第一章>>總則

	第一條	為協助上市、上櫃公司(以下簡稱公司)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·特擬定本資通安全管控指引。		
	第二條	一、資通系統:指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或 對資訊為其他處理、使用或分享之系統。 一、資通服務:指與資訊之蒐集、控制、傳輸、儲存、流通、刪除、 一、其他處理、使用或分享相關之服務。 三、 <mark>核心業務</mark> :公司維持營運與發展必要之業務。		
		四、 核心資通系統:支持核心業務持續運作必要之資通系統。 五、 機敏性資料:依公司業務考量,評估需保密或具敏感性之重要資料,如涉及營業秘密資料或個人資料等。		
第	三章>>資	通安全政策及推動組織		
	第三條	成立 <u>資通安全推動組織</u> ,組織配置適當之人力、物力與財力資源,並指派適當人員擔任資安專責主管及資安專責人員,以負責推動、協調監督及審查資通安全管理事項。		各單位 主管
	第四條	訂定<u>資通安全政策及目標</u> ·由副總經理以上主管核定·並 定期檢視 政策及目標且有效傳達員工其重要性。		副 總經理
	第五條	訂定資通安全作業程序,包含核心業務及其重要性、資通系統盤點及風險評估、資通系統發展及維護安全、資通安全防護及控制措施、資通系統或資通服務委外辦理之管理措施、資通安全事件通報應變及情資評估因應、資通安全之持續精進及績效管理機制等。		各單位 主管
	第六條	所有使用資訊系統之人員· 每年 接受資訊安全宣導課程·另負責資訊安全之主管及人員· 每年 接受資訊安全專業課程訓練。	+資訊安全 宣導課程/專業課程	人資
第	三章>>核	心業務及其重要性		
	第七條	鑑別並定期檢視 公司之 <mark>核心業務</mark> 及應保護之機敏性資料。		
	第八條	鑑別應遵守之法令及契約要求。		人資 法務
	第九條	鑑別可能造成營運中斷事件之發生機率及影響程度,並明確 訂定核心業務之復原時間目標(RTO)及資料復原時間點目標(RPO) ,設置適當之 <u>備</u> 份機制及備援計畫。	+雲備份 異地備份規劃 異地備援規劃	
	第十條	制定核心業務持續運作計畫,定期辦理核心業務持續運作演練,演練內 容包含核心業務備援措施、人員職責、應變作業程序、資源調配及演練 結果檢討改善。	+災難還原演練	
 第八條 鑑別可能造成營運中斷事件之發生機率及影響程度,並明確訂定核心業 務之復原時間目標(RTO)及資料復原時間點目標(RPO),設置適當之備 份機制及備援計畫。 第十條 第十條 第十條 第一會包含核心業務情援措施、人員職責、應變作業程序、資源調配及演練 結果檢討改善。 第四章>>資通系統盤點及風險評估 				
	第十一條	定期盤點資通系統·並建立核心 <u>系統資訊資產清冊</u> ·以鑑別其資訊資產價值。	+風險評鑑服務	
	第十二條	定期辦理資安風險評估,就核心業務及核心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。	+風險評鑑服務	

第五章>> 寶通条統發展及維護安全 第十三條 制:用戶登入身分體證及用戶輸入輸出之檢查過過等 是期執行實理系統與立性要求測式。包含機敬資料存取控制,用戶登入 身分體證及用戶輸入輸出之檢查過過測試等 第十五條 安替福存及管理資理系統開發及維護用文件 對核心實通系統附理下列資安檢測作業,並完成系統弱點修補 一、定期辦理認點掃描。 一、定期辦理認點掃描。 一、定期辦理認點掃描。 一、定期辦理認點掃描。 一、定期辦理認點掃描。 一、定期辦理認點掃描。 一、定期辦理認點掃描。 一、定期辦理認數指揮下列資安檢測作業,並完成系統弱點修補。 一、定期辦理認點掃描。 一、定期辦理認點掃描。 一、定期辦理或型於關控制措施 「在網路聚務需要取得獨立的週轉網域(如:DMZ、內部或外部網路等),並將開發、測部及正式作業環境區隔。且針對不同作業環境 理立強節當立安的隨建期措施。 具備下列資安防護控制措施。 一、奶毒軟附。 一、奶毒軟附。 一、奶毒軟附。 一、奶毒軟門內理。 一、網路區隔 第十八條 第十八條 一、於事軟階。 一、奶毒軟外服務之後心資通系統者,具備應用程式防火牆。 一、地學用程式防火體。 一、如有學性例服器者,具備電子學性過減機制。 四、人性個測及防禦機制。 四、人性個測及防禦機制。 一、如有學性與形成之環境系統者,具備應用程式防火牆。 一、地學與發生與大定環境和交建立強黨之防護措施。 一、"是關本與大處環境和存建立強黨之防護措施。如、"實體兩潮、專用程關件業環境、存取權限、資料加密、傳輸加密、資料建廠、人員豐期及產種與整計。」與了稱證或人員豐期及產種,等551條的加密,如實根數 第二十一條 第二十一條 建立使用者通行确管理之性業規定。如:所設密碼。學人民財制定機制。 少定可以所及配數整理程序,並簽署保度協議明確告知條配等,451條的加密,如實根數 第二十一條 建立使用者通行确管理之性業規定。如:預設密碼,密碼長度,多人民財制定機制。 十人及與對定機制。 第二十一條 建立使用者通行确等型之整理相能。如:身外破疾失敗,存取資 注入表述經 等三十四條 第二十四條 第二條 第二條 第二條 第二條 第二條 第二條 第二條 第二條 第二條 第二	第五音、、 2	8.通乡练發展 B.维维安令		
第十四條 第十四條 身外體發力用動入軸上及音腦與實料存取控制,用戶發入 身分體發力開發及性數相關文件。 對核心質調系統跨整件要求測試,包含機數資料存取控制,用戶發入 身分體發力關發力關發及推發相關文件。 對核心質調系統開發及推發相關文件。 對核心質調系統開發及推發相關文件。 對核心質調系統開發及推發相關文件。 對核心質調系統開發及推發相關文件。 對核心質調子統開發及推發相關文件。 第六章 >> 資通安全防護及控制措施 依線的級務需要原隔獨立的機類網域(如:DMZ、內部或外部網路等), 並將兩級、測試及正式件業環境區兩,且針對不同作業環境 建立策當之實質的護控制措施。 具備下列官安防護控制措施。 具備下列官安防護控制措施。 果備下列官安防護控制措施。 一、防毒軟體。 一、奶酒動代個服器者,具備電子部件過遠機制。 一、、奶酒動代圖服制。 一、如酒動作個服器者,具備電子部件過遠機制。 一、、奶酒動代圖服制。 一、、奶酒動代圖服制。 一、、奶酒動代圖服制。 一、、奶酒動代圖服制。 一、、奶酒動代圖服制。 一、、奶酒動代圖服制。 一、、奶酒動代圖服制。 一、、奶酒動代圖服制。 一、、奶酒動代圖服的工程, 一、、奶酒動代圖服制。 一、、奶酒動代圖服制。 一、、奶酒動代圖服制。 一、、奶酒動作過程與發動物, 一、一、 與國子發動與一及國際人類一致動態, 一、 如用可動化。 一、 如用在學所表演使、 存取權限、資料加密、 傳輸加密、 資制應數 人 與營 法務 是	寿 丑早>>員			
第十五條 安善儲存及管理資通系統開發及維護相關文件。 財核心寶通系統辦理下列資安檢測作業、並完成系統弱點修補。 一、定期辦理發起到話。 一、定期辦理發起到話。 一、定期辦理後差別話。 一、定期辦理後差別話。 一、定期辦理後差別話。 一、定期辦理後差別話。 一、定期辦理後差別話。 一、定期辦理後差別話。 一、完新所發、測試及正式作業環境區隔,且針對不同作業環境 如立強當之實政務護控制措施。 (如約部股務需要區隔獨立的选輯網域(如:DMZ、內部或外部網路等)。 並約開發、測試及正式作業環境區隔,且針對不同作業環境 如立強當之實政務護控制措施。 一、奶店軟體。 一、別倉野外渡邊上或作學環境區隔,且針對不同作業環境 中型化所決牆。 一、別倉野外渡邊之核心質遜系統者,具備應用程式防火牆。 一、如有影外而假器者,具備電子部件過減機制。 四、入侵偵測及防禦機制。 五、如有影外成器之核心質遜系統者,具備應用程式防火牆。 一、推踏存建性或養型支防療措施。 七、資遊安全域脅偵測管理機制(SOC)。 針對機敏性資料之處理及儲存建立遊當之防護措施,如:實體隔離、專用電化所決牆。 一、推踏持續性度養型支煙等與制物。如:實體隔離、入員置 理及處理規範等。 第二十條 第二十條 第二十條 第二十條 第二十條 第二十條 第二十條 第二十一條 第二十一條 第二十一條 第二十一條 第二十一條 第四項通系統及相關設備為當之監控措施,如:預稅破境定機制。 一、企評估於核心資通系統保取多重認證技術。如:預稅破境定機制。 一、企評估於核心資通系統保取多重認證技術。如:預稅破境定機制。 一、企評估於核心資通系統保取多重認證技術。如:自分驗證定機制。 一、企評估於核心資通系統保取多重認證技術。如:自分驗證定機制。 一、企評估於核心實通系統及相關設備與應當之監控措施。如:自分驗證定機制。 一、企評任於核心實通系統及相關設備與應之權定,如:預稅或權便、如:經稅經經, 第二十五條 第三十五條 第二十五條 第三十五條 第三十五條	第十三條			_
第十六條 第十六條 第六章>>實通安全防護及控制措施 二、定期辦理弱點掃描。 二、系統上線前執行源碼掃描安全檢測。 第六章>>實通安全防護及控制措施 依網路服務需要區隔獨立的攝輯網域(如:DMZ、內部或外部網路等),並將開發、測試及正式作業環境區隔。且針對不同作業環境 建立適當之質安防護控制措施 。具備下列賣安防護控制措施: ,防毒軟體。 與備下列賣安防護控制措施。 具備下列賣安防護控制措施。 四、入侵傾測及防禦機制。 五、如有對外服務之故質與系統者。具備應用程式防火牆。 一、海路防火牆。 一、如有對外服務之故質與系統者。具備應用程式防火牆。 一、如有對外服務之故質與系統者。具備應用程式防火牆。 一、如有對外服務之故可與系統者。具備應用程式防火牆。 一、如有對外服務之故可與系統者。具備應用程式防火牆。 一、強體持續性威勢攻擊防禦措施。 一、一、查通安全威勢傾測管理機制(SOC)。 第十九條 第十九條 第十九條 第十十條 第二十條 建立使用者通行碼管理之作變規定,如:預設密碼、密碼長度、密碼複樂 等因數定機關。 一、並將性於核心資道系統採取多重認證技術。 第二十一條 建立使用者通行碼管理之作變規定,如:預設密碼、密碼長度、密碼複樂 等」中,經過一數,經過一數,經過一數,不經不經經經 達立使用者通行碼管理之性變規定,如:預設密碼、密碼長度、密碼複樂 等」中,經過一數,經過一數,經過一數,不能以是機圖 第二十一條 建立使用者通行碼管理之作變規定,如:預設密碼、密碼長度、密碼複樂 等」中,經過一數,經過一數,不能以是機圖等重認證技術。 第二十二條 建立使用者通行碼管理之性變視定,如:預設密碼、密碼長度、密碼複樂 等」中,經過一數,經過一數,經過一數,不能以是機圖等,不以可等。 中,不可以可以與一個,一次將一次將一次將一次將一次將一次將一次將一次將一次將一次將一次將一次將一次將一	第十四條			_
第十六條 一、定期辦理物點掃描。 一、定期辦理物點掃描。 一、定期辦理物透測試。 三、系統上線前執行源碼掃描安全檢測。 第六章>>資通安全防護及控制措施 佐網洛服務需要區隔獨立的過程網域(如:DMZ、內部或外部網路等), 如為可聲文防護控制措施 佐網洛服務需要區隔獨立的過程網域(如:DMZ、內部或外部網路等), 維持衛星、對國文的實理機制構施 一、防毒軟體。 一、如為對於人間。 一、如為對外服務之核心資通系統者,具備應用程式防火牆。 一、如有對外服務之核心資通系統者,具備應用程式防火牆。 一、如有對外服務之核心資通系統者,具備應用程式防火牆。 一、如有對外服務之核心資通系統者,具備應用程式防火牆。 一、如有對外服務之核心資通系統者,具備應用程式防火牆。 一、如有對外服務之核心資通系統者,具備應用程式防火牆。 一、推斷持續則整理機制(SOC)。 計對機象性資料之處理及儲存建立適當之防護措施,如;實體隔離、專用電關作業環境。存取確限、資料加密、傳輸加密、資料連蔽、人員實理及應到數種轉。 第二十條 第二十一條 建立使用者通行碼管理之作業規定,如:預設密碼、密碼長度、密碼接 制定總部 第二十一條 建立使用者通行碼管理之作業規定,如:預設密碼、密碼長度、密碼接 制定總部 第二十一條 建立使用者通行碼管理之作業規定,如:預設密碼、密碼長度、密碼接 上個宣總部 十定期審查方案 建立資通系統及相關設備適當之監控措施,如:身分驗證失敗、存取資網上等組定,如:過程規制,並計估於核心資通系統深限多量認證技術。 第二十一條 定期審查者權帳號、使用者根據及權限,停用久未使用之帳號。 建立資通系統及相關設備適當之監控措施,如:身分驗證失敗、存取資 第二十一條 建立強監查之經護機制,如:數體沒權更不使用之未使用之帳號。 建立資通查者條號 使用者帳號及管理者行為等,並針對 日話建立遊舊之保護機制。 第二十一條 第三十一條 第三十一條 第三十一條 第三十一條 第三十四條 第三十五條	第十五條	妥善儲存及管理資通系統開發及維護相關文件。		-
第十六條 一、定期辦理渗透測試。 一、系統上線前執行源碼掃描安全檢測。 第六章>>資通安全防護及控制措施 依網路服務需要區隔獨立的運動網域(如:DMZ、內部或外部網路等),並將開發、測試及正式作業環境區隔,且針對不同作業環境 建立常文的護控制措施。 具佛下列資安防護控制措施。 具佛下列資安防護控制措施。 一、納路區隔 等十八條 第十八條 第一十人條 第二十一條 第二十一條 第二十一條 第二十一條 第二十一條 第二十一條 第二十一條 第二十一條 第二十一條 第三十一條 第三十一十一條 第三十一十一條 第三十一十一條 第三十一十一十一條 第三十一十一條 第三十一十一十一十一條 第三十一十一十一十一十一十一十一十一十一十一十一十一十一十一十一十一十一十一十一		對核心資通系統辦理下列資安檢測作業,並完成系統弱點修補。		-
□ 、 東統上線前執行源碼掃描安全檢測。	给上 业权	一、定期辦理弱點掃描。	+弱點掃描	-
第六章>>資通安全防護及控制措施 依網路服務需要區隔獨立的邏輯網域(如:DMZ、內部或外部網路等),並將開發、測試及正式作業環境區隔,且針對不同作業環境 建立適當之資安防護控制措施。 具備下列資安防護控制措施: 一、防毒軟體。 二、網路防火牆。 三、如有郵件伺服器者,具備電子郵件過濾機制。 四、入侵偵測及防禦機制。 五、如有對外服務之核心資通系統者,具備應用程式防火牆。 六、進階持續性臟勞攻擊防禦措施。 七、資通安全威脅偵測管理機制(SOC)。 針對機歇性資料之處理及儲存建立適當之防護措施,如:實體隔離、專 + 存取罹限管理 + 按取被方 接 接 + 接 + 表 以 使用者通行隔管理之作機規定 是 如	第十八 條	二、定期辦理滲透測試。	+滲透測試	-
第十七條 並将開發、測試及正式作業環境區隔,且針對不同作業環境		三、 系統上線前 執行源碼掃描安全檢測。	+源碼掃描	-
第十七條 並將開發、測試及正式作業環境區隔,且針對不同作業環境 建立適當之資安防護控制措施。 具備下列資安防護控制措施: 一、防毒軟體。 二、網路防火牆。 三、如有郵件伺服器者,具備電子郵件過濾機制。 五、如有對外服務之核心資通系統者,具備應用程式防火牆。 土、資腦安全威脅偵測管理機制(SOC)。 針對機敵性資料之處理及儲存建立適當之防護措施,如;實體隔離、專 用電腦作業環境、存取權限、資料加密、傳輸加密、資料遮蔽、人員置 對人處理規範等。 第二十條 訂定到職、在職及離職管理程序,並簽署保密協議明確告知保密事項。 第二十條 訂定到職、在職及離職管理程序,並簽署保密協議明確告知保密事項。 第二十一條 定期審查特權帳號、使用者帳號及嚴定、如:預設密碼、密碼長度、密碼複報查,多重的資源系統採取多重認證技術。 第二十二條 定期審查特權帳號、使用者帳號及權限、停用久未使用之帳號。 建立資通系統及相關與廣適當之監控措施,如;身分驗證失敗、存取資策。 第二十二條 定期審查特權帳號、使用者帳號及權限、停用久未使用之帳號。 第二十二條 定期審查持權帳號、使用者帳號及權限、停用久未使用之帳號。 第二十二條 定期審查持權帳號、使用者帳號及權限、停用久未使用之帳號。 第二十二條 定期審查持權帳號、使用者帳號及權限、停用久未使用之帳號。 第二十二條 定期審查持權帳號、使用者帳號及權限、等即,分驗證失敗、存取資第一十一條 方則等項目建立適當之管理措施。 第二十五條 定期審查持之保護機制。 第二十五條 官意安全漏洞通告,即時修補高風險漏洞,定期評估辦理設備、系統元作、資料庫系統及軟體安全性漏洞修補。 第三十五條 訂定資通設衡回收再使用及汰除之安全控制作業程序,以確保機敏性資料確實刪除。日 訂定人員裝置使用管理規範、如:軟體安裝、電子郵件、即時通訊軟	第六章>>資	፻通安全防護及控制措施		
一、防毒軟體。 二、網路防火牆。 二、網路防火牆。 三、如有郵件伺服器者。具備電子郵件過濾機制。 四、入侵偵測及防禦機制。 五、如有對外服務之核心資通系統者、具備應用程式防火牆。 一、進階持續性威脅攻擊防禦措施。 中、資通安全威脅偵測管理機制(SOC)。 針對機敏性資料之處理及儲存建立適當之防護措施,如:實體隔離、專用電腦作業環境、存取權限、資料加密、傳輸加密、資料遮蔽、人員管理及處理規範等。 第二十條 訂定到職、在職及雕雕管理程序,並簽署保密協議明確告知保密事項。 建立使用者通行碼管理程序,並簽署保密協議明確告知保密事項。 建立使用者通行碼管理程序,並簽署保密協議明確告知保密事項。 建立使用者通行碼管理程序,並簽署保密協議明確告知保密事項。 建立使用者通行碼管理程序,並簽署保密協議明確告知保密事項。 建立使用者通行碼管理程序,如:預設密碼、密碼長度、密碼複將 中多重認證技術。 第二十一條 定期審查特權帳號、使用者帳號及權限,停用久未使用之帳號。 建立資通系統及相關設備適當之監控措施,如:身分驗證失敗、存取資第二十二條 定期審查特權帳號、使用者帳號及權限,停用久未使用之帳號。 建立資通系統及相關設備適當之監控措施。 第二十二條 定期審查特權帳號、使用者帳號及權限,停用久未使用之帳號。 建立資通系統及相關設備適當之監控措施,如:身分驗證失敗、存取資第二十二條 定期審查方案 建立資通系統及權限,停用久未使用之帳號。 建立資通系統及相關設備適當之監控措施,如:身分驗證失敗、存取資等上期審查方案 建立資通手權帳號、使用者帳號及管理者行為等,並針對十二次期審查方案 建立資通手權帳號、使用者帳號及管理者行為等,並針對十二次期審查方案 建立資通手權帳號、使用者帳號及管理者行為等,並針對十二次期審查方案 建立資通手權帳號、使用者帳號及管理者行為等,並針對十二次期審查方案 是期審查方案 建立資通手權帳號、使用者帳號及管理者行為等,並對應於實施,上述期審查方案 是期審查方案 是期審查方案 是期審查方案 是期審查方案 是期審查方案 上述明審查方案 上述明確議(如溫潛方案)上述明述所述的。如溫潤可能之可能,可能達成例。	第十七條	並將開發、測試及正式作業環境區隔,且針對不同作業環境	+網路區隔	
□、 網路防火牆。 □、 如有郵件伺服器者,具備電子郵件過濾機制。 □、 入侵偵測及防禦機制。 五、 如有對外服務之核心資通系統者,具備應用程式防火牆。 六、 進階持續性威脅攻擊防禦措施。 七、 資通安全威脅偵測管理機制(SOC)。 針對機敏性資料之處理及儲存建立適當之防護措施,如:實體隔離、專用電腦作業環境、存取權限、資料加密、資料遮蔽、人員管理及處理規範等。 第二十條 訂定到職、在職及離職管理程序,並簽署保密協議明確告知保密事項。 建立使用者通行碼管理之作業規定,如:預設密碼、密碼長度、密碼複額上,並評估於核心資通系統採取多重認證技術。 第二十一條 定期審查特權帳號、使用者帳號及權限,停用久未使用之帳號。 建立資通系統及相關設備適常之監控措施,如:身分驗證失敗、存取資源失敗、重要資料異動、功能錯誤及管理者行為等,並針對十之關稅,並可發通之安全控制、人員進出管控、環境維護(如溫潛第二十三條度,則等項目建立適當之管理措施。 第二十一條 實際安全漏洞通告,即時修補高風險漏洞,定期評估辦理設備、系統元件、資料庫系統及軟體安全性漏洞修補。 第二十五條 留意安全漏洞通告,即時修補高風險漏洞,定期評估辦理設備、系統元件、資料庫系統及軟體安全性漏洞修補。 第二十六條 智利庫系統及軟體安全性漏洞修補。 第二十六條 對電腦發房及重要區域之安全控制作業程序,以確保機敏性資料確實删除。□				_
第十八條 三、如有郵件伺服器者・具備電子郵件過濾機制。 四、入侵偵測及防禦機制。 五、如有對外服務之核心資通系統者・具備應用程式防火牆。 六、進階持續性威脅攻擊防禦措施。 七、資通安全威脅偵測管理機制(SOC)。 針對機敏性資料之處理及儲存建立適當之防護措施・如:實體隔離、專 用電腦作業環境、存取權限、資料加密、資料遮蔽、人員實 理及處理規範等。 第二十條 訂定到職、在職及離職管理程序,並簽署保密協議明確告知保密事項。 建立使用者通行碼管理之性業規定,如:預設密碼、密碼長度、密碼複 雜度、密碼歷程記錄、密碼最短及最長之效期限制、登入失敗鎖定機制。 並評估於核心資通系統採取多重認證技術。 第二十一條 定期審查特權帳號、使用者帳號及權限,停用久未使用之帳號。 建立資通系統及相關設備適當之監控措施,如:身分驗證失敗、存取資 第二十三條 定期審查特權帳號、使用者帳號及權限,停用久未使用之帳號。 建立資通系統及相關設備適當之監控措施,如:身分驗證失敗、存取資 第二十三條 定期審查符權帳號、使用者帳號及權限,停用久未使用之帳號。 建立資通系統及相關設備適當之監控措施,如:身分驗證失敗、存取資 第二十一條 定期審查持權帳號、使用者帳號及權限,停用久未使用之帳號。 建立資通系統及相關設備適當之監控措施,如:身分驗證失敗、存取資 第二十一條 定期審查符權帳號、使用者帳號及權限,停用久未使用之帳號。 建立資通系統及相關設備適當之監控措施,如:身分驗證失敗、存取資 第二十一條 定期審查持權帳號、使用者帳號及管理者行為等,並針對 日誌建立適當之保護機制。 第二十一條 實制體限及重要區域之安全控制、人員進出管控、環境維護(如溫溼 非二次所不等,上監視部別 第二十一條 實利與重義的人員進出管控、環境維護(如溫溼 非二次所不等,上監視部別 第二十一條 實利與重義的人員進出管控、環境維護(如溫溼 非二次所不等,上監視部別 非二次所有。 第二十一條 實利條即以再使用及法除之安全控制作業程序,以確保機敏性資料確實刪除。 訂定資通設備回收再使用及法除之安全控制作業程序,以確保機敏性資料確實刪除。 訂定人員裝置使用管理規範,如:軟體安裝、電子郵件、即時通訊軟		· · · · · · · · · · · · · · · · · · ·		-
第十八條 四、入侵偵測及防禦機制。 五、如有對外服務之核心資通系統者,具備應用程式防火牆。 六、進階持續性威脅攻擊防禦措施。 七、資通安全威脅偵測管理機制(SOC)。 針對機敏性資料之處理及儲存建立適當之防護措施,如:實體隔離,專用電腦作業環境、存取權限、資料加密、傳輸加密、資料遮蔽、人員管理及處理規範等。 第二十條 訂定到職、在職及離職管理程序,並簽署保密協議明確告知保密事項。 建立使用者通行碼管理之作業規定,如:預設密碼、密碼長度、密碼複維的。 第二十一條 建立使用者通行碼管理之作業規定,如:預設密碼、密碼長度、密碼複維的 大資 法務 全 中面 上海 大學				-
五、如有對外服務之核心資通系統者,具備應用程式防火牆。 六、進階持續性威脅攻擊防禦措施。 七、資通安全威脅偵測管理機制(SOC)。 針對機敏性資料之處理及儲存建立適當之防護措施,如:實體隔離、專用電腦作業環境、存取權限、資料加密、資料遮蔽、人員管 + 5 資料加密方案 + 5 以相應管理 + 5 以相應管理 + 5 以相應管理 + 5 以相應等 第二十條 訂定到職、在職及離職管理程序,並簽署保密協議明確告知保密事項。 第二十條 訂定到職、在職及離職管理程序,並簽署保密協議明確告知保密事項。 建立使用者通行碼管理之作業規定,如:預設密碼、密碼長度、密碼複 # 4 A D 架構建置 + 3 重認證技術 第二十一條 雜度、密碼歷程記錄、密碼展短及最長之效期限制、登入失敗鎖定機制 + 3 重認證技術 第二十二條 定期審查特權帳號、使用者帳號及權限,停用久未使用之帳號。 建立資通系統及相關設備適當之監控措施,如:身分驗證失敗、存取資 # 5 IEM監控方案 日誌建立適當之保護機制,功能錯誤及管理者行為等,並針對 + 5 IEM監控方案 日誌建立適當之保護機制。 第二十四條 針對電腦機房及重要區域之安全控制、人員進出管控、環境維護(如溫溼度控制)等項目建立適當之管理措施。 第二十四條 留意安全漏洞通告,即時修補高風險漏洞,定期評估辦理設備、系統元 件、資料庫系統及軟體安全性漏洞修補。 + 1 無關後補 表統 + 1 未漏源修補系統 + 1 上 條 對電腦機房及重要區域之安全控制 ← 2 財評估辦理設備、系統元 件、資料庫系統及軟體安全性漏洞修補。 + 1 上 6 訂定資通設備回收再使用及汰除之安全控制作業程序,以確保機敏性資料確實删除。□	第十八條			-
一一十一條 一一大學 一一大學 一一大學 一一大學 一一大學 一一大學 一一大學 一一大學 一一大學 一一大學 一一大學 一一大學 一一大學 一一大學 一一				-
### ### ### ### ### ### ### ### ### ##				-
第十九條 用電腦作業環境、存取權限、資料加密、傳輸加密、資料遮蔽、人員管 理及處理規範等。 第二十條 訂定到職、在職及離職管理程序,並簽署保密協議明確告知保密事項。 第二十條 訂定到職、在職及離職管理程序,並簽署保密協議明確告知保密事項。 建立使用者通行碼管理之作業規定,如:預設密碼、密碼長度、密碼複 +AD架構建置 +多重認證技術。 第二十一條 雜度、密碼歷程記錄、密碼最短及最長之效期限制、登入失敗鎖定機制 +多重認證技術。 第二十二條 定期審查特權帳號、使用者帳號及權限,停用久未使用之帳號。 #定期審查方案 建立資通系統及相關設備適當之監控措施,如:身分驗證失敗、存取資 源失敗、重要行為、重要資料異動、功能錯誤及管理者行為等,並針對 +SIEM監控方案 日誌建立適當之保護機制。 第二十四條 對對電腦機房及重要區域之安全控制、人員進出管控、環境維護(如溫溼度控制)等項目建立適當之管理措施。 #門等万案 +監視錄影 +監視錄影 +温濕度監控 +漏洞修補系統 + 監視錄影 + 無洞修補系統 + 虛擬補丁 訂定資通設備回收再使用及汰除之安全控制作業程序,以確保機敏性資料確實刪除。日 訂定人員裝置使用管理規範,如:軟體安裝、電子郵件、即時通訊軟 人資		七、 資通安全威脅偵測管理機制(SOC)。		<u>-</u>
第二十條 第二十條	第十九條	用電腦作業環境、存取權限、資料加密、傳輸加密、資料遮蔽、人員管	+資料加密方案 +SSL傳輸加密	
第二十一條 雜度、密碼歷程記錄、密碼最短及最長之效期限制、登入失敗鎖定機制 + AD架構建置 + 多重認證技術。 第三十三條 定期審查特權帳號、使用者帳號及權限・停用久未使用之帳號。 + 定期審查方案 建立資通系統及相關設備適當之監控措施,如:身分驗證失敗、存取資	第二十條	訂定 到職、在職及離職 <u>管理程序</u> ・並簽署 <u>保密協議</u> 明確告知保密事項。		
建立資通系統及相關設備適當之監控措施,如:身分驗證失敗、存取資源失敗、重要行為、重要資料異動、功能錯誤及管理者行為等,並針對 + SIEM監控方案日誌建立適當之保護機制。 第二十四條 針對電腦機房及重要區域之安全控制、人員進出管控、環境維護(如溫潛度控制)等項目建立適當之管理措施。 第二十五條 留意安全漏洞通告,即時修補高風險漏洞,定期評估辦理設備、系統元件、資料庫系統及軟體安全性漏洞修補。 第二十六條 訂定資通設備回收再使用及汰除之安全控制作業程序,以確保機敏性資料確實刪除。日	第二十一條	雜度、密碼歷程記錄、密碼最短及最長之效期限制、登入失敗鎖定機制		
第二十三條 源失敗、重要行為、重要資料異動、功能錯誤及管理者行為等,並針對 +SIEM監控方案 日誌建立適當之保護機制。 第二十四條 針對電腦機房及重要區域之安全控制、人員進出管控、環境維護(如溫溼度控制)等項目建立適當之管理措施。 第二十五條 留意安全漏洞通告,即時修補高風險漏洞,定期評估辦理設備、系統元件、資料庫系統及軟體安全性漏洞修補。 第二十六條 訂定資通設備回收再使用及汰除之安全控制作業程序,以確保機敏性資料確實刪除。日	第二十二條	定期審查特權帳號、使用者帳號及權限,停用久未使用之帳號。	+定期審查方案	_
第二十四條 對對電腦機房及重要區域之安主控制、人員建出管控、環境維護(如温率 +監視錄影	第二十三條	源失敗、重要行為、重要資料異動、功能錯誤及管理者行為等,並針對	+SIEM監控方案	
#二十五條 件、資料庫系統及軟體安全性漏洞修補。 +虛擬補丁 # # # # # # # # # # # # # # # # # # #	第二十四條		+監視錄影	
第一十六條 料確實刪除。□ 第一十七條 第二十七條 第二十七條 第二十七條 11定人員裝置使用管理規範,如:軟體安裝、電子郵件、即時通訊軟	第二十五條			_
	第二十六條			
	第二十七條			人資
第二十八條 行教育訓練·並留存相關紀錄。 本語報告表表表表表表表表表表表表表表表表表表表表表表表表表表表表表表表表表表表表	第二十八條			人資

第七章>>資	通系統或資通服務委外辦理之管理措施					
第二十九條	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·確保委外廠商執行委外作業時·具備完善之資通安全管理措施。		採購			
第三十條	訂定 委外廠商之資通 安全責任及保密規定 ,於採購文件中 載明 服務水準協議(SLA)、資安要求及對委外廠商資安稽核權。		法務 廠商			
第三十一條	公司於委外關係終止或解除時,確認委外廠商返還、移交、刪除或銷毀 履行契約而持有之資料。					
第八章>>資	通安全事件通報應變及情資評估因應		-			
第三十二條	訂定資安事件 <u>應變處置及通報作業程序</u> ,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。		事件 應變 小組			
第三十三條	加入資安情資分享組織,取得資安預警情資、資安威脅與弱點資訊,如:所屬產業資安資訊分享與分析中心(ISAC)、臺灣電腦網路危機處理暨協調中心(TWCERT/CC)。					
第三十四條	發生符合「臺灣證券交易所股份有限公司對有價證券上市公司重大訊息 之查證暨公開處理程序」或「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。	財務人員	發言人			
第九章>>資	通安全之持續精進及績效管理機制					
第三十五條	資通安全推動組織 定期向 董事會或管理階層報告資通安全執行情形·確保運作之適切性及有效性。					
第三十六條	定期辦理 內部及委外廠商之資安稽核·並就發現事項擬訂改善措施·且 定期追蹤改善情形。		稽核			
第十章>>附則						
第三十七條	除法令、臺灣證券交易所股份有限公司及財團法人中華民國證券櫃檯買 賣中心相關章則另有規定外,本指引條文,上市、上櫃公司可衡諸產業 特性、規模大小及資安風險適度採行之。					