附件9

|  |
| --- |
| **參加軍品研發產製維修作業委外廠商資通安全規範查核報告(參考格式)** |
| 法人團體 | ○○股份有限公司 |
| 資安防護查核等級 | □普級 □中級 □高級 |
| 查核時間 | 民國○年○月○日○時 |
| 查核項目統計 | 資通安全維護計畫 | 1. 資通安全政策之推動及目標訂定計5項，\_\_\_項符合，\_\_\_\_項不符合。
2. 設置資通安全推動組織計3項，\_\_\_項符合，\_\_\_\_項不符合。
3. 配置適當之資通安全專業人員及適當之資源計4項，\_\_\_項符合，\_\_\_\_項不符合。
4. 資訊及資通系統之盤點及風險評估計4項，\_\_\_項符合，\_\_\_\_項不符合。
5. 資通安全管理措施之實施情況計34項，\_\_\_項符合，\_\_\_\_項不符合。
6. 訂定資通安全事件通報及應變之程序及機制計3項，\_\_\_項符合，\_\_\_\_項不符合。
7. 定期辦理資通安全認知宣導及教育訓練計4項，\_\_\_項符合，\_\_\_\_項不符合。
8. 資通安全維護計畫實施情形之精進改善機制計4項，\_\_\_項符合，\_\_\_\_項不符合。
9. 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計3項，\_\_\_項符合，\_\_\_\_項不符合。

合計64項，\_\_\_\_項符合，\_\_\_\_項不符合。 |
| 資通系統技術要求 | 1. 存取控制計3項，\_\_\_項符合，\_\_\_\_項不符合。
2. 稽核與可歸責性計6項，\_\_\_項符合，\_\_\_\_項不符合。
3. 營運持續計畫計2項，\_\_\_項符合，\_\_\_\_項不符合。
4. 識別與鑑別計4項，\_\_\_項符合，\_\_\_\_項不符合。
5. 系統與服務獲得計7項，\_\_\_項符合，\_\_\_\_項不符合。
6. 系統與通訊保護計2項，\_\_\_項符合，\_\_\_\_項不符合。
7. 系統與資訊完整性計2項，\_\_\_項符合，\_\_\_\_項不符合。

合計26項，\_\_\_\_項符合，\_\_\_\_項不符合。 |
| 鑑定標準 | (1) 「合格」：各項檢核項目均須符合，判定為合格。(2) 「部分符合」：若有五項(含)以下不符合者，須於14天內補正改善；補正後若達「合格」標準判定為合格，其餘為「不合格」。(3) 「不合格」：若有超過六項(含)以上不符合者，判定為不合格。 |
| 結果評定 | □合 格。□部分符合。□不 合 格。 | 備考 |  |
| 資安驗證機構簽署 |  | 查核機構聯絡資訊 | 機構認證編號：電話：傳真： |
| 查核人員簽章 |  | 主導稽核員證照登錄號碼 |  |
| 報告簽署日期 | 民國○年○月○日 |
| **1.法人團體請先期規劃資通安全防護規範(CNS 27001)導入及執行事宜。****2.本查核報告近1年為自查核日起算個月內，逾效期須重行辦理資安防護規範驗證事宜。** |

資訊安全查核項目(區分兩部分：資通安全維護計畫、資通系統技術要求)

一、資通安全維護計畫(共通性要求)

|  |  |  |  |
| --- | --- | --- | --- |
| 查核項目 | 查核內容 | 等級區分 | 備考 |
| 高 | 中 | 普 |
| **1.**資通安全政策之推動及目標訂定 | 1.1 是否定義符合組織需要之資通安全政策及目標？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 1.2 組織是否訂定資通安全政策及目標？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 1.3 組織之資通安全政策文件是否由管理階層核准並正式發布且轉知所有同仁？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 1.4 組織是否對資通安全政策、目標之適切性及有效性，定期作必要之審查及調整？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 1.5 是否隨時公告資通安全相關訊息？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
| **2.**設置資通安全推動組織 | 2.1 是否指定適當權責之高階主管負責資通安全管理之協調、推動及督導等事項？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 有設置內部資通安全推動小組，並制訂相關之權責分工。 | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 2.3 是否訂定組織之資通安全責任分工？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
| **3.**配置適當之資通安全專業人員及適當之資源 | 3.1 是否訂定人員之安全評估措施？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 3.2 是否符合組織之需求配置專業資安人力？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 3.3 是否具備相關專業資安證照或認證？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 3.4 是否配置適當之資源？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
| **4.**資訊及資通系統之盤點及風險評估 | 4.1 是否建立資訊及資通系統資產目錄，並隨時維護更新？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 4.2 各項資產是否有明確之管理者及使用者？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 4.3 是否定有資訊、資通系統分級與處理之相關規範？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 4.4 是否進行資訊、資通系統之風險評估，並採取相應之控制措施？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
| **5.**資通安全管理措施之實施情況 | 5.1 人員進入重要實體區域是否訂有安全控制措施？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 5.2 重要實體區域的進出權利是否定期審查並更新？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 5.3 電腦機房及重要地區，對於進出人員是否作必要之限制及監督其活動？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 5.4 電腦機房操作人員是否隨時注意環境監控系統，掌握機房溫度及溼度狀況？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 5.5 各項安全設備是否定期檢查？同仁有否施予適當的安全設備使用訓練？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 5.6 第三方支援服務人員進入重要實體區域是否經過授權並陪同或監視？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 5.7 重要資訊處理設施是否有特別保護機制？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 5.8 重要資通設備之設置地點是否檢查及評估火、煙、水、震動、化學效應、電力供應、電磁幅射或民間暴動等可能對設備之危害？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 5.9 電源之供應及備援電源是否作安全上考量？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 5.10 通訊線路及電纜線是否作安全保護措施？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 5.11 設備是否定期維護，以確保其可用性及完整性？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 5.12 設備送場外維修，對於儲存資訊是否訂有安全保護措施？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 5.13 可攜式的電腦設備是否訂有嚴謹的保護措施(如設通行碼、檔案加密、專人看管)？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 5.14 設備報廢前是否先將機密性、敏感性資料及版權軟體移除或覆寫？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 5.15 公文及儲存媒體在不使用或不在班時是否妥為存放？機密性、敏感性資訊是否妥為收存？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 5.16 系統開發測試及正式作業是否區隔在不同之作業環境？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 5.17 是否全面使用防毒軟體並即時更新病毒碼？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 5.18 是否定期對電腦系統及資料儲存媒體進行病毒掃瞄？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 5.19 是否定期執行各項系統漏洞修補程式？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 5.20 是否要求電子郵件附件及下載檔案在使用前需檢查有無惡意軟體(含病毒、木馬或後門等程式)？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 5.21 重要的資料及軟體是否定期作備份處理？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 5.22 備份資料是否定期回復測試，以確保備份資料之有效性？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 5.23 對於敏感性、機密性資訊之傳送是否採取資料加密等保護措施？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 5.24 是否訂定可攜式媒體(磁帶、磁片、光碟片、隨身碟及報表等)管理程序？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 5.25 是否訂定使用者存取權限註冊及註銷之作業程序？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 5.26 使用者存取權限是否定期檢查(建議每六個月一次)或在權限變更後立即複檢？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 5.27 通行碼長度是否超過6個字元(建議以8位或以上為宜)？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 5.28 通行碼是否規定需有大小寫字母、數字及符號組成？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 5.29 是否依網路型態(Internet、Intranet、Extranet)訂定適當的存取權限管理方式？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 5.30 對於重要特定網路服務，是否作必要之控制措施，如身份鑑別、資料加密或網路連線控制？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 5.31 是否訂定行動式電腦設備之管理政策(如實體保護、存取控制、使用之密碼技術、備份及病毒防治要求)？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 5.32 重要系統是否使用憑證作為身份認證？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 5.33 系統變更後其相關控管措施與程序是否檢查仍然有效？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 5.34 是否可及時取得系統弱點的資訊並作風險評估及採取必要措施？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
| **6.**訂定資通安全事件通報及應變之程序及機制 | 6.1 是否建立資通安全事件發生之通報應變程序？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 6.2 機關同仁及外部使用者是否知悉資通安全事件通報應變程序並依規定辦理？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 6.3 是否留有資通安全事件處理之記錄文件，記錄中並有改善措施？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
| **7.**定期辦理資通安全認知宣導及教育訓練 | 7.1 是否定期辦理資通安全認知宣導？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 7.2 是否對同仁進行資安評量？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 7.3 同仁是否依層級定期舉辦資通安全教育訓練？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 7.4 同仁是否瞭解單位之資通安全政策、目標及應負之責任？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
| **8.**資通安全維護計畫實施情形之精進改善機制 | 8.1 是否設有稽核機制？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 8.2 是否定有年度稽核計畫？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 8.3 是否定期執行稽核？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 8.4 是否改正稽核之缺失？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
| **9.** 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  | 9.1 是否訂定安全維護計畫持續改善機制？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 9.2 是否追蹤過去缺失之改善情形？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 9.3 是否定期召開持續改善之管理審查會議？ | ☑ | ☑ | ☑ | □ 適用 □不適用 |

二、資通系統技術要求(產品研發、產製、維修交付相關系統適用)

|  |  |  |  |
| --- | --- | --- | --- |
| 查核項目 | 查核實作內容 | 等級區分 | 備考1. 普級需檢附符合資安規範之佐證文件。
2. 中、高級需檢具符合資安規範之程序書備驗。
 |
| 高 | 中 | 普 |
| 1.存取控制 |  |  |  |  |  |
| 1.1帳號管理  | 1.1.1使用者的會談階段，設定該帳號在合理的時間(至多30分鐘)內未活動即自動失效  | ☑ | ☑ | ☑ | □ 適用 □不適用 |
| 1.1.2使用者的會談階段在登出後失效  | ☑ | ☑ | ☑ | □ 適用 □不適用 |
| 1.1.3管理者介面限制存取來源或不允許遠端存取  | ☑ | ☑ | ☑ | □ 適用 □不適用 |
| 1.2最小權限 | 1.2.1對使用者/角色，僅賦予所需要的最低權限  | ☑ | ☑ | □ | □ 適用 □不適用 |
| 1.2.2軟體程序(process)及伺服器服務，以一般使用者權限執行，不以系統管理員或最高權限  | ☑ | ☑ | □ | □ 適用 □不適用 |
| 1.3遠端存取  | 1.3.1採用伺服端的集中過濾機制檢查使用者授權  | ☑ | ☑ | ☑ | □ 適用 □不適用 |
| 2.稽核與可歸責性 |  |  |  |  |  |
| 2.1稽核事件  | 2.1.1針對身分鑑別失敗、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進行日誌記錄  | ☑ | ☑ | ☑ | □ 適用 □不適用 |
| 2.1.2應稽核資訊系統管理者帳號所執行之各項功能  | ☑ | ☑ | ☑ | □ 適用 □不適用 |
| 2.2稽核紀錄內容  | 2.2.1日誌紀錄包含以下項目1.識別使用者之ID(不可為個資類型)。2.經系統校時後的時間戳記。3.執行的功能或存取的資源。4.事件類型或等級(priority)。5.事件描述 | ☑ | ☑ | ☑ | □ 適用 □不適用 |
| 2.2.2採用單一的日誌紀錄機制，確保輸出格式的一致性  | ☑ | ☑ | ☑ | □ 適用 □不適用 |
| 2.3稽核儲存容量 | 2.3.1依據稽核紀錄儲存需求，配置稽核紀錄所需之儲存容量 | ☑ | ☑ | ☑ | □ 適用 □不適用 |
| 2.4稽核處理失效之回應 | 2.4.1資訊系統應在稽核處理失效(如儲存容量不足)之情況下，採取適當之行動，例如：關閉資訊系統、覆寫最舊的稽核紀錄或停止產生稽核紀錄等。 | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 2.4.2當機關規定需要即時通報的稽核失效事件發生時，資訊系統應在機關規定之時效內，對機關特定之人員、角色提出告警(適用於高等級) | ☑ | □ | □ | □ 適用 □不適用 |
| 2.5時戳 | 2.5.1資訊系統應使用系統內部時鐘產生稽核紀錄所需時戳，並可以對映到世界協調時間(UTC)或格林威治標準時間(GMT) | ☑ | ☑ | ☑ | □ 適用 □不適用 |
| 2.5.2系統內部時鐘應具備定期同步機制 | ☑ | ☑ | ☑ | □ 適用 □不適用 |
| 2.6稽核資訊之保護 | 2.6.1對日誌紀錄進行適當保護及備份，避免未經授權存取 | ☑ | ☑ | ☑ | □ 適用 □不適用 |
| 2.6.2定期備份稽核紀錄到與原稽核系統不同之實體系統 (如Log伺服器) | ☑ | ☑ | ☑ | □ 適用 □不適用 |
| 2.6.3重要系統資料或紀錄留存雜湊值以確保完整性 | ☑ | □ | □ | □ 適用 □不適用 |
| 3.營運持續計畫 |  |  |  |  |  |
| 3.1資訊系統備份 | 重要資料定時同步至備份或備援環境，並加以保護限制存取 | ☑ | ☑ | ☑ | □ 適用 □不適用 |
| 3.2資訊系統備援 | 採用「高可用性」(High Availability) 架構(分散式或叢集伺服器架構) | ☑ | □ | □ | □ 適用 □不適用 |
| 4.識別與鑑別 |  |  |  |  |  |
| 4.1內部使用者之識別與鑑別 | 4.1.1採用多重因素身分鑑別(兩種以上驗證類型) | ☑ | □ | □ | □ 適用 □不適用 |
| 4.1.2資訊系統在建立連線前，應識別允許存取之特定來源(如IP) | ☑ | □ | □ | □ 適用 □不適用 |
| 4.2身分鑑別管理 | 4.2.1確實規範使用者密碼強度(密碼長度12個字元以上、包含英文大小寫、數字，以及特殊字元) | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 4.2.2使用者必須定期更換密碼，且至少不可以與前3次使用過之密碼相同 | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 4.2.3具備帳號鎖定機制，帳號登入進行身分鑑別失敗達5次後，至少15分鐘內不允許該帳號及來源IP繼續嘗試登入 | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 4.2.4身分鑑別相關資訊不以明文傳輸 | ☑ | ☑ | ☑ | □ 適用 □不適用 |
|  | 採用圖形驗證碼(CAPTCHA)機制於身分鑑別及重要交易行為，以防範自動化程式之嘗試 | ☑ | ☑ | □ | □ 適用 □不適用 |
|  | 4.2.5密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性令牌(Token)，檢查傳回令牌有效性後，才允許使用者進行重設密碼動作 | ☑ | ☑ | □ | □ 適用 □不適用 |
| 4.3鑑別資訊回饋 | 資訊系統應遮蔽在鑑別過程中之資訊(如密碼)，以防止未授權之使用者可能之窺探/使用 | ☑ | ☑ | ☑ | □ 適用 □不適用 |
| 4.4加密模組鑑別 | 密碼添加亂數(Salt)進行雜湊函式(HASH Function)處理後，分別儲存亂數及雜湊後密碼 | ☑ | ☑ | □ | □ 適用 □不適用 |
| 5.系統與服務獲得 |  |  |  |  |  |
| 5.1安全系統發展生命週期需求階段 | 針對系統安全需求，以檢核表方式進行確認 | ☑ | ☑ | ☑ | □ 適用 □不適用 |
| 5.2安全系統發展生命週期設計階段安全系統發展生命週期開發階段 | 5.2.1應根據系統功能與要求，識別可能影響系統之威脅，進行風險分析與評估 | ☑ | ☑ | □ | □ 適用 □不適用 |
| 5.2.2將風險評估結果回饋需求階段的檢核項目，並提出安全需求修正 | ☑ | ☑ | □ | □ 適用 □不適用 |
| 5.2.3具有防範SQL命令注入攻擊(SQL Injection)之措施 | ☑ | ☑ | ☑ | □ 適用 □不適用 |
| 5.2.4具有防範跨站腳本攻擊(XSS, Cross-Site Scripting)之措施 | ☑ | ☑ | ☑ | □ 適用 □不適用 |
| 5.2.5具有防範「跨站請求偽造」(Cross-Site Request Forgery, CSRF)攻擊之措施 | ☑ | ☑ | ☑ | □ 適用 □不適用 |
| 5.2.6發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細的錯誤訊息 | ☑ | ☑ | ☑ | □ 適用 □不適用 |
| 5.2.7所有功能皆進行錯誤及例外處理，並確保將資源正確釋放 | ☑ | ☑ | ☑ | □ 適用 □不適用 |
| 具備系統嚴重錯誤之通知機制(例如電子郵件或簡訊)  | ☑ | □ | □ | □ 適用 □不適用 |
| 5.3安全系統發展生命週期測試階段 | 5.3.1執行「弱點掃描」安全檢測 | ☑ | ☑ | ☑ | □ 適用 □不適用 |
| 5.3.2執行「滲透測試」安全檢測 | ☑ | □ | □ | □ 適用 □不適用 |
| 5.4安全系統發展生命週期部署與維運階段 | 5.4.1作業平台定期更新並關閉不必要服務及埠口(Port) | ☑ | ☑ | ☑ | □ 適用 □不適用 |
| 5.4.2針對系統依賴的外部元件或軟體，注意其安全漏洞通告，定期評估更新 | ☑ | ☑ | ☑ | □ 適用 □不適用 |
| 5.4.3系統依賴的外部元件或軟體，不使用預設或空的密碼 | ☑ | ☑ | ☑ | □ 適用 □不適用 |
| 5.5安全系統發展生命週期委外階段 | 資訊系統開發若委外服務應將系統發展生命週期各階段依安全等級將安全需求納入委外合約 | ☑ | ☑ | ☑ | □ 適用 □不適用 |
| 5.6獲得程序 | 開發、測試以及正式作業環境應作區隔 | ☑ | ☑ | ☑ | □ 適用 □不適用 |
| 5.7資訊系統文件 | 應儲存與管理系統發展生命週期之相關文件 | ☑ | ☑ | ☑ | □ 適用 □不適用 |
| 6.系統與通訊保護 |  |  |  |  |  |
| 6.1傳輸之機密性與完整性 | 6.1.1機敏資料傳輸時，採用加密機制 | ☑ | ☑ | □ | □ 適用 □不適用 |
| 6.1.2使用公開、國際機構驗證且未遭破解的演算法 | ☑ | □ | □ | □ 適用 □不適用 |
| 6.2資料儲存之安全 | 6.2.1參數設定或系統設定存放處，限制存取或進行適當保護 | ☑ | □ | □ | □ 適用 □不適用 |
| 6.2.2機敏資料儲存時，採用加密機制 | ☑ | □ | □ | □ 適用 □不適用 |
| 7.系統與資訊完整性 |  |  |  |  |  |
| 7.1資訊系統監控 | 7.1.1發現資訊系統有被入侵跡象時，應通報機關特定人員 | ☑ | ☑ | ☑ | □ 適用 □不適用 |
| 7.1.2監控資訊系統，以偵測攻擊和未授權之連線，並識別資訊系統之未授權使用 | ☑ | ☑ | □ | □ 適用 □不適用 |
| 7.1.3資訊系統應採用自動化工具監控進出之通信流量，並於發現不尋常或未授權之活動時針對該事件進行分析 | ☑ | □ | □ | □ 適用 □不適用 |
| 7.2軟體及資訊完整性 | 於伺服器端以正規表示式(Regular Expression)方式，檢查使用者輸入資料合法性 | ☑ | ☑ | □ | □ 適用 □不適用 |

法人團體代表： 資通安全單位主管：