天仁茶業股份有限公司
資訊安全暨風險管理辦法

壹、資通安全政策及目標

一、資訊安全對象與範圍

1. 對象：包括本公司全體員工，客戶，供應商和股東以及營運相關資訊軟硬體設備。
2. 範圍：為確保本公司資訊安全，制定相關規章制度，應用技術和數據安全標準制定，並納入管理運作體系，以保障員工，供應商和客戶進行業務接洽時之隱私權保護與資訊安全維護。

二、資通安全政策

為使本公司業務於安全營運基礎上順利運作，防止資訊或資通系統受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，並確保其機密性、完整性及可用性，特制訂本政策如下，供全體同仁遵循：

1. 應建立資通安全風險管理機制，定期因應內外在資通安全情勢變化，檢討資通安全風險管理之有效性。
2. 應保護機敏資訊及資通系統之機密性與完整性，避免未經授權的存取與竄改。
3. 應強固核心資通系統之韌性，確保公司業務持續營運。
4. 應因應資通安全威脅情勢變化，辦理資通安全教育訓練，以提高本公司同仁之資通安全意識，本公司同仁亦應確實參與訓練。
5. 針對辦理資通安全業務有功人員應進行獎勵。
6. 勿開啟來路不明或無法明確辨識寄件人之電子郵件。
7. 禁止多人共用單一資通系統帳號。

三、資通安全目標

1. 公司營運業務持續運作，且本公司提供的資訊服務可穩定使用
2. 確保本公司所保管的資訊資產之機密性、完整性與可用性，並保障人員資料之隱私。
3. 達成資通安全責任等級分級之要求，並降低遭受風險之威脅。
4. 提升人員資安防護意識，定期進行社交工程演練與資安宣導。

四、資通安全政策及目標之核定程序

資通安全政策由本公司財務暨行政群副總經理核定。

五、資通安全政策及目標之宣導

本公司之資通安全政策及目標應每年透過教育訓練、內部會議、張貼公告等方式，向公司內所有人員進行宣導，並檢視執行成效。

六、資通安全政策及目標定期檢討程序

資通安全政策及目標應定期檢討其適切性。

貳、資通安全推動組織

為推動本公司資通安全相關政策、落實資通安全事件通報及相關應變處理，由財務暨行政群副總經理成立資通安全推動小組。資通安全推動小組工作職掌如下:

1. 資通安全政策及目標之研議。
2. 訂定公司資通安全相關規章與程序、制度文件，並確保相關規章與程序、制度合乎法令及契約之要求。
3. 傳達公司資通安全政策與目標。
4. 資通安全相關規章與程序、制度之執行。
5. 資訊及資通系統之盤點及風險評估。
6. 資料及資通系統之安全防護事項之執行。
7. 資通安全事件之通報及應變機制之執行。
8. 其他資通安全事項之規劃。

參、專責人力及資源之配置

本公司依上市上櫃公司資通安全管控指引規定，屬資通安全責任等級第二級，最低應設置資安專責主管及至少一名資安專責人員。

資通安全專責主管一人，負責推動資通系統防護需求分級、資通安全管理系統導入及驗證、內部資通安全稽核、公司資安治理成熟度評估及教育訓練等業務之推動。

資通安全專責人員一人，負責資通安全監控管理機制、政府組態基準導入，資通安全防護設施建置及事件通報及應變業務之推動。

本公司之承辦單位於辦理資通安全人力資源業務時，應加強資通安全人員之培訓，並提升公司內資通安全專業人員之資通安全管理能力。相關單位於辦

理資通安全業務時，如資通安全人力或經驗不足，得洽請相關學者專家或專業機構提供顧問諮詢服務。

本公司負責重要資通系統之管理、維護、設計及操作之人員， 應妥適分工，分散權責，若負有機密維護責任者，應簽屬書面約定，並視需要實施人員輪調，建立人力備援制度。

肆、資通安全風險評估

1. 本公司應每年針對資訊及資通系統資產進行風險評估。
2. 執行風險評估時應參考「上市上櫃公司資通安全管控指引」訂定。
3. 本公司應每年分別就機密性、完整性、可用性、法律遵循性等構面評估自行或委外開發之資通系統防護需求分級。

伍、資通安全防護及控制措施

本公司依據前條資通安全風險評估結果、自身資通安全責任等級之應辦事項及核心資通系統之防護基準，實行相關之防護及控制措施如下:

一、資訊及資通系統之管理

（一）資訊及資通系統之保管

1. 資訊及資通系統管理人應確保資訊及資通系統已盤點造冊並適切分級，並持續更新以確保其正確性。
2. 資訊及資通系統管理人應確保資訊及資通系統被妥善的保存或備份。
3. 資訊及資通系統管理人應確保重要之資訊及資通系統已採取適當之存取控制政策。

（二）資訊及資通系統之使用

1. 本公司同仁使用資訊及資通系統前應經其管理人授權。
2. 本公司同仁使用資訊及資通系統時，應留意其資通安全要求事項，並負對應之責任。
3. 本公司同仁使用資訊及資通系統後，應依規定之程序歸還，確保相關資訊已正確移轉，並安全地自原設備上抹除。
4. 非本公司同仁使用本公司之資訊及資通系統，應確實遵守本公司之相關資通安全要求，且未經授權不得任意複製資訊。
5. 對於資訊及資通系統，宜識別並以文件記錄及實作可被接受使用之規則。

（三）資訊及資通系統之刪除或汰除

1. 資訊及資通系統之刪除或汰除前，應評估公司是否已無需使用，或是否已妥

善移轉或備份。

2. 資訊及資通系統之刪除或汰除時宜加以清查，以確保所有機敏性資訊及具使用授權軟體已被移除或安全覆寫。
3. 具機敏性之資訊或具授權軟體之資通系統，宜採取實體銷毀，或以毀損、刪除或覆寫之技術，使原始資訊無法被讀取，並避免僅使用標準刪除或格式化功能。

二、存取控制與加密機制管理

（一）網路安全控管

1. 本公司之網路區域劃分如下：
   (1) 外部網路(Wide Area Network, WAN)：對外網路區域，連接外部廣網路。
   (2) 非軍事區(DMZ)：放置公司對外服務伺服器之區段。
   (3) 內部區域網路（Local Area Network, LAN）：公司內部單位人員及內部伺服器使用之網路區段。
2. 外部網路、非軍事區及內部區域網路間連線需經防火牆進行存取控制，非允許的服務與來源不能進入其他區域。
3. 應定期檢視防火牆政策是否適當，並適時進行防火牆軟、硬體之必要更新或升級。
4. 對於通過防火牆之來源端主機 IP 位址、目的端主機 IP 位址、來源通訊埠編號、目的地通訊埠編號、通訊協定、登入登出時間、存取時間以及採取的行動，均應予確實記錄。
5. 本公司內部網路之區域應做合理之區隔，使用者應經授權後在授權之範圍內存取網路資源。
6. 對網路系統管理人員或資通安全人員的操作，均應建立詳細的紀錄。並應定期檢視網路安全相關設備設定規則與其日誌紀錄，並檢討執行情形。
7. 使用者應依規定之方式存取網路服務，不得於辦公室內私裝電腦及網路通訊等相關設備。
8. 網域名稱系統(DNS)防護
   (1) 一般伺服器應關閉 DNS 服務，防火牆政策亦應針對 DNS 進行控管，關閉不需要的 DNS 服務存取。
   (2) DNS 伺服器應經常性進行弱點漏洞管理與修補、落實存取管控機制。
   (3) 內部主機位置查詢應指向公司內部 DNS 伺服器。
9. 無線網路防護
   (1) 機密資料原則不得透過無線網路及設備存取、處理或傳送。
   (2) 無線設備應具備安全防護機制以降低阻斷式攻擊風險，且無線網路之安全防護機制應包含外來威脅及預防內部潛在干擾。
   (3) 行動通訊或紅外線傳輸等無線設備原則不得攜入涉及或處理機密資料之區

域。

(4) 用以儲存或傳輸資料且具無線傳輸功能之個人電子設備與工作站，應安裝防毒軟體，並定期更新病毒碼。

（二）資通系統權限管理

1. 本公司之資通系統應設置通行碼管理，通行碼之要求需滿足：

(1) 通行碼長度 8 碼以上。
(2) 通行碼複雜度應包含英文大寫小寫、特殊符號或數字三種以上。
(3) 使用者應定期更換通行碼。

2. 使用者使用資通系統前應經授權，並使用唯一之使用者ID，除有特殊營運或作業必要經核准並紀錄外，不得共用ID。
3. 使用者無繼續使用資通系統時，應立即停用或移除使用者 ID，資通系統管理者應定期清查使用者之權限。

（三）特權帳號之存取管理

1. 資通系統之特權帳號請應經正式申請授權方能使用，特權帳號授權前應妥善審查其必要性，其授權及審查記錄應留存。
2. 特權帳號不得共用。
3. 特權帳號宜指派與該使用者日常公務使用之不同使用者ID。
4. 特權帳號應妥善管理，並應留存特殊權限帳號之使用軌跡。
5. 資通系統之管理者應定期清查系統特權帳號並劃定特權帳號逾期之處理方式。

（四）加密管理

1. 本公司之機密資訊於儲存或傳輸時應進行加密。
2. 本公司之加密保護措施應遵守下列規定：

(1) 應落實使用者更新加密裝置並備份金鑰。
(2) 應避免留存解密資訊。
(3) 一旦加密資訊具遭破解跡象，應立即更改之。

三、作業與通訊安全管理

（一）防範惡意軟體之控制措施

1. 本公司之主機及個人電腦應安裝防毒軟體，並時進行軟、硬體之必要更新或升級。

(1) 經任何形式之儲存媒體所取得之檔案，於使用前應先掃描有無惡意軟體。
(2) 電子郵件附件及下載檔案於使用前，宜於他處先掃描有無惡意軟體。
(3) 確實執行網頁惡意軟體掃描。

2. 使用者未經同意不得私自安裝應用軟體，管理者並應定期針對管理之設備進行軟體清查。
3. 使用者不得私自使用已知或有嫌疑惡意之網站。
4. 設備管理者應定期進行作業系統及軟體更新，以避免惡意軟體利用系統或軟體漏洞進行攻擊。

（二）遠距工作之安全措施

1. 本公司資通系統之操作及維護以現場操作為原則，避免使用遠距工作，如有緊急需求時，應申請並經資通安全推動小組同意後始可開通。
2. 資通安全推動小組應定期審查已授權之遠距工作需求是否適當。
3. 針對遠距工作之連線應採適當之防護措施(並包含伺服器端之集中過濾機制檢查使用者之授權)，並且記錄其登入情形。

（三）電子郵件安全管理

1. 本公司人員到職後應經申請方可使用電子郵件帳號，並應於人員離職後刪除電子郵件帳號之使用。
2. 電子郵件系統管理人應定期進行電子郵件帳號清查。
3. 電子郵件伺服器應設置防毒及過濾機制，並適時進行軟硬體之必要更新。
4. 使用者使用電子郵件時應提高警覺，建議使用純文字模式瀏覽， 避免讀取來歷不明之郵件或含有巨集檔案之郵件。
5. 原則不得電子郵件傳送機密性或敏感性之資料，如有業務需求者應依相關規定進行加密或其他之防護措施。
6. 使用者不得利用公司所提供電子郵件服務從事侵害他人權益或違法之行為。
7. 使用者應確保電子郵件傳送時之傳遞正確性。
8. 使用者使用電子郵件時，應注意電子簽章之要求事項。
9. 本公司應定期舉辦電子郵件社交工程演練，並檢討執行情形。

（四）確保實體與環境安全措施

1. 資料中心及電腦機房之門禁管理

(1) 公司人員或來訪人員應申請及授權後方可進入資料中心及電腦機房，管理者並應定期檢視授權人員之名單。
(2) 人員進入管制區應配載身分識別之標示，並隨時注意身分不明或可疑

人員。

(3) 僅於必要時准許外部支援人員進入資料中心及電腦機房。

(4) 人員及設備進出資料中心及電腦機房應留存記錄。

2. 資料中心及電腦機房之環境控制

(1) 資料中心及電腦機房之空調、電力應建立備援措施。

(2) 資料中心及電腦機房之管控：

A. 資料中心及電腦機房應安裝之安全偵測及防護措施，包括熱度及煙霧偵測設備、火災警報設備、溫濕度監控設備、漏水偵測設備、入侵者偵測系統，以減少環境不安全引發之危險。

B. 各項安全設備應定期執行檢查、維修，並應定時針對設備之管理者進行適當之安全設備使用訓練。

3. 辦公室區域之實體與環境安全措施

(1) 應考量採用辦公桌面的淨空政策，以減少文件及可移除式媒體等在辦公時間之外遭未被授權的人員取用、遺失或是被破壞的機會。

(2) 文件及可移除式媒體在不使用或不上班時，應存放在櫃子內。

(3) 機密性及敏感性資訊，不使用或下班時應該上鎖。

(4) 機密資訊或處理機密資訊之資通系統應避免存放或設置於公眾可接觸之場域。

(5) 顯示存放機密資訊或具處理機密資訊之資通系統地點之通訊錄及內部人員電話簿，不宜讓未經授權者輕易取得。

(6) 資訊或資通系統相關設備，未經管理人授權，不得被帶離辦公室。

（五）資料備份

1. 重要資料及核心資通系統應進行資料備份，其備份之頻率應滿足復原時間點目標之要求，並執行異地存放。
2. 本公司應定期確認核心資通系統資料備份之有效性，且測試該等資料備份時，宜於專屬之測試系統上執行，而非直接於覆寫回原資通系統。
3. 敏感或機密性資訊之備份應加密保護。

（六）媒體防護措施

1. 使用隨身碟或磁片等存放資料時，具機密性、敏感性之資料應與一般資料分開儲存，不得混用並妥善保管。
2. 資訊如以實體儲存媒體方式傳送，應留意實體儲存媒體之包裝，選擇適當人員進行傳送，並應保留傳送及簽收之記錄。
3. 為降低媒體劣化之風險，宜於所儲存資訊因相關原因而無法讀取前，將

其傳送至其他媒體。

4. 對機密與敏感性資料之儲存媒體實施防護措施，包含機密與敏感之紙本或備份磁帶，應保存於上鎖之櫃子，且需由專人管理鑰匙。

（七）電腦使用之安全管理

1. 電腦、業務系統或憑證，若超過十五分鐘不使用時，應立即登出或啟動螢幕保護功能並取出憑證。
2. 禁止私自安裝點對點檔案分享軟體及未經合法授權軟體。
3. 連網電腦應隨時配合更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。
4. 筆記型電腦及實體隔離電腦應定期以人工方式更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。
5. 下班時應關閉電腦及螢幕電源。
6. 如發現資安問題，應主動循公司之通報程序通報。
7. 支援資訊作業的相關設施如影印機、傳真機等，應安置在適當地點，以降低未經授權之人員進入管制區的風險，及減少敏感性資訊遭破解或洩漏之機會。

（八）行動設備之安全管理

1. 機密資料不得由未經許可之行動設備存取、處理或傳送。
2. 機敏會議或場所不得攜帶未經許可之行動設備進入

（九）即時通訊軟體之安全管理

1. 使用即時通訊軟體傳遞公司內部公務訊息，其內容不得涉及機密資料。

四、業務持續運作演練

本公司應針對核心資通系統制定業務持續運作計畫，並定期辦理核心資通系統持續運作演練。

五、執行資通安全健診

本公司應定期辦理進行安全弱點掃描， 並檢討執行情形

六、資通安全防護設備

1. 本公司應建置防毒軟體、網路防火牆、電子郵件過濾裝置，持續使用並適時進行軟、硬體之必要更新或升級。
2. 資安設備應定期備份日誌紀錄，定期檢視並由主管複核執行成果，並檢討執行情形。

陸、資通安全事件通報應變機制

1. 資訊安全事件包括：系統被入侵、對外攻擊、針對性攻擊、散播惡意程式、中繼站、電子郵件社交工程攻擊、垃圾郵件、命令或控制伺服器、殭屍電腦、惡意網頁、惡意留言、網頁置換、釣魚網頁、個資外洩以及通訊中斷…等。

2. 資訊安全事件等級，由輕微至嚴重區分等級如下：

(1)符合下列任一情形者，屬1級事件：

非核心業務資料遭洩漏。
非核心業務系統或資料遭竄改。
非核心業務運作遭影響或短暫停頓。

(2)符合下列任一情形者，屬2級事件：

非屬機密級或敏感之核心業務資料遭洩漏。
核心業務系統或資料遭輕微竄改。
核心業務運作遭影響或系統效率降低，於可容忍中斷時間內回復正常運作。

(3)符合下列任一情形者，屬3級事件：

機密級或敏感公務資料遭洩漏。
核心業務系統或資料遭嚴重竄改。
核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作。

(3) 符合下列任一情形者，屬4級事件：

公司機密資料遭洩漏。
公司重要資訊基礎建設系統或資料遭竄改。
公司重要資訊基礎建設運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作。

3. 任何人發現異常情況或疑似資安事件，應立即向資訊部資安人員通報，資訊部門應儘速處理並研判事件等級。

4. 資安人員當發生研判事件等級3以上之事件，立即通報資訊權責主管及管理單位最高主管，應儘快召集會議研商處理的方式。

5. 公司發生無法處理之資通安全事件，應通報資通安全廠商協助處理。

6. 資安事件須於發生後1小時內進行通報，1、2 級事件於事件發生後72小時內處理完成(包括通報與應變)，3、4 級事件於事件發生後36小時內完成

柒、資通安全情資之評估及因應

強化上市公司資安情資共享，提升資安事件通報應變能量，本公司已成為台灣電腦網路危機處理暨協調中心(TWCERT/CC)會員，該中心可提供資安事件諮詢及協調服務，使上市公司有效接收及傳遞資安情資，達橫向資安聯防目標，提升資安防護能量。

接獲資通安全情資，應評估該情資之內容，並視其對影響、可接受之風險及資源，決定最適當之因應方式，必要時得調整資通安全維護計畫之控制措施，並做成紀錄。

捌、資通系統或服務委外辦理之管理

本公司委外辦理資通系統之建置、維運或資通服務之提供時，應考量受託者之專業能力與經驗、委外項目之性質及資通安全需求，選任適當之受託者，並監督其資通安全維護情形。

一、選任受託者應注意事項

1. 受託者辦理受託業務之相關程序及環境，應具備資通安全管理措施或通過第三方驗證。
2. 受託者應配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員。

二、監督受託者資通安全維護情形應注意事項

1. 受託者執行受託業務，違反資通安全相關法令或知悉資通安全事件時，應立即通知委託公司及採行之補救措施。
2. 委託關係終止或解除時，應確認受託者返還、移交、刪除或銷毀履行委託契約而持有之資料。
3. 受託者應採取之其他資通安全相關維護措施。
4. 本公司應定期或於知悉受託者發生可能影響受託業務之資通安全事件時，以稽核或其他適當方式確認受託業務之執行情形。

玖、資通安全教育訓練及辦理

本公司資安及資訊人員每年至少二名人員接受12小時以上之資安專業課程訓練或資安職能訓練。

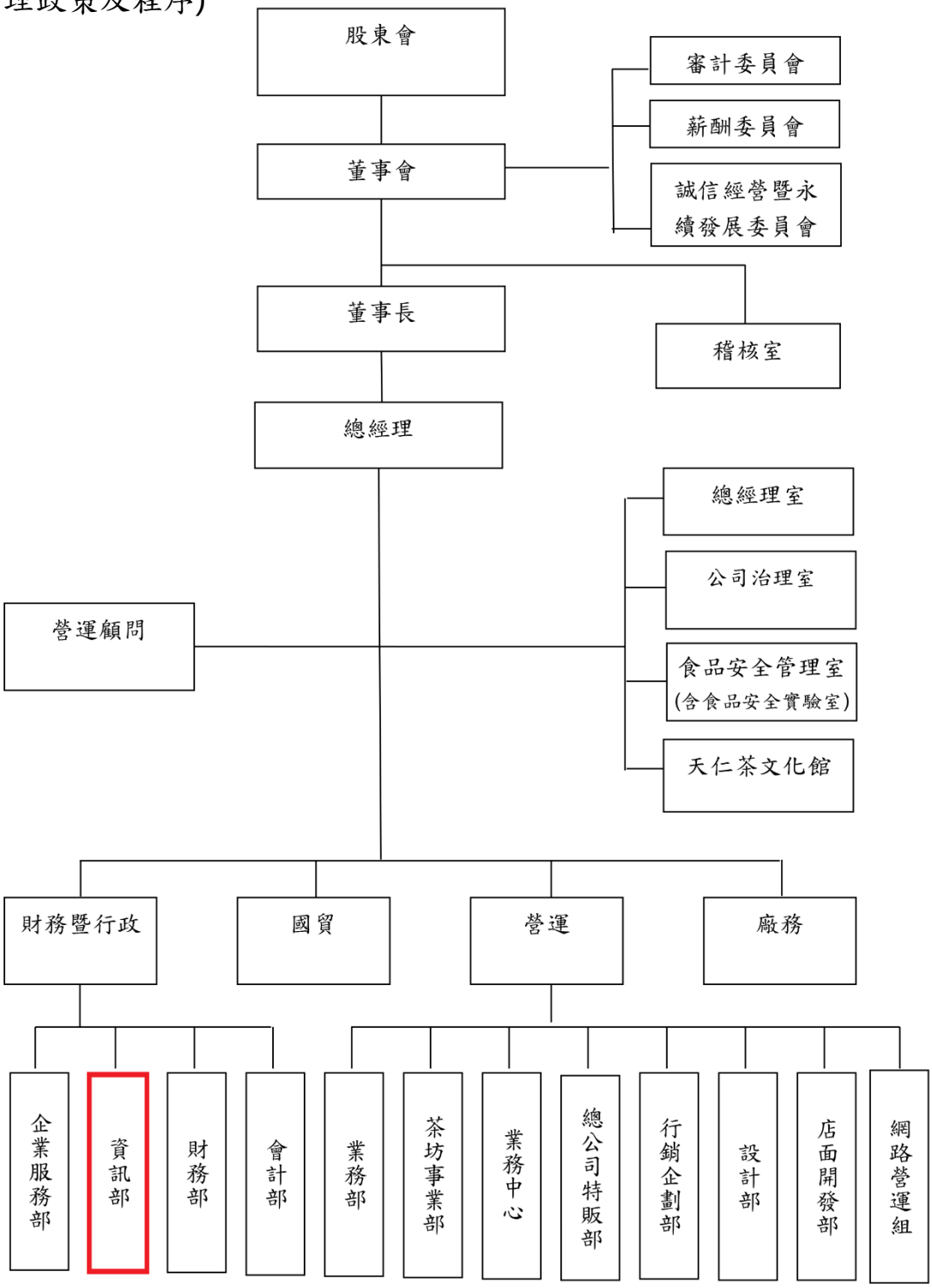
本公司之一般使用者與主管，每人每年接受3小時以上之一般資通安全教育訓練。

承辦單位應考量管理、業務及資訊等不同工作類別之需求，擬定資通安全認知宣導，以建立員工資通安全認知，提升公司資通安全水準，並應保存相關之資通安全認知宣導及教育訓練紀錄。

資通安全教育及訓練之政策，除適用所屬員工外，對公司外部的使用者，亦應一體適用。

(資訊安全暨風險管理 控制組織圖)詳如下頁所示

天仁茶業股份有限公司

資訊安全暨風險管理 控制組織圖

(本圖係明確資訊安全暨風險管理中，明確標註「**資訊部**」於公司組織內部的管理位階， 其他部門名稱請簡要方式列入，其職能詳見本公司組織圖及風險管理政策及程序)