腦設備財產編號，應對應所屬單位人員，以便查核。對於報廢的電腦周邊設備，統一集中置放，以便分類回收。
3. 主機重要資料的備份作業，除了本機備份，需另外做異地備份，以確保重要資料完整。

#### 第十一條 實體及環境安全管理

1. 除了資訊人員維護作業需求，機房進出管制登記，確實紀錄人員進出時間與作業。
2. 機房內部主機設備，應設置不斷電供應系統與穩壓設備，以應付停電時的處理。
3. 機房內部主機設備，需最少半年做一次維護保養，以排除內部灰塵產生的靜電而損傷零組件，增長使用壽命。

大統新創股份有限公司		文件編號	IS
文件名稱	資訊安全政策	頁次	4/4
		頁版別	C

第十二條 資訊安全政策檢討與修正

資訊單視年度重大資訊安全風險內容，進行政策修正及變更。並與每年度資訊稽核配合，進行檢討。同時依其需求，提出軟、硬體購置，加強資訊安全維護。

第十三條 本辦法自報請總經理以上主管核准後實施，修正時亦同。