**中華民國證券商業同業公會網路安全防護自律規範**

**修正條文對照表**

| **修正條文** | **現行條文** | **說明** |
| --- | --- | --- |
| **第二條 名詞定義**  一、～五、（略）  六、資訊服務供應商：係指符合「本公會證券商資通系統與服務供應鏈風險管理自律規範」遴選條件之廠商。 | **第二條 名詞定義**  一、～五、（略） | 1. 新增本條第六款。 2. 參照本公會「證券商資通系統與服務供應鏈風險管理自律規範」新增「六、資訊服務供應商」之名詞定義。 |
| 七、第一類證券商：係指依「證券暨期貨市場各服務事業建立內部控制制度處理準則」第三十六條之二條文指派資訊安全長之證券商。 | 六、第一類證券商：係指依「證券暨期貨市場各服務事業建立內部控制制度處理準則」第三十六條之二條文指派資訊安全長之證券商~~或「建立證券商資通安全檢查機制-分級防護應辦事項附表」所列第一級、第二級、第三級證券商~~。 | 1. 項次調整。 2. 依據金管會113年1月4日金管證券字第1120385996號令，有關設立資訊安全長條件調整，刪除分類之條件。 |
| 八、第二類證券商：係指非屬第一類證券商之證券商。 | ~~七~~、第二類證券商：係指非屬第一類證券商之證券商。 | 項次調整 |
| 九、外國證券商：係指外資集團在台子公司或分公司。外國證券商如有標準較佳之規範則從其規範；若無，則應遵守本國的規範。 | ~~八~~、外國證券商：係指外資集團在台子公司或分公司。外國證券商如有標準較佳之規範則從其規範；若無，則應遵守本國的規範。 | 項次調整 |
| **第三條 網路架構與網路安全管理**  二、網路區域劃分  (二)網段應以維持業務運作劃分區域：如隔離區(非軍事區， Demilitarized Zone，DMZ)、營運區(Production， Prod.)、測試區(Unit Test, UT 或 User Acceptance Test, UAT)及其他等網段。證券商應每半年檢視DMZ區之防火牆規則，並留存相關檢視紀錄。  (三)證券商應定義外部網路與內部網路，外部網路連接網際網路，內部網路區域為組織人員與內部服務的伺服器配置區域。由外部網路到內部網路的流量需要經過存取控制，僅限於內部人員公務用或資訊服務供應商申請核准後使用，避免非允許的服務進入。  (五)證券商應使用適當方式隔離限制存取與特定服務，且應視區隔方式，每年定期檢視防火牆規則或存取控制清單(Access Control List, ACL)。  三、內部網路與外部網路管理  (一)證券商如有提供內部無線網路使用，其存取保護應採用現行公開資訊已認可且無弱點之安全協定，並比照內部網路管理程序，僅限於內部人員公務用或資訊服務供應商申請核准後使用。  (二)證券商如有提供外部無線網路使用，其存取保護應採用現行公開資訊已認可且無弱點之安全協定。  (三)證券商應建立無線網路密碼原則，以降低密碼破解之風險。  (四)證券商如允許內部人員或資訊服務供應商使用外部設備存取內部網路，應提出申請並檢視設備安全性與相關授權，並限制存取範圍。 | **第三條 網路架構與網路安全管理**  二、網路區域劃分  (二)網段應以維持業務運作劃分區域：如隔離區(非軍事區，Demilitarized Zone，DMZ)、營運區(Production，Prod.)、測試區(Unit Test, UT 或 User Acceptance Test, UAT)及其他等網段。  (三)證券商應定義外部網路與內部網路，外部網路連接網際網路，內部網路區域為組織人員與內部服務的伺服器配置區域。由外部網路到內部網路的流量需要經過存取控制，避免非允許的服務進入。  (五)證券商應使用適當方式隔離限制存取與特定服務，且應視區隔方式，定期檢視防火牆規則或存取控制清單(Access Control List, ACL)。  三、內部網路管理  ~~(一)~~證券商如有提供無線網路供內/外部人員使用，無線網路存取保護應採用現行公開資訊已認可且無弱點之安全協定。  ~~(二)~~證券商應建立無線網路密碼原則，以降低密碼破解之風險。  ~~(三)~~證券商如允許內/外部人員使用外部設備存取內部網路，應提出申請並檢視設備安全性與相關授權，並限制存取範圍。 | 一、修正本條第二款第二目及第五目。配合證交所113年5月15日臺證輔字第1130008401號函修正「建立證券商資通安全檢查機制」通訊與作業管理（CC-17000）（1）b. (f)之規定，新增證券商應每半年檢視DMZ區之防火牆規則，及每年定期檢視並維護防火牆存取控管設定。  二、修正本條第二款第三目，配合期交所113年4月19日台期規字第1130001018號函修正「證券暨期貨市場各服務事業網路安全防護參考指引」第五條第三款之規定，由外部網路到內部網路之存取控制，增訂僅限於組織人員公務用或資訊服務供應商申請核准後使用。  三、新增本條第三款第一項，配合前開期交所修正網路安全防護參考指引第七條第一款之規定，將無線網路區分為內、外部網路進行管理，新增第一款有關內部無線網路之管理、使用者及申請使用方式。  四、以下項次配合調整。  五、修正本條第三款第二目，參照前開期交所修正網路安全防護參考指引第七條第二款之規定，規範外部無線網路之存取保護方式。  六、修正本條第三款第四目，參照前開期交所修正網路安全防護參考指引第八條第一項之規定，證券商如允許內/外部人員使用外部設備存取內部網路，修訂為「組織內人員或資訊服務供應商」。 |
| **第四條 網路設備安全管理**  四、網路設備委外  證券商所有網路設備若委由資訊服務供應商維運或管理應依「本公會證券商資通系統與服務供應鏈風險管理自律規範」。 | **第四條 網路設備安全管理**  四、網路設備委外  證券商所有網路設備若委由~~外部廠~~商維運或管理應依「本公會供應鏈風險管理自律規範」。 | 修正本條第四款，參照前開期交所修正網路安全防護參考指引第十二條第一項之規定，將外部廠商修訂為資訊服務供應商，其維運及管理應依本公會「證券商資通系統與服務供應鏈風險管理自律規範」。 |