證券商內部控制制度標準規範—內部控制制度修正對照表

編號	作業項目	修正後內容	修正前內容	修正說明
CC-17010	網路安全管理	作業程序及控制重點： 適用網際網路下單證券商，另(一)、(二)、(六)、(十三)項並適用於所有證券商 (一)網路系統安全評估： 1.應定期評估自身網路系統安全(例如：作業系統、網站伺服器、瀏覽器、防火牆及防毒版本等)，並留存相關紀錄。 2.應定期或適時修補網路運作環境及作業系統之安全漏洞（含伺服器、攜帶型、個人端及營業處所內供投資人共用之電腦等），並留存相關文件。 3.有關電腦網路安全(如資訊安全政策宣導、防範網路駭客入侵事件、電腦防毒等)之事項應隨時對內部公告。 4.各電腦主機、重要軟硬體設備應有專人負責。 5.公司網路應依用途區分為 DMZ、營運環境、測試環境及其他環境，並有適當區隔機制(如防火牆、虛擬區域網路、實體隔離等)。 6.個人資料及機敏資料應存放於安全的網路區域，不得存放於網際網路等區域。 7.系統應僅開啟必要之服務及程式，未使用之服務功能應關閉。(網際網路下單證券商適用)。 8.公司應建立遠端連線管理辦法，對使用外	作業程序及控制重點： 適用網際網路下單證券商，另(一)、(二)、(六)、(十三)項並適用於所有證券商 (一)網路系統安全評估： 1.應定期評估自身網路系統安全(例如：作業系統、網站伺服器、瀏覽器、防火牆及防毒版本等)，並留存相關紀錄。 2.應定期或適時修補網路運作環境及作業系統之安全漏洞（含伺服器、攜帶型、個人端及營業處所內供投資人共用之電腦等），並留存相關文件。 3.有關電腦網路安全(如資訊安全政策宣導、防範網路駭客入侵事件、電腦防毒等)之事項應隨時對內部公告。 4.各電腦主機、重要軟硬體設備應有專人負責。 5.公司網路應依用途區分為 DMZ、營運環境、測試環境及其他環境，並有適當區隔機制(如防火牆、虛擬區域網路、實體隔離等)。 6.個人資料及機敏資料應存放於安全的網路區域，不得存放於網際網路等區域。 7.系統應僅開啟必要之服務及程式，未使用之服務功能應關閉。(網際網路下單證券商適用)。 8.公司應建立遠端連線管理辦法，對使用外	1.參酌「證券商辦理資通系統資通安全評估作業程序」，增訂情資評估及處理之規定。；2.調整用字一致性； 3.調整用字一致性及範例，避免使用安全性不足之協議； 4.調整用字一致性； 5.調整用字一致性； 6.調整用字一致性； 7.增訂上網連線管控機制規定； 8.調整用字一致性； 9.調整用字一致性；10.調整用字一致性；

編號	作業項目	修正後內容	修正前內容	修正說明
		部網路遠端連線至公司內部作業進行控管及多因子身分認證，留存相關維護紀錄並由權責主管定期覆核。 9.公司應防止未經授權設備使用內部網路。 10.應避免使用生命週期終止(End of Service， EOS/End of Life, EOL)之軟體及網路設備，且於到期前擬定汰除計畫，並視情況建立補償性措施。 11.公司應就所接收資安情資，辨識其來源之可靠性及時效性，及時進行威脅與弱點分析及研判潛在風險，並採取對應之預防或應變措施。 (二)網路設備之安全管理： 1.應建立防火牆。 2.防火牆應有專人管理。 3.防火牆進出紀錄及其備份應至少保存三年。 4.重要網站及伺服器系統(如網際網路下單系統等)應以防火牆與外部網際網路隔離。 5.防火牆系統之設定應經權責主管之核准。 6.公司應每年定期檢視並維護防火牆存取控管設定，每半年檢視 DMZ 區之防火牆規則，包含評估高風險設定及六個月內無流量之防火牆之必要性，及針對已下線資通系統於六個月內調整或停用該規則，並留存相關檢視紀錄。	部網路遠端連線至公司內部作業進行控管及多因子身分認證，留存相關維護紀錄並由權責主管定期覆核。 9.公司應防止未經授權設備使用內部網路。 10.應避免使用生命週期終止(End of Service， EOS/End of Life, EOL)之軟體及網路設備，且於到期前擬定汰除計畫，並視情況建立補償性措施。 (新增) (二)網路設備之安全管理： 1.應建立防火牆。 2.防火牆應有專人管理。 3.防火牆進出紀錄及其備份應至少保存三年。 4.重要網站及伺服器系統(如網路下單系統等)應以防火牆與外部網際網路隔離。 5.防火牆系統之設定應經權責主管之核准。 6.公司應每年定期檢視並維護防火牆存取控管設定，每半年檢視 DMZ 區之防火牆規則，包含評估高風險設定及六個月內無流量之防火牆之必要性，及針對已下線資通系統於六個月內調整或停用該規則，並留存相關檢視紀錄。	

編號	作業項目	修正後內容	修正前內容	修正說明
		7.公司建立網路設備規則應以最小授權及正面表列為原則。 8.公司應至少每年檢視一次對外網路設備規則，並留存相關紀錄。 (三)網路傳輸安全管理： 1.網際網路下單畫面應採加密方式(例如：TLS)處理。 2.公司應每日針對核心系統之帳號登入失敗紀錄、非客戶帳號嘗試登入紀錄等進行監控及分析，發現有帳號登入異常情事(如密碼輸入錯誤達三次、一定時間內大量帳號登入失敗、帳戶申請或更新憑證下載異常)，應即時了解異常原因，並留存相關紀錄。 3.公司提供網際網路下單服務，應於網際網路下單登入時採多因子認證方式(例如：固定密碼、圖形鎖、下單憑證、綁定裝置、OTP、生物辨識等機制)，以確保為客戶本人登入。 4.公司加密機制應優先考慮使用公開、國際機構驗證且未遭破解之演算法。 (四)多因子驗證： 公司使用多因子驗證應具下列三項之任兩項技術： 1.公司所約定之資訊，且無第三人知悉（如固定密碼、圖形鎖或手勢等）。	7.公司建立網路設備規則應以最小授權及正面表列為原則。 8.公司應至少每年檢視一次對外網路設備規則，並留存相關紀錄。 (三)網路傳輸安全管理： 1.網路下單畫面應採加密方式(例如：SSL)處理。 2.公司應每日針對核心系統之帳號登入失敗紀錄、非客戶帳號嘗試登入紀錄等進行監控及分析，發現有帳號登入異常情事(如密碼輸入錯誤達三次、一定時間內大量帳號登入失敗、帳戶申請或更新憑證下載異常)，應即時了解異常原因，並留存相關紀錄。 3.公司提供網路下單服務，應於網路下單登入時採多因子認證方式(例如：固定密碼、圖形鎖、下單憑證、綁定裝置、OTP、生物辨識等機制)，以確保為客戶本人登入。 4.公司加密機制應優先考慮使用公開、國際機構驗證且未遭破解之演算法。 (四)多因子驗證： 公司使用多因子驗證應具下列三項之任兩項技術： 1.公司所約定之資訊，且無第三人知悉（如固定密碼、圖形鎖或手勢等）。	

編號	作業項目	修正後內容	修正前內容	修正說明
		2.客戶所持有之實體設備(如密碼產生器、密碼卡、晶片卡、電腦、行動裝置、憑證載具等)，公司應確認該設備為客戶與公司所約定持有之設備。 3.客戶提供給公司其所擁有之生物特徵(如指紋、臉部、虹膜、聲音、掌紋、靜脈、簽名等)，公司應直接或間接驗證該生物特徵。 (五)身分認證與憑證管理： 1.網際網路下單證券商應訂定憑證交付程序，避免非本人取得憑證。客戶申請或更新憑證下載，必須採用多因子(如：下單憑證、綁定裝置、OTP、生物辨識及SIM 認證等)驗證方式，且與登入帳戶時使用之因子不同，確實辨認客戶身分並留存紀錄。 2.網際網路下單證券商應全面使用認證機制。 3.公司應於伺服器端驗證客戶交易身分及使用者帳號。 4.公司對電子交易身分之申請、交付、使用、更新與驗證應訂定相關規範。 (六)電腦病毒及惡意軟體之防範： 1.應安裝防毒軟體，並及時更新程式及病毒碼。 2.應定期對資通系統及資料儲存媒體進行病毒描(含電子郵件)。	2.客戶所持有之實體設備(如密碼產生器、密碼卡、晶片卡、電腦、行動裝置、憑證載具等)，公司應確認該設備為客戶與公司所約定持有之設備。 3.客戶提供給公司其所擁有之生物特徵(如指紋、臉部、虹膜、聲音、掌紋、靜脈、簽名等)，公司應直接或間接驗證該生物特徵。 (五)身分認證與憑證管理： 1.網路下單證券商應訂定憑證交付程序，避免非本人取得憑證。客戶申請或更新憑證下載，必須採用多因子(如：下單憑證、綁定裝置、OTP、生物辨識及SIM 認證等)驗證方式，且與登入帳戶時使用之因子不同，確實辨認客戶身分並留存紀錄。 2.網路下單應全面使用認證機制。 3.公司應於伺服器端驗證客戶交易身分及使用者帳號。 4.公司對電子交易身分之申請、交付、使用、更新與驗證應訂定相關規範。 (六)電腦病毒及惡意軟體之防範： 1.應安裝防毒軟體，並及時更新程式及病毒碼。 2.應定期對資通系統及資料儲存媒體進行病毒描(含電子郵件)。	

編號	作業項目	修正後內容	修正前內容	修正說明
		3.防毒應涵蓋個人端(含攜帶型及營業處所內供投資人共用之電腦等）及網路伺服器端電腦。 4.勿開啟來歷不明之電子郵件，對於電子郵件中帶有執行檔之附件，尤應特別小心開啟。 5.為防範電腦病毒擴散，影響電腦安全，公司應訂定電子郵件使用安全相關規定及建立郵件過濾機制。 6.公司應建立軟體白名單及上網控管機制。 7.公司應偵測釣魚網站及惡意網站連結並提醒客戶防範網路 釣魚。 8.公司應每年定期辦理社交工程演練，並對誤開啟信件或連結之人員進行教育訓練，並留存相關紀錄。 (七)網路系統功能檢查： 1.應定期檢查網際網路下單系統提供之功能，並留存 紀錄。 2.公司應就提供外部連線使用網路系統偵測網頁與程式異動、記錄並通知相關人員處理。 (八)公司提供 API 服務規範： 依據「證券商受理投資人使用應用程式介面(API)服務作業規範」，公司提供客戶使用應用程式介面(API)服務之相關作業，應依下列申請流程、核可標準及相關控管配套措施辦理：	3.防毒應涵蓋個人端(含攜帶型及營業處所內供投資人共用之電腦等）及網路伺服器端電腦。 4.勿開啟來歷不明之電子郵件，對於電子郵件中帶有執行檔之附件，尤應特別小心開啟。 5.為防範電腦病毒擴散，影響電腦安全，公司應訂定電子郵件使用安全相關規定及建立郵件過濾機制。 6.公司應建立軟體白名單控管機制。 7.公司應偵測釣魚網站及惡意網站連結並提醒客戶防範網路 釣魚。 8.公司應每年定期辦理社交工程演練，並對誤開啟信件或連結之人員進行教育訓練，並留存相關紀錄。 (七)網路系統功能檢查： 1.應定期檢查網路下單系統提供之功能，並留存 紀錄。 2.公司應就提供外部連線使用網路系統偵測網頁與程式異動、記錄並通知相關人員處理。 (八)公司提供 API 服務規範： 依據「證券商受理投資人使用應用程式介面(API)服務作業規範」，公司提供客戶使用應用程式介面(API)服務之相關作業，應依下列申請流程、核可標準及相關控管配套措施辦理：	

編號	作業項目	修正後內容	修正前內容	修正說明
		1.申請流程： (1)客戶申請 API 服務時，應親持身分證明文件提出書面申請並於營業場所當場簽名或蓋章，或得採足以確認申請人為本人及其意思表示之通信或電子化方式向公司申請。 (2)客戶為法人者，應由法人及其代表人在申請書上簽名或蓋章，並出具授權書。 (3)公司於受理客戶提出使用 API 服務之申請時，應由登記合格之業務員向客戶詳盡說明有關使用 API 服務之注意事項及各項權利義務關係（包含使用 API 服務所可能產生之相關風險及相關使用約定等），並經客戶出具聲明書確認已受充分告知、閱讀並瞭解。上述聲明書應由客戶簽名或蓋章確認並加註日期存執。聲明書亦得採下列電子簽章簽署程序為之： A.聲明書之內容需逐條（段）勾選。 B.點選進入聲明書內容後至同意簽署確認前，其畫面停留之時間以可以適當閱讀該聲明書之完整內容為依據。 C.客戶確認以電子簽章簽署後，公司可以電子郵件、網址、簡訊等方式，傳送聲明書副本予客戶，並經客戶確認後始生效。 (4)有關客戶所出具之聲明書內容，至少應	1.申請流程： (1)客戶申請 API 服務時，應親持身分證明文件提出書面申請並於營業場所當場簽名或蓋章，或得採足以確認申請人為本人及其意思表示之通信或電子化方式向公司申請。 (2)客戶為法人者，應由法人及其代表人在申請書上簽名或蓋章，並出具授權書。 (3)公司於受理客戶提出使用 API 服務之申請時，應由登記合格之業務員向客戶詳盡說明有關使用 API 服務之注意事項及各項權利義務關係（包含使用 API 服務所可能產生之相關風險及相關使用約定等），並經客戶出具聲明書確認已受充分告知、閱讀並瞭解。上述聲明書應由客戶簽名或蓋章確認並加註日期存執。聲明書亦得採下列電子簽章簽署程序為之： A.聲明書之內容需逐條（段）勾選。 B.點選進入聲明書內容後至同意簽署確認前，其畫面停留之時間以可以適當閱讀該聲明書之完整內容為依據。 C.客戶確認以電子簽章簽署後，公司可以電子郵件、網址、簡訊等方式，傳送聲明書副本予客戶，並經客戶確認後始生效。 (4)有關客戶所出具之聲明書內容，至少應	

編號	作業項目	修正後內容	修正前內容	修正說明
		聲明對下列事項已充分瞭解並遵循： A.使用 API 服務下單所可能產生之相關風險，如因網路壅塞、斷電、斷線、電腦程式交易錯誤等所導致之風險。 B.使用 API 服務下單之客戶應自行決定買賣之執行。 C.應妥善保管個人交易帳戶、網路登錄密碼及數位憑證(電子簽章)，不得交由第三人或資訊廠商從事未經核准之全權委託交易，以免發生交易糾紛。 D.使用 API 服務下單除應遵循與公司所訂之相關約定外，並不得為任何不法之使用。 2.核可標準：由公司自行訂定 API 申請資格。 3.相關控管配套措施： (1)公司應能區分使用 API 服務所傳送之委託，對於使用 API 服務下單與其他下單方式之委託應有公平之先後次序。 (2)對於客戶使用 API 服務下單應訂定具體之異常標準及異常狀況處理程序，並確實執行。必要時得暫停客戶使用 API 服務下單，並通知客戶改用其他委託方式，至排除異常狀況後，再通知客戶得恢復使用 API 服務下單。 (3)公司應於客戶首次使用 API 委託下單	聲明對下列事項已充分瞭解並遵循： A.使用 API 服務下單所可能產生之相關風險，如因網路壅塞、斷電、斷線、電腦程式交易錯誤等所導致之風險。 B.使用 API 服務下單之客戶應自行決定買賣之執行。 C.應妥善保管個人交易帳戶、網路登錄密碼及數位憑證(電子簽章)，不得交由第三人或資訊廠商從事未經核准之全權委託交易，以免發生交易糾紛。 D.使用 API 服務下單除應遵循與公司所訂之相關約定外，並不得為任何不法之使用。 2.核可標準：由公司自行訂定 API 申請資格。 3.相關控管配套措施： (1)公司應能區分使用 API 服務所傳送之委託，對於使用 API 服務下單與其他下單方式之委託應有公平之先後次序。 (2)對於客戶使用 API 服務下單應訂定具體之異常標準及異常狀況處理程序，並確實執行。必要時得暫停客戶使用 API 服務下單，並通知客戶改用其他委託方式，至排除異常狀況後，再通知客戶得恢復使用 API 服務下單。 (3)公司應於客戶首次使用 API 委託下單	

編號	作業項目	修正後內容	修正前內容	修正說明
		前，就相關傳輸設定進行連線測試，並留存相關測試紀錄。 (4)客戶利用網際網路使用 API 服務下單前，必須通過網際網路下單帳號、網路登錄密碼及數位憑證（電子簽章）等身分驗證程序。 (5)公司提供客戶使用應用程式介面(API)服務係屬證券商電子式交易型態之網際網路委託買賣方式，應符合「證券商採網際網路等電子式交易型態交易所使用之交易主機應具備之相關受託買賣有價證券檢查點控制項目」之規定，確實遵循證券市場相關規定、落實資通安全與風險管控，不得有影響證券集中市場秩序與效率之行為。 (6)客戶使用應用程式介面(API)服務，其原始委託資料、條件觸發時之委託資料及憑證機構所簽發之電子簽章應由公司予以完整保存，且於委託紀錄之委託方式中記載係以網際網路「客戶使用應用程式介面(API)服務下單」以資區別，前揭委託資料之電腦檔案委託紀錄及電腦稽核紀錄 (log)之保存年限仍應依「證券經紀商使用網際網路等電子式交易型態製作買賣委託紀錄之處理流程」及「網際網路等電子式交易型態交易資料保存規範」之規定辦理。	前，就相關傳輸設定進行連線測試，並留存相關測試紀錄。 (4)客戶利用網際網路使用 API 服務下單前，必須通過網路下單帳號、網路登錄密碼及數位憑證（電子簽章）等身分驗證程序。 (5)公司提供客戶使用應用程式介面(API)服務係屬證券商電子式交易型態之網際網路委託買賣方式，應符合「證券商採網際網路等電子式交易型態交易所使用之交易主機應具備之相關受託買賣有價證券檢查點控制項目」之規定，確實遵循證券市場相關規定、落實資通安全與風險管控，不得有影響證券集中市場秩序與效率之行為。 (6)客戶使用應用程式介面(API)服務，其原始委託資料、條件觸發時之委託資料及憑證機構所簽發之電子簽章應由公司予以完整保存，且於委託紀錄之委託方式中記載係以網際網路「客戶使用應用程式介面(API)服務下單」以資區別，前揭委託資料之電腦檔案委託紀錄及電腦稽核紀錄 (log)之保存年限仍應依「證券經紀商使用網際網路等電子式交易型態製作買賣委託紀錄之處理流程」及「網際網路等電子式交易型態交易資料保存規範」之規定辦理。	

編號	作業項目	修正後內容	修正前內容	修正說明
		(7)公司提供客戶使用應用程式介面(API)服務，不得違反證交法第 159 條有關全權委託禁止之規定。 (8)公司若有提供交易資訊予其開戶之客戶應依證交所「交易資訊使用管理辦法」之規定辦理。 (9)API 服務下單交易相關資料，公司應併同網際網路及語音資料，由單一窗口系統於每月前 4 個營業日申報。 (九)網際網路下單服務品質相關標準： 公司提供網際網路下單業務時，兼顧客戶服務品質，應訂定網際網路下單服務品質相關標準，並應包含下列重點： 1.交易之安全性：包括建立相關資訊安全機制，並擬定緊急應變計畫及備援措施。 2.交易之穩定及系統可用性：為維持網路交易之順暢與便捷，應定期評估系統可用性並留存紀錄，就網際網路下單客戶數、交易流量及預期將來交易量，衡量現有設備是否足以負載、是否需擴充相關軟硬體設備，以避免發生網路塞單、委託成交速度遲緩甚或當機之風險。 3.提供客戶服務：提供客戶多元之附加價值，基本服務應包括報價資訊、委託下單、帳務查詢、技術分析、即時庫存、資券配額及整戶維持率等七項。 (十Ｏ)網路攻擊防護機制導入及安全性檢測	(7)公司提供客戶使用應用程式介面(API)服務，不得違反證交法第 159 條有關全權委託禁止之規定。 (8)公司若有提供交易資訊予其開戶之客戶應依證交所「交易資訊使用管理辦法」之規定辦理。 (9)API 服務下單交易相關資料，公司應併同網際網路及語音資料，由單一窗口系統於每月前 4 個營業日申報。 (九)網際網路下單服務品質相關標準： 公司提供網際網路下單業務時，兼顧客戶服務品質，應訂定網際網路下單服務品質相關標準，並應包含下列重點： 1.交易之安全性：包括建立相關資訊安全機制，並擬定緊急應變計畫及備援措施。 2.交易之穩定及系統可用性：為維持網路交易之順暢與便捷，應定期評估系統可用性並留存紀錄，就網路下單客戶數、交易流量及預期將來交易量，衡量現有設備是否足以負載、是否需擴充相關軟硬體設備，以避免發生網路塞單、委託成交速度遲緩甚或當機之風險。 3.提供客戶服務：提供客戶多元之附加價值，基本服務應包括報價資訊、委託下單、帳務查詢、技術分析、即時庫存、資券配額及整戶維持率等七項。 (十Ｏ)網路攻擊防護機制導入及安全性檢測	

編號	作業項目	修正後內容	修正前內容	修正說明
		1.公司應依其所屬資安分級定期對提供網際網路服務之核心系統辦理滲透測試，並依測試結果進行改善。 2.公司應依「證券商辦理資通系統資訊安全評估作業程序」並就其所屬資安分級定期辦理資通安全健診作業。 3.公司應依其所屬資安分級建立資通安全威脅偵測管理機制(應含括事件收集、異常分析、偵測攻擊並判斷攻擊行為) 4.公司應依其所屬資安分級建立入侵偵測及防禦機制。 5.公司應依其所屬資安分級設置應用程式防火牆。 6.公司應依其所屬資安分級辦理進階持續性威脅攻擊防禦措施。 7.核心系統身分驗證機制應防範自動化程式之登入或密碼更換嘗試，非核心系統宜防範自動化程式之登入或密碼更換嘗試。 (十一)帳號登入或異常態樣通知： 公司對於客戶帳號登入時宜進行通知，如有符合以下異常態樣應即通知客戶，並留存紀錄，避免非客戶本人登入情事： 1.密碼輸入錯誤或帳戶被鎖定。 2.申請或更新憑證。 3.變更基本資料。 4.異常來源或行為嘗試登入等。	1.公司應依其所屬資安分級定期對提供網際網路服務之核心系統辦理滲透測試，並依測試結果進行改善。 2.公司應依「證券商辦理資通系統資訊安全評估作業程序」並就其所屬資安分級定期辦理資通安全健診作業。 3.公司應依其所屬資安分級建立資通安全威脅偵測管理機制(應含括事件收集、異常分析、偵測攻擊並判斷攻擊行為) 4.公司應依其所屬資安分級建立入侵偵測及防禦機制。 5.公司應依其所屬資安分級設置應用程式防火牆。 6.公司應依其所屬資安分級辦理進階持續性威脅攻擊防禦措施。 7.核心系統身分驗證機制應防範自動化程式之登入或密碼更換嘗試，非核心系統宜防範自動化程式之登入或密碼更換嘗試。 (十一)帳號登入或異常態樣通知： 公司對於客戶帳號登入時宜進行通知，如有符合以下異常態樣應即通知客戶，並留存紀錄，避免非客戶本人登入情事： 1.密碼輸入錯誤或帳戶被鎖定。 2.申請或更新憑證。 3.變更基本資料。 4.異常來源或行為嘗試登入等。	

編號	作業項目	修正後內容	修正前內容	修正說明
		5.密碼申請異動或補發時。 (十二)異常 IP 登入之監控與預警： 公司應依其所屬資安分級對異常及不明來源 IP 連線進行監控分析及留存紀錄，如有發現下列情形，應設有警示機制，並定期檢視以確認機制有效運作： 1.同一來源 IP 登入不同帳號達一定次數以上。 2.同一帳號在一定時間內由不同國家登入。 3.發現異常來源 (如金融資安資訊分享與分析中心 F-ISAC 公布之黑名單或國外 IP)嘗試登入。 (十三)無線網路管理： 1.公司設置無線網路應採用現行公開資訊已認可且無弱點之安全協定。 2.公司提供內部無線網路使用應限內部人員公務用或資訊服務供應商申請核准後使用。	5.密碼申請異動或補發時。 (十二)異常 IP 登入之監控與預警： 公司應依其所屬資安分級對異常及不明來源 IP 連線進行監控分析及留存紀錄，如有發現下列情形，應設有警示機制，並定期檢視以確認機制有效運作： 1.同一來源 IP 登入不同帳號達一定次數以上。 2.同一帳號在一定時間內由不同國家登入。 3.發現異常來源 (如金融資安資訊分享與分析中心 F-ISAC 公布之黑名單或國外 IP)嘗試登入。 (十三)無線網路管理： 1.公司設置無線網路應採用現行公開資訊已認可且無弱點之安全協定。 2.公司提供內部無線網路使用應限內部人員公務用或資訊服務供應商申請核准後使用。	