資通安全作業程序

壹、依據及目的 5
貳、適用範圍 5
參、核心業務及重要性 5
1、 核心業務及重要性： 5
肆、資通安全政策及目標 5
1、 資通安全政策 5
2、 資通安全目標 6
3、 資通安全政策及目標之核定程序 6
4、 資通安全政策及目標之宣導 6
5、 資通安全政策及目標定期檢討程序 6
伍、資通安全推動組織 6
1、 資通安全推動小組 7
(1).組織 7
(2)分工及職掌 7
陸、專職（責）人力及經費配置 8
1、 專職（責）人力及資源之配置 8
2、 經費之配置 9
柒、資通系統及資訊之盤點 9
1、 資通系統及資訊之盤點 9
捌、資通安全風險評估 10
1、 資通安全風險評估 10
玖、資通安全防護及控制措施 10
1、 資通系統及資訊之管理 10
(1)資通系統及資訊之保管 10
(2)資通系統及資訊之使用 10
(3)資通系統及資訊之刪除或汰除 11
2、 存取控制與加密機制管理 11
(1)網路安全控管 11
(2)資通系統權限管理 12
(3)特權帳號之存取管理 12
3、 作業與通訊安全管理 12
(1)防範惡意軟體之控制措施 12

(2)電子郵件安全管理.....13
(3)確保實體與環境安全措施.....13
(4)資料備份.....14
(5)電腦使用之安全管理.....14
4、 執行資通安全檢查.....15
5、 資通安全防護設備.....15
壹拾、資通安全事件通報、應變及演練相關機制.....15
壹拾壹、資通安全情資之評估及因應.....15
壹拾貳、資通系統或服務委外辦理之管理.....15
1、 監督受託者資通安全維護情形應注意事項.....15
壹拾參、資通安全教育訓練.....16
1、 資通安全教育訓練要求.....16
壹拾肆、資通安全維護計畫及實施情形之持續精進及績效管理機制.....16
1、 資通安全維護計畫之實施.....16
2、 資通安全維護計畫實施情形之稽核機制.....16
(1)稽核機制之實施.....16
(2)稽核改善報告.....17
3、 資通安全維護計畫之持續精進及績效管理.....17
壹拾伍、相關法規、程序及表單.....18
1、 相關法規及參考文件.....18
2、 附件表單.....18

依據及目的

本程序為強化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，依據上市上櫃公司資通安全管控指引訂定。

適用範圍

本程序適用範圍涵蓋全公司。

核心業務及重要性

1、 核心業務及重要性：

本公司之核心業務及重要性如下表：

核心業務	核心~~業務~~資通系統	重要性說明	業務失效影響說明	最大可容忍中斷時間	業務之復原時間目標	資料復原時間點目標
業務與財會作業	ERP 系統	■公司維運必要 ■具公司機敏資料	公司財會及業務作業，如應收應付銷售訂單無法登打。	48Hr	36Hr	24Hr
人事薪資作業	HRM 系統	■公司維運必要 ■具公司機敏資料	公司人事薪資相關作業無法登打及計薪。	48Hr	36Hr	24Hr

核心業務資通安全政策及目標

1、 資通安全政策

為使本公司業務順利運作，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（Confidentiality)、完整性（Integrity）及可用性（Availability)，特制訂本政策如下，以供全體同仁共同遵循：

(1) 因應資通安全威脅情勢變化，本公司同仁應定期參與資通安全相關教育訓練，以提高資通安全意識。

(2) 保護公司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) 定期進行內部稽核，確保各項作業皆能確實落實。

2、 資通安全目標

(1) 核心資通系統可用性達99.99%以上。(中斷時數/總運作時數≤0.1%)

(2) 知悉資安事件發生，能於規定的時間完成通報、應變及復原作業(年度重大事件發生<= 1)。

(3) 所有使用資訊系統之人員，每年接受資訊安全宣導資訊，另負責資訊安全專責主管及資訊安全專責人員，每年接受資訊安全專業課程訓練。

3、 資通安全政策及目標之核定程序

資通安全政策由資通安全管理單位草擬，送本公司總經理室簽陳至集團總經理核定。

4、 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，向本公司內所有人員進行宣導，並檢視執行成效。

5、 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於「資通安全管理委員會」會議中檢討其適切性。

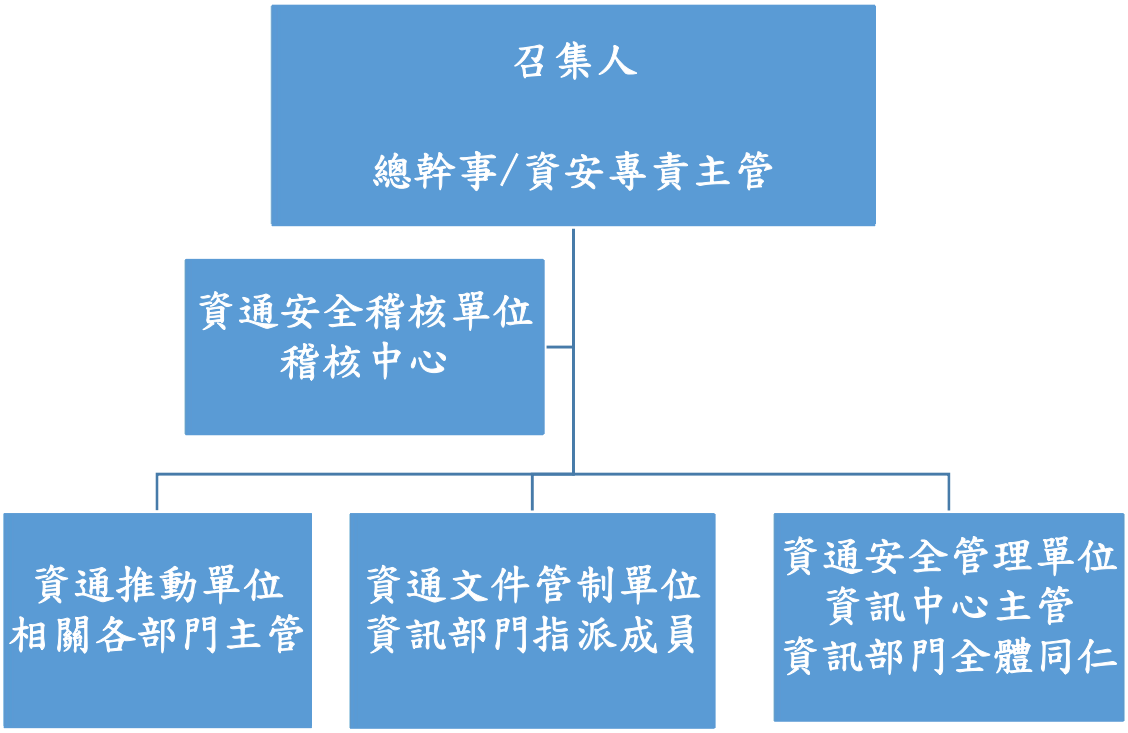
資通安全推動組織

依「上市上櫃公司資通安全管理指引」第二章之規定，本公司指派陳正煌 集團總經理為「資通安全管理委員會」召集人，洪壽隆經理為資安專責主管擔任「資通安全管理委員會」總幹事，本委員會成員，負責本公司「資通安全政策與目標」及所訂定「資通安全作業程序」之推動，協調監督及督導審查資通安全管理事項，其任務包跨定期檢視政策及目標，並有效傳達員工並認知其重要性。(是否考慮將資安專責人員也一併敘明)

每年定期召開資通安全管理委員會會議，或在內部管理階會議/董事會中提報資通安全事項執行情形，並進行管理審查。

1、 資通安全推動小組

(1) 組織



(2) 分工及職掌

本公司之資通安全推動小組依下列分工進行責任分組，並依資通安全長之指示負責下列事項，本公司資通安全推動小組分組人員名單及職掌應列冊，並適時更新之：

委員會責任	職能別說明	備註
召集人	定期檢視 政策及目標	
總幹事/資安專責主管	推動、 協調監督及審查資通安全管理事項	
資通安全稽核單位	定期審核相關資通安全執行	
資通安全管理單位		

資通文件管制單位		
資通推動單位	人事部主管，訂定到職在職離職程序集保密協定	
	採購法務委外契約管理主管，訂定相關委外辦理管理措施	
	發言人與櫃買重大訊息平台相關人員	

專職（責）人力及經費配置

1、 專職（責）人力及資源之配置

(1) 本公司依「上市上櫃公司資通安全管理指引」第二章第三條之規定，應設置資安專職（責）主管一人，資通安全專職（責）人員一人，本公司現有資通安全專責人員名單及職掌應列冊，並適時更新[1]。

(2) 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，並提升機關內資通安全專業人員之資通安全管理能力。本機關之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關（構）提供顧問諮詢服務。

(3) 資安專職（責）人員專業職能之培養(如證書、證照、培訓紀錄等)，應依據資通安全責任等級分級辦法之規定。

(4) 資安專職（責）人員總計每年應進修6Hr 以上資通安全專業課程。

(5) 專業人力資源之配置情形應每年定期檢討，並納入資通安全維護計畫持續改善機制之管理審查。

2、 經費之配置

(1)「資通安全推動小組」於規劃配置相關經費及資源時，應考量本公司之資通安全政策及目標，並提供建立、實行、維持及持續改善資通安全維護計畫所需之資源。

(2)各單位於規劃建置資通系統建置時，應一併規劃資通系統之資安防護需求，並於整體預算中合理分配資通安全預算所佔之比例。

(3)各單位如有資通安全資源之需求，應每年配合公司預算規劃期程向「資通安全推動小組」提出，由「資通安全推動小組」視整體資通安全資源進行分配，並經「資通安全推動小組召集人」核定後，進行相關之建置。

(4)資通安全經費、資源之配置情形應每年定期檢討，並納入資通安全維護計畫持續改善機制之管理審查。

資通系統及資訊之盤點

1、 資通系統及資訊之盤點

(1)本公司每年應定期盤點資訊及資通系統，並建立資訊資產清冊辦理核心資通系統及資訊資產盤點，依管理責任指定對應之資產管理人，並鑑別其資產價值。

(2)每年度應依資訊及資通系統盤點結果，製作「資產清冊」，另各單位管理之資通系統或資訊資產如有異動，應即時通知「資通安全推動小組」更新資產清冊。

資產編號	資產分類	資產名稱	資通系統名	權責單位	存放位置	數量	維護廠商	維護狀態	資產等及價值	備註

(3)資訊資產應以標籤標示於設備明顯處，並載明財產編號、保管人、等資訊。資訊及資通系統及相關資產，並應加註標示。

資通安全風險評估

1、 資通安全風險評估

(1)本公司應每年定期針對資訊及資通系統資產進行風險評估。

(2) 本公司應每年定期依據資訊及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。

2、 資通安全風險之因應

本公司完成資訊及資通系統資產風險評估後，應考量本公司可接受之風險，選擇並採行相關之防護及控制措施。

資通安全防護及控制措施

本公司依據前章資通安全風險評估結果，採行相關之防護及控制措施如下:

1、 資通系統及資訊之管理

(1) 資通系統及資訊之保管

I. 管理人應確保資通系統及資訊已盤點造冊並適切分級，並持續更新以確保其正確性。

II. 管理人應確保資通系統及資訊被妥善地保存或備份。

III. 管理人應確保重要之資通系統及機敏資料已採取適當之存取控制政策。

(2) 資通系統及資訊之使用

I. 本公司同仁使用資通系統及資訊前應經其管理人授權。

II. 本公司同仁使用資通系統及資訊時，應留意其資通安全要求事項，並負對應之責任。

III. 本公司同仁使用資通系統及資訊後，應依規定之程序歸還。資訊類資訊之歸還應確保相關資訊已正確移轉，並安全地自原設備上抹除。

IV. 非本公司同仁使用本公司之資通系統及資訊，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。

V. 對於資通系統及資訊，宜識別並以文件記錄及實作可被接受使用之規則。

VI. 本公司同仁應簽署到職、在職及離職保密協議並明確告知保密事項。

(3) 資通系統及資訊之刪除或汰除

I. 資通系統及資訊之刪除或汰除前應評估公司是否已無需使用、已妥善移轉或備份。

II. 資通系統及資訊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。

III. 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。

2、 存取控制與加密機制管理

(1) 網路安全控管

I. 本公司之網路區域劃分如下：

i. 外部網路：對外網路區域，連接外部廣網路（Wide Area Network, WAN)。

ii. 非軍事區（DMZ)：放置公司對外服務伺服器之區段。

iii. 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。

II. 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。

III. 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。

IV. 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。

V. 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。

VI. 對網路系統管理人員或資通安全主管人員的操作，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。

VII. 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。

VIII. 無線網路防護

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。

(2) 資通系統權限管理

I. 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：

i. 通行碼長度8碼以上。(可考量增加密碼長度並規定密碼複雜度)

ii. 使用者每90天應更換一次通行碼，並避免重複使用前3代已變更之密碼。

iii. 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。

iv. 依業務需要限制1天內密碼之變更次數。

v. 帳號登入進行身分驗證失敗達五次後，至少十五分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制。

vi. 若因系統限制無法設定上述密碼原則，則至少需包含長度8碼及複雜度

II. 使用者使用資通系統前應經授權，並使用唯一之使用者ID。

III. 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。

(3) 特權帳號之存取管理

I. 資通系統之特權帳號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。

II. 資通系統之特權帳號不得共用。

III. 對於特權帳號，宜指派與該使用者日常公務使用之不同使用者ID。

IV. 資通系統之特權帳號應妥善管理，並應留存特殊權限帳

號之使用軌跡。

V. 資通系統之管理者每季應清查系統特權帳號並劃定特權帳號逾期之處理方式。

3、 作業與通訊安全管理

(1)防範惡意軟體之控制措施

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

II. 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。

III. 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。

IV. 確實執行網頁惡意軟體掃描。

V. 使用者未經同意不得私自安裝應用軟體，管理者並應每半年定期針對管理之設備進行軟體清查。

VI. 使用者不得私自使用已知或有嫌疑惡意之網站。

VII. 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。

(2)遠距工作之安全措施

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，如有使用需求時，應申請並經權責主管同意後，允須開放使用。

(3)電子郵件安全管理

I. 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。

II. 電子郵件系統管理人應定期進行電子郵件帳號清查。

III. 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。

IV. 使用者使用電子郵件時應提高警覺，並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。

V. 使用者不得利用本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。

VI. 使用者應確保電子郵件傳送時之傳遞正確性。

VII. 本公司每年應定期舉辦電子郵件社交工程演練，並對勿開啟信件或連結之人員進行教育訓練，並留存相關紀錄。並檢討執行情形。

(4) 確保實體與環境安全措施

I. 資料中心及電腦機房之門禁管理

i. 資料中心及電腦機房應進行實體隔離。

ii. 公司人員或來訪人員應授權後方可進入資料中心及電腦機房，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。

iii. 人員進入管制區應配戴身分識別之標示，並隨時注意身分不明或可疑人員。

iv. 僅於必要時，得准許外部支援人員進入資料中心及電腦機房。

v. 人員及設備進出資料中心及電腦機房應留存記錄，並考量針對可攜式移動裝置(筆記型電腦、平板電到)及儲存媒體(USB、行動硬碟..等)進行安全性檢核。

II. 資料中心及電腦機房之環境控制

i. 資料中心及電腦機房之空調、電力應建立備援措施。

ii. 資料中心及電腦機房之溫濕度管控範圍應維持在20℃至27℃，相對溼度維持在40% RH 至75% RH。

iii. 資料中心及電腦機房應參考安裝之安全偵測及防護措施，包括煙霧偵測設備、火災警報設備、溫濕度監控設備、漏水偵測設備及入侵偵測系統，以減少環境不安全引發之危險。

iv. 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。

III. 辦公室區域之實體與環境安全措施

i. 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。

ii. 機密性及敏感性資訊，不使用或下班時應該上鎖。

iii. 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。

iv. 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。

(5) 資料備份

I. 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。

II. 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。

(6) 電腦使用之安全管理

I. 電腦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。

II. 禁止私自安裝點對點檔案分享軟體及未經合法授權軟體。

III. 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。

IV. 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。

V. 下班時應關閉電腦及螢幕電源。

VI. 如發現資安問題，應主動循公司之通報程序通報。

VII. 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。

VIII. 免費軟體應於軟體開發原始網站進行下載使用，若有疑慮，應與資訊中心資訊人員確認後使用，以避免安裝已遭惡意軟體植入後門程式或感染電腦病毒之軟體。

4、 系統獲取、開發及維護

(1) 於資訊及資通系統開發前，設計安全性要求，包含機敏資料存取、用戶登入資訊檢核及用戶輸入輸出之檢查過濾，並檢討執行情形。

(2) 於上線前執行安全性要求測試，包含機敏資料存取、用戶登入資訊檢核及用戶輸入輸出之檢查過濾測試，並檢討執行情形。

5、 業務持續運作演練

(1) 本公司應識別資訊及資通系統及相關資源，依據各系統等級，評估各資訊及資通系統遇到服務中斷衝擊之影響，判斷可以最大可容忍中斷時間(MTPD)，決定資通系統的目標復原時間及復原順序，已建立復原方案及備份策略。

本公司113年核心系統營運衝擊分析如下表：

核心業務	核心資通系統	業務失效影響說明	最大可容忍中斷時間
業務與財會作業	業務與財會作業	公司財會及業務作業，如應收應付銷售訂單無法登打。	48 小時
人事薪資作	人事薪資作業	公司人事薪資相關作業無法登打及計薪	48 小時

(2) 本公司應針對營運衝擊分析結果，對資訊及資通系統制定業務持續運作計畫，並每年辦理一次核心資通系統持續運作演練。

本公司113年營運持續運作計畫演練規劃如下表：

系統	演練時間	演練情境
業務與財會作業	113/12	
人事薪資作業	113/12	

6、 執行資通安全檢查

(1) 本公司每二年應辦理資通安全檢查，其至少應包含下列項

目，並檢討執行情形：

I. 網路架構檢視。

II. 使用者端電腦惡意活動檢視。

III. 伺服器主機惡意活動檢視。

IV. 檔案伺服器設定及防火牆連線設定檢視。

(2) 本公司應定期針對核心系統辦理下列資安檢測作業，並完成漏洞修補：

I. 弱點掃描。

II. 滲透測試。

III. 系統上線前執行源碼掃描安全檢測。

7、 資通安全防護設備

(1) 本公司資通設備應安裝防毒軟體，並適時進行防毒系統軟、硬體之必要更新或升級。

(2) 本公司對外網路連線應設置網路防火牆，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。

(3) 本公司應具備電子郵件過濾系統，並適時進行系統軟、硬體之必要更新或升級。

資通安全事件通報、應變及演練相關機制

1、 資通安全事件應變及演練相關機制

為即時掌控資通安全事件，並有效降低其所造成之損害，本公司應訂定資通安全事件通報、應變及演練相關機制。，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，得參考臺灣電腦網路危機處理暨協調中心（TWCERT/CC)「企業資安事件應變處理指南」。

2、 資通安全事件通報

若發生符合「財團法人中華民國證券櫃檯買賣中心對有價證券上櫃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。

資通安全情資之評估及因應

本公司接獲資通安全情資，應評估該情資之內容，並視其對本機關之影響、本機關可接受之風險及本機關之資源，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。

資通系統或服務委外辦理之管理

本公司為確保委外廠商在執行委外作業時，具備完善之資通安全管理措施，應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。

1、 委外選商與資通安全責任監督受託者資通安全維護情形應注意事項

(1) 本公司在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。

(2) 於採購文件中載明委外廠商之資通安全責任及保密規定，包含服務水準協議（SLA）、資安要求，並明確訂定對委外廠商資安稽核權。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，應立即通知委託機關及採行之補救措施。

(3) 委託關係終止或解除時，應要求受託者返還、移交、刪除或銷毀履行委託契約而持有之資料。

2、 監督管理

(1) 本公司應監督受託者之資通安全維護情形，必要時對供應商與合作夥伴進行稽核，以確保其遵循資通安全相關規範。

(2) 受託者若涉及利用非自行開發之系統或資源，應標示非自行開發之內容與其來源，並提供授權證明。

(3) 受託者在執行受託業務時，如違反資通安全相關法令或知悉資通安全事件，應立即通知本公司並採取補救措施。

3、 委外關係終止之相關規定

委託關係終止或解除時，本公司應確認受託者返還、移交、刪除或銷毀履行契約而持有之所有資料。

資通安全教育訓練

1、 資通安全教育訓練要求

本公司依「上市上櫃公司資通安全管理指引」責任等級分級屬二級，資安及資訊人員每年至少二名人員接受六小時以上之資安專業課程訓練或資安職能訓練。

2、 資通安全教育訓練辦理方式

(1) 承辦單位應於每年年終前，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及教育訓練計畫或派員接受外部單位辦理之專業資安課程，以建立員工資通安全認知，提升本公司資通安全水準，並應保存相關之資通安全認知宣導及教育訓練紀錄。

(2) 本公司資通安全認知宣導及教育訓練之內容得包含資通安全政策(含相關申請規定、人員責任及資通安全事件通報程序等)。

(3) 員工報到時，應使其充分瞭解本中心資通安全相關作業規範及其重要性。

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

資通安全維護計畫及實施情形之持續精進及績效管理機制

1、 資通安全維護計畫之實施

為落實本安全維護計畫，使本公司之資通安全管理有效運作，相關單位於訂定各階文件、流程、程序或控制措施時，應與本公司之資通安全政策、目標及本安全維護計畫之內容相符，並應保存相關之執行成果記錄。

2、 資通安全維護計畫實施情形之稽核機制

(1) 稽核機制之實施

I. 資通安全推動小組應定期（至少每年一次）或於系統重大變更或組織改造後執行一次內部及委外廠商之資安稽核作業，以確認人員是否遵循本規範與公司之管理程序要求，並有效實作及維持管理制度。

II. 辦理稽核前，資通安全推動小組應擬定資通安全稽核計畫或於資訊循環內稽一併實施，稽核範圍應包括內部與

委外廠商的前次稽核結果，以確保持續改善。並安排稽核成員，應將前次稽核之結果納入稽核範圍。

III. 辦理稽核時，資通安全推動小組應於執行稽核前七日，通知受稽核單位與委外廠商，並將稽核期程、稽核項目紀錄表及稽核流程等相關資訊提供受稽單位。

IV. 本公司之稽核人員應受適當培訓並具備稽核能力，且不得稽核自身經辦業務，以確保稽核過程之客觀性及公平性；另，於執行稽核時，應填具稽核項目紀錄表，待稽核結束後，應將稽核項目紀錄表內容彙整至稽核結果及改善報告中，並提供給受稽單位與委外廠商填寫辦理情形。

V. 稽核結果應對「資通安全管理委員會」報告，留存相關紀錄以作為稽核計畫及稽核事件之證據。

VI. 資通安全稽核後，應就稽核中發現事項擬訂改善措施，並定期追蹤內部與委外廠商之改善情形。稽核結果應對相關管理階層（含資安長）報告，並留存稽核過程之相關紀錄以作為資通安全稽核計畫及稽核事件之證據。

(2) 稽核改善報告

I. 受稽單位於稽核實施後發現有缺失或待改善項目者，應對缺失或待改善之項目研議改善措施、改善進度規劃，並落實執行。

II. 受稽單位於稽核實施後發現有缺失或待改善者，應判定其發生之原因，並評估是否有其類似之缺失或待改善之項目存在。

III. 受稽單位於判定缺失或待改善之原因後，應據此提出並執行相關之改善措施及改善進度規劃，必要時得考量對現行資通安全管理制度或相關文件進行變更。

IV. 公司應定期審查受稽單位缺失或待改善項目所採取之改善措施、改善進度規劃及佐證資料之有效性。

V. 受稽單位於執行改善措施時，應留存相關之執行紀錄，並填寫稽核結果及改善報告。

3、 資通安全維護計畫之持續精進及績效管理

(1)本公司之資通安全推動小組應定期（每年至少一次）召開資通安全管理審查會議，確認資通安全維護計畫之實施情形，確保其持續適切性、合宜性及有效性。

(2)管理審查議題應包含下列討論事項：

I. 過往管理審查議案之處理狀態。

II. 與資通安全管理系統有關之內部及外部議題的變更，如法令變更、上級機關要求、資通安全推動小組決議事項等。

III. 資通安全維護計畫內容之適切性。

IV. 資通安全績效之回饋，例：

i. 資通安全政策及目標之實施情形。

ii. 資通安全人力及資源之配置之實施情形。

iii. 資通安全防護及控制措施之實施情形。

iv. 資通安全監督及有效性量測結果。

v. 內外部稽核結果。

vi. 不符合項目及矯正措施。

V. 風險評鑑結果及風險處理計畫執行進度。

VI. 重大資通安全事件之處理及改善情形。

VII. 利害關係人之回饋。

VIII. 持續改善之機會。

(3)持續改善機制之管理審查應做成改善績效追蹤報告，相關紀錄並應予保存，以作為管理審查執行之證據。

(4)資通安全推動小組應於年度報告中敘明資通安全政策、具體管理方案、投入之資安管理資源、重大資通安全事件之損失與其可能影響，並說明已採取的因應措施，以加強資訊透明度並確保利益相關者對於資安管理之了解。

相關法規、程序及表單

1、 相關法規及參考文件

1. 上市上櫃公司資通安全管控指引

2. 公開發行公司建立內部控制制度處理準則

2、 附件表單

1. 核心業務評估調查表

2. 年度費用預算表

3. 資通安全推動小組成員及分工表

4. 資通訊系統盤點表

5. 資產價值識別表

6. 資安風險評估報告