版次	茂生農經股份有限公司	CM01038
1.0	資訊安全政策	106/1/26

一、前言

為確保本公司之資料、資訊、設備、人員、網路等重要資訊資產之機密性、完整性與可用性，特訂定本公司「資訊安全政策」。

二、適用範圍

舉凡本公司相關的資訊紀錄、實體環境、機器設備、軟／硬體、人員(含外包廠商)與程序均應遵守本資訊安全政策。

三、名詞定義

3.1 資料(Data)：

用於溝通、說明或處理事情、觀念或指示等正式表達形式。例如網路流量(未經分析過的)、專案實際執行狀況報告等。

3.2 資訊(Information)：

有意義的資料，資料的使用意義或經過整理分析彙總的資 料，以多種方式呈現，如以印刷品、手寫稿或電子方式等保存；以郵件、電子郵件、影片播放或口語等傳遞，如契約、設計文件、訓練教材、典章制度等。

3.3 資訊系統(Information System)：

為了支援決策和組織控制而收集(或獲取)、處理、存儲、分配資訊的一組相互關聯的元件。

3.4 安全(Security)：

對資產被竊、系統無法使用或機密資訊外洩等風險，限制在可承受範圍內之所有措施。

3.5 資訊安全(Information Security)：

確保持續營運、降低損失、提高投資效益的所有措施。舉凡與資訊相關的人、事、物均是資訊安全涵蓋的範圍，如電腦設備、規劃／管理／使用／操作系統的人員、作業流程均包含在內。資訊安全具有下列特性：

3.5.1 機密性(Confidentiality)：

確保只有獲得授權者才可存取資訊，處理、傳輸、儲存都不會洩漏資訊。

3.5.2 完整性(Integrity)：

確保資訊及系統未遭到惡意的竄改或變更，保持資訊與系統的完整性。

3.5.3 可用性(Availability)：

確保獲得授權的使用者可以取得資訊。

3.6 阻斷服務(Denial of Service)

妨礙存取資訊或延遲操作時間。

3.7 威脅(Threat)

任何事件有潛在的機會經由非法存取、破壞、洩密、竄改資料或阻斷服務(Denial of Service)式攻擊，而造成系統傷害者稱之。威脅來

源有二：

3.7.1 人為因素：如非法竊取、使用與駭客行為等。

3.7.2 天然災害：如水災、地震、颱風及不可抗拒因素等。

3.8 脆弱性(點)(Vulnerability)

是系統的弱點，而此弱點是指在系統安全開發之各階段(需求、設計、施工與運轉)，被利用會造成違反資通安全政策的結果，例如：

3.8.1 網路環境任何進入點、伺服器、Active X 或 Java Applet。

3.8.2 任何安全保護措施：如門禁系統、帳號密碼等。

3.9 風險評鑑(Risk Assessment)

是釐清資訊與資訊系統所可能遭遇到的威脅與脆弱性發生的可能性、分析相關的衝擊(Impacts)以及決定風險等級的程序，是風險管理(Risk Management)的一部份。

3.10 風險管理(Risk Management)

是一持續進行的程序，經由分析威脅、脆弱性與對業務的衝擊影響，進而選取合適且具成本/效益的控制點，以降低資訊與資訊系統的風險，以達到維持組織可承受的風險等級。

四、資訊安全政策與目標

4.1 為配合本公司之經營理念，訂定本公司的資訊安全政策聲明，公司人員需閱讀個人資料保護之管理辦法及資訊安全政策，確保資訊資產受適當之保護，防止資訊安全事件對資訊資產所造成之損害。符合政府資訊安全相關政策、規定以及相關法令要求。確保資訊業務持續運作與永續經營。

4.2 資訊安全目標

4.2.1 確保資訊安全之機密性、完整性與可用性，並保障使用者資料隱私之安全。

4.2.2 保護個人隱私資訊之安全，確保資訊需經授權人員才可存取資訊。

4.2.3 保護個人隱私資訊之安全，避免未經授權的修改。

4.2.4 確保各項業務服務之執行符合相關法令或法規之要求。

五、人員管理與責任及教育訓練

5.1 員工應遵守法規與公司內各項資訊安全規定。

5.2 員工有參加本公司舉辦各類資訊安全宣導教育之義務。

5.3 員工發現資訊安全事件時，應儘速通報並協助處理資訊安全事件。

六、網路安全

6.1 每周不定期監測所有網路設備是否正常運作。

6.2 非資訊單位許可，員工不得私自架設網路主機與設備。

6.3 若有遠端連線的需求，需經申請並核准後開放遠端登入系統。

6.4 各項網路服務之使用應依據資訊安全政策執行，關閉不必要之網路服務，如須裝置並提供其它網路服務應提出申請並於核准後開放。

七、主機系統安全

8.1 公司電腦軟體一律要經固定資產採購辦法取得。

8.2 非工務相關各項軟體不得安裝。

8.3 用戶端電腦無本機系統管理員權限，以利安全管制

8.4 登入密碼管制:

8.4.1 每180天須要更換一次密碼。

8.4.2 密碼長度必須大於六碼。

8.5 為確保作業系統平台及資料庫之安全，各主機應安裝最新版的病毒碼並定期更新作業系統修正程式(WINDOWS)

8.7 機房主機應進行例行性檢查並登記

九、委外管理

9.1 為提高委外作業安全，應要求廠商簽署保密協議書

9.2 委外廠商應遵守公司相關資料安全等相關管理規定並明定於保密協議書內

十、實體安全

10.1 若外一部人員或單位內部未具機房或管制場所進出權限之人員，因執行業務需求進入該場所時，應指派人員隨行並填寫「電腦室進出登記表」後方可進出，並上鎖管制人員進出。

10.2 為確保相關設施安全，非單位指定人員不得擅自進入機房或使用相關資訊設備。

10.3 於單位安全區域與辦公室內需隨時注意身分不明或可疑的人員。發現不明身分之人員時，需主動詢問並儘速通知相關單位進行處理。

10.4 機房應設置滅火器

10.5 設備之管理、報廢應遵守固定資產管理辦法

十一、應用系統安全

11.1 為確保應用系統開發、測試、上線及維護之安全，所有系統開發應依內部控制制度進行程式規格確認與測試後始可上線。

11.2 應設製系統測試環境供未完成測試之系統能依此環境進行測試

十二、存取安全

12.1 為避免資訊資產因未授權之存取而使機密性或敏感性資料遭不當使用，帳號申請須核准後開立(含遠端登入系統、電子郵件等有關資訊系統之帳號申請)。

12.2 加強使用者通行密碼管理(至少六碼)，使用者通行密碼之更新，最長以不超過 180 天為原則。

12.3 對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，並只允許固定單一 IP。

12.4 建立資訊安全稽核制度，定期或不定期進行資訊安全稽核作業。

12.5 帳號開立完成後以電話通知，並告知『公司資訊安全政策』，及『個人資料保護之管理辦法』。

十三、資訊安全事件管理

13.1 接獲其他單位檢舉通知資訊安全事件通知後，資訊課將立即管制異常的主機之網路連線。

13.2 情節重大者，聯絡該 IP 使用者通知該主管，給予正常的法律認知後，確認問題已經處理後，方能解除對違規主機之網路封鎖。

13.3 其他資安事件導致主機中斷之處理應依據本公司所訂之『資訊設備災害復原計劃』辦理通報與事件管理。

十四、業務永續運作管理

為避免資訊資產遭受災害而營響業務永續運作，本公司訂定『資訊設備災害復計劃』並定期演練。

十五、資訊安全政策之修訂

本資訊安全政策呈奉 總經理核定後發布實施，修訂時亦同。

十六、變更紀錄

版次	修訂內容	制訂日期
1.0	新制定	106/01/26