ISO :27001:2013

資訊安全管理系條文

1. **簡介**
   1. **概述**

本標準之制定係為提供以建立、實作、維護與持續改進資訊安全管理系統。採用資訊安全管理系統細微組織的策略性決策。組織資訊安全管理系統的建立與實作受其需求與目標、安全要求、所採用的組織流程，以及組織之規模與架構所影響。所有的影響因素預期將會隨時間而有所改變。

資訊安全安全管理系統係透過採用風險管理流程來維護資訊的機密性、完整性與可用性，並讓利害相關團體因認為風險已經被適切地管理而產生信心。

重要的事是，將資訊安全管理系統組織流程的一部分，並應與組織流程及整體管理架構整合；並應在流程、資訊系統與控制措施的設計中將資訊安全列入考量。可預期的是資訊安全管理系統實作將依組織需求加以達成。

本標準可由內部或外部團體使用評估組織達成本身資訊安全要求事項的能力。

本標準要求市鄉的排列順序並不能用以反映其中要程度，或作為實作的優先順序。所驢列之編號僅作為參考之用。

ISO/IEC 27000描述資訊安全管理系統的概述與字彙，以提供所有資訊安全管理系統標準家族 (包含 ISO/IEC 27003, ISO/IEC 2004 and ISO/IEC 27005),的相關用語與釋義。

* 1. **與其他管理系統之相容性**

本標準採用高階架構，相同的刺條款標，相同的內容，共通的用語，以及界定於Annex SL of ISO/IEC Directives, Part 1 , Consolidated ISO Supplement,的核心定義，因此可以維持與其他採用Annex SL管理系統的標準的一致性。

定義於Annex SL 的通用方法，對於選擇利用單一管理系統來遵循兩種以上管理系統要求的組織，將是非常有用的。

1. **適用範圍**

本標準係規範建立、實作、維持即持續改善組織範圍內的資訊安全管理系統的要求事項。本標準亦包含符合組織需求之資訊安全風險評鑑與處理的要求事項。本標準的要求事項為一般性要求，適用各類組織，無論其形態、規模與性質。在組織宣稱符合本標準時，排除條款4至10所規定之任何要求，均不被接受。

1. **引用標準**

下列為本標準完全或部分引用之參考文件，為本標準應用時不可或缺之文件。有日期註記的引用標準，僅適用於註記引用的版本。未註記日期的引用標準，則是用於該引用標準的最新版本（包括任何修訂）。

ISO/IEC 27000, *資訊技術－安全技術－資訊安全管理系統－概述與字彙。*

1. **用語釋義**

為本文件使用目的，用語與定義請參照 ISO/IEC 27000。

1. **組織環境**
   1. **瞭解組織及其環境**

組織應決定與組織目標相關，並會影響達成資訊安全管理系統預定成果的外部與內部議題。

*備註：決定議題可參考 ISO 31000:2009條文5.3建立組織外部與內部環境*

* 1. **了解先關利害團體需求與期望**

組織應決定：

1. 資訊安全管理系統相關的利害相關團體；與
2. 利害相關團體對資訊安全相關的要求事項。

*備註：利害相關團體的要求是向考包含法令法規要求與契約義務*

* 1. **決定資訊安全管理系統範圍**

組織應決定資訊安全管理系統的邊界與適用性來建立範圍。

在決定範圍時，組織應考量：

1. 4.1的外部與內部議題；
2. 4.2的要求事項；
3. 組織所執行的活動，以及由其他組織執行活動間的界面與相依性。

範圍應以文件化資訊方式提供使用。

* 1. **資訊安全管理系統**

組織應依據本標準要求事項，建立、實作、維護與持續改進資訊安全管理系統。

1. **領導**
   1. **領導與承諾**

高階管理階層應展現對資訊安全管理系統的領導力與承諾：

1. 確保資訊安全政策與目標建立，且切合組織策略方向；
2. 確保整合ISMS要求於組織流程中；
3. 確保ISMS所需資源得以取用；
4. 溝通有效的資訊安全管理與遵循ISMS要求的重要性；
5. 確保ISMS達成預定成效；
6. 指揮與支援人員貢獻於ISMS有效性；
7. 推動持續改善；以及
8. 支援其他管理角色來展現用於負責領域的領導性。
   1. **政策**

高階管理階層應建立資訊安全政策：

1. 切合組織目標；
2. 包含資訊安全目標或提供設定目標架構；
3. 包含滿足資訊安全相關要求的承諾；以及
4. 包含持續改善資訊安全管理系統的承諾。

資訊安全政策應該：

1. 提供文件化資訊；
2. 向全組織溝通；及
3. 適當時，提供給利害相關團體。
   1. **組織角色、責任與授權**

高階管理階層應確保資訊安全相關角色的責任與授權加以指派與溝通。

高階管理階層應指派責任與授權以：

1. 確保ISMS符合奔標準要求；及
2. 向高階管理階層報告ISMS績效。

*備註：高階管理階層也可在組織內指派資訊安全管理系統報告績效的責任與授權。*

1. **規劃**
   1. **風險與機會處理措施**
      1. **概述**

當規劃資訊安全系統時，組織應考量4.1的議題，與4.2的要求事項，以及決定應被提出的風險與機會：

1. 確保ISMS能達成預定成效；
2. 預防、或降低非預期影響；以及
3. 達成持續改善。

組織應規劃：

1. 風險與機會的處理措施，及
2. 如何
3. 將措施整合入ISMS流程並執行；以及
4. 評估措施有效性。
   * 1. **資訊安全風險評鑑**

組織應界定與應用資訊安全風險評鑑流程已：

1. 建立與維護資訊安全風險準則，包含：
2. 風險接受準則；以及
3. 決定執行資訊安全風險評鑑的準則；
4. 確保重複執行的資訊安全評鑑能產生一致、有效並可比較的結果。
5. 識別資訊安全風險。
6. 應用資訊安全風險評鑑流程來識別ISMS範圍中與資訊機密性、完整性與可用性喪失相關的風險。
7. 是險擁有者。
8. 分析資訊安全風險。
9. 評估在6.1.2 c) 1)以識別風險可能產生的潛在及果；
10. 評估在6.1.2 c) 1)以識別風險發生真正的可能性；
11. 決定風險的等級；
12. 評估資訊安全風險：
13. 將風險分析結果與6.1.2 a)建立風險準則進行比較分析；並
14. 維分析的風險排列風險處理的優先順序。

組織應維持有關資訊安全風險評鑑流程的文件化資訊。

* + 1. **資訊安全風險處理**

組織應執行資訊安全風險處理流程以：

1. 考量風險評鑑結果，選擇適切的資訊安全風險處理選項；
2. 決定所有執行資訊安全風險處理選響的控制措施；

*備註：組織可依需求設計控制措施，或是由其他資訊來識別措施。*

1. 與附錄A控制措施加以比較，以釐清無必要措施被省略；

*備註1：附錄A包含完整的控制目標與措施清單。本標準使用者依據附錄A指導來卻包不會忽略必要的控制措施。*

*附錄2：控制目標隱含於所選用的控制措施中。附錄A控制目標與措施清單並未盡列，亦可選擇其他所需的控制目標與措施。*

1. 產生適用性聲明書包含所需的控制措施（參照6.1.3 b) and c)），無論是否施行， 均應說明其選擇之理由；並應包含所排除知所有附錄A控制措施及其被排除的衡量理由；
2. 規劃資訊安全風險處理計畫；以及
3. 資訊安全風險處理計畫與殘餘風險獲得風險擁有者核准。

組織應維持有關資訊安全風險處理流程的文件化資訊。

*備註：本標準中的資訊安全風險評鑑與處理流程，英語ISO31000提供的原則與一般性指引相校準。*

* 1. **資訊安全目標與達成計畫**

組織應於適當單位與層級建立資訊安全目標。

資訊安全目標應：

1. 與資訊安全政策一致；
2. 可量測的（如可執行時）；
3. 考量應用的資訊安全要求，以及風險評鑑與處理的結果；
4. 加以溝通；以及
5. 適當更新。

組織應維持有關資訊安全目標的文件化資訊。

當規劃如何達成資安目標時，組織應決定：

1. 執行事項；
2. 所需資源；
3. 負責人員；
4. 完成時間；
5. 成果評估方式；
6. **支援**
   1. **資源**

組織應決定並提供建立、實行、維護與持續改善資訊安全管理系統所需的資源。

* 1. **能力**

組織應：

1. 決定在影響資訊安全績效控制措施下，工作人員所必備的能力；
2. 確保人員在適切教育、訓練或經驗下具備能力；
3. 適當時，採取措施已獲得必要的能力，並評估該措施的有效性：以及
4. 維持適切的文件化資訊以作為能力的證據。

*備註：適用措施可包含如對現有員工的訓練提供，監督與重新指派任務；或對於適任人員的招募與簽約等。*

* 1. **認知**

在組織管制下工作之人員應認知到：

1. 資訊安全政策；
2. 他們資訊安全管理系統有效性貢獻，其包含資訊安全績效改善的效益；以及
3. 未遵循資訊安全管理系統要求事項的意涵。
   1. **溝通**

組織應決定有關ISMS內外部溝通的需求，包含：

1. 溝通事項；
2. 溝通時機；
3. 溝通對象；
4. 應執行溝通人員；以及
5. 影響溝通的流程。
   1. **文件化資訊**
      1. **概述**

組織的ISMS應包含：

1. 本標準與組織要求的文件化資訊；以及
2. 組織決定資訊安全管系統有效性所需的文件化資訊。

*備註：ISMS的文件化資訊範圍，應依組織而有所不同，因為：*

1. *組織規模，與其活動、流程、產品以及服務的型態。*
2. *流程與其互動的複雜度；以及*
3. *人員能力。*
   * 1. **新訂與更新**

新訂與更新文件化資訊時，組織確保適當的：

1. 識別與描述（如：標題、日期、作者、或參照編號）；
2. 格式（如：語言、軟體版本與製圖）與媒體（如：紙本、電子格式），以及
3. 對適切性與正確性的審查與核准。
   * 1. **文件化資訊的管制**

ISMS與本標準所要求的文件化資訊應加以管制，以確保：

1. 在所需地點與時間，軍合適可用；並
2. 加以適當保護（如：機密性喪失、不適當利用，或完整性喪失）

文件化資訊管制應於可行時進行下列活動：

1. 分發、存取、檢索與利用；
2. 儲存與維護，包含一是別的維護；
3. 變更管制（如版本管控）；以及
4. 保存與銷毀。

由組織決定規劃與執行資訊安全管理系統所需的文件化資訊，應加以適切地識別與管制。

*備註：存取表示有關對文件化資訊僅可閱讀或是可讀寫等授權的決定。*

1. **運作**
   1. **運作規劃與控制**

組織應規劃、實作與控制達成資訊安全要求事項所需的流程與6.1決定實行的行動方案。組織也應執行計畫來達成6.2所決定的資訊安全目標。

組織應保存用來確認流程依計畫執行信心所需必要程度的文件化資訊。

組織應管制計畫性變更與審查位預期變更的結果，並於需要時，採取行動方案來降低任何不良影響。

組織應確保委外流程加以決定與管制。

* 1. **資訊安全風險評鑑**

組織應定期或於預定或執行重大變更時，執行風險評鑑，並可量6.1.2 a)所建立的準則。

組織應保存資訊安全風險評鑑結果的文件化資訊。

* 1. **資訊安全風險處理**

組織應執行資訊安全風險處理計畫。

組織應保存資訊安全風險處理結果的文件化資訊。

1. **績效評估**
   1. **量測、分析與評估**

組織應評估資訊安全績效與ISMS的有效性。

組織應決定：

1. 監視與量測項目，包含資訊安全流程與控制措施等；
2. 監視、測量、分析與評估方法，並於可行時確認結果有效；

*備註：選擇的方法宜產生可以比較與重製結果，以確認其有效。*

1. 監視與量測執行時間；
2. 監視與量測執行人員；
3. 監視與量測結果應分析與評估時間；以及
4. 分析與評估結果執行人員。
   1. **內部稽核**

組織應定期執行內部稽核以提供資訊，來確認資訊安全管理系統是否：

1. 符合
2. 組織對資訊安全管理系統的要求事項；以及
3. 本標準的要求；
4. 有效實行與維護。

組織應：

1. 規劃、建立、實作與維護稽核方案，包含頻率、方法、責任、規劃要求事項與報告等。稽核方案應將受機流程的重要性與前次稽核的結果；
2. 界定稽核準則與稽核範圍
3. 稽核員選擇與稽核執行應確保稽核流程的客觀性與公平性；
4. 確保稽核結果向相關管理單位報告；以及
5. 保存作為稽核方案與稽核結果證據的文件化資訊。
   1. **管理審查**

高階管理階層應定期審查組織ISMS已持續確保適切性、合適性與有效性。

管理審查應考量：

1. 前次管審措施狀態；
2. 資訊安全管理系統內外部議題的變更；
3. 資訊安全績效回饋，包含下列趨勢；
   1. 不符合事項與矯正措施；
   2. 監視與量測結果；
   3. 稽核結果；以及
   4. 資訊安全目標符合度；
4. 利害相關團體回饋；
5. 風險評鑑結果與風險處理計畫狀態；以及
6. 持續改善的機會。

管理審查的輸出項目應包含資訊安全管理系統持續改善機會與變更需求的決策。

組織應保存作為管理審查結果證據的文件化資訊。

1. **改善**
   1. **不符合事項與矯正措施**

不符合事項發生時，組織應：

1. 因應不符合事項，並於可行時：
2. 採取措施控制與矯正；以及
3. 處理其後果
4. 評估消除不符合事項原因措施，以使其不在發生的需求：
5. 審查不符合事項；
6. 決定不符合事項的原因；以及
7. 決定相似的不符合事項是否存在或可能發生；
8. 實行所需的措施；
9. 審查採取措施有效性；以及
10. 於需要時，對ISMS進行變更。

矯正措施應切合不符合事項所受到的影響。

組織應保存文件化資訊以作為下列的證據：

1. 不符合事項本質與所採取措施；
2. 矯正措施的結果。
   1. **持續改善**

組織應持續改善ISMS的適切性、合適性與有效性。

附錄A

**參考控制目標與控制措施**

表A.1所列之各項控制目標與控制措施，乃直接取自ISO/IEC 17002:2013條文第5 to 18節，並能用於條款6.1.3的內容。

**表1 -- 控制目標與控制措施**

**A.5 資訊安全政策**

***A.5.1 資訊安全管理方向***

目標：依照營運要求及相關法律法規， 提供管理階層對資訊安全之方向與支持。

**A.5.1.1 資訊安全政策**

*控制措施*

資訊安全相關政策應由管理階層制定、核准、公布並傳達給所有員工與相關外部團體。

**A.5.1.2 資訊安全相關政策審查**

*控制措施*

資訊安全政策應依規劃之期間或發生重大變更時審查，以確保其持續的適用性、適切性及有效性。

**A. 6 資訊安全組織**

***A.6.1 內部組織***

目標：建立用於啟動與管制組織內資訊安全實作與運作的

管理架構。

**A.6.1.1 資訊安全角色與責任**

*控制措施*

所有資訊安全責任應加以界定與安排。

**A.6.1.2 職務的區隔**

*控制措施*

具有衝突性的職務與責任領域應加以區隔，以降低

組織資產遭未經授權或非意圖的修改或誤用之機會。

**A.6.1.3 與權責機關的聯繫**

*控制措施*

應與相關權責機關維持適當聯繫。

**A.6.1 .4與特殊利害相關團體的聯繫**

*控制措施*

應與各特殊利害相關團體或其他各種專家安全性論壇及專業協會維持適當聯繫。

**A.6.1.5 事案管理的資訊安全**

*控制措施*

無論任何型態的專案，資訊安全都應在專案管理加以陳述。

***A.6.2 行動設備與遠距工作***

目標：確保遠距工作偵行動設備使用的安全

**A. 6 .2.1 行動設備政策**

*控制措施*

政策與支援性的安全措施應加以適用，以管理因使用行動設備而產生的風險。

**A.6.2.2 遠距工作**

*控制措施*

政策與支援性的安全措施應加以實作，以保護由遠距區域存取、處理與儲存的資訊。

**A.7 人力資源安全**

***A.7.1 聘僱之前***

目標：確保員工與承包者了解其責任，並勝任其所被認定的角色。

**A.7. 1. 1 篩選**

*控制措施*

應依照相關法律、法規及倫理，並兼顧營運要求的比例原則、所存取資訊的機密類別及所察覺的風險，對所有聘僱之應徵者進行背景查證檢核(verification check) 。

**A.7.1.2 聘僱條款與條件**

*控制措施*

與員工及契約人員的契約協議應陳述其與組織對資訊安全的責任。

***A.7.2 聘僱期間***

目標：確保員工與外部團體使用者認知與達成資訊安全責任。

**A.7.2.1 管理階層責任**

*控制措施*

管理階層應要求員工與契約人員，依照組織己制定的政策與程序施行安全事宜。

**A.7.2.2 資訊安全認知、教育及訓練**

*控制措施*

組織所有員工和相關的契約人員，均應接受與其工作職務相關之適切認知教育與訓練，以及定期更新的組織政策與程序內容。

**A.7.2.3 懲處過程**

*控制措施*

應有正式並已溝通的懲處過程，來採取行動處理違反資訊安全的員工。

***A.7.3 聘僱的終止或變更***

目標：將保護組織的利益，視作在變更或中止職務的流程的一部分。

**A.7.3 .1 終止或變更聘僱責任**

*控制措施*

在聘僱中止或變更後持續有效的資訊安全責任與義務，應加以界定，並向員工與契約人員溝通與執行。

**A.8 資產管理**

***A.8.1 資產責任***

目標：識別組織資產，並界定適當的保護責任。

**A.8.1.1 資產清冊**

*控制措施*

資訊與資訊處理設施相關的資產應加以識別，該資產

清單應加以製作與維護。

**A.8.1.2 資產的擁有權**

*控制措施*

資產清冊中維護的資產應有擁有者。

**A.8 .1 .3 資產之可被接受的使用**

*控制措施*

資訊與資訊處理設施相關的資訊與資產，其可被接受的使用規則應予以識別、文件化及實作。

**A.8.1.4 資產歸還**

*控制措施*

所有員工與外部團體使用者在其聘僱、契約或協議終止時，應歸還其擁有的所有組織資產。

***A.8.2 資訊分級***

目標:：確保所有資產能依據對組織的重要性獲得適切程度的保護。

**A.8.2.1 分級資訊**

*控制措施*

資訊應依其對未經授權的揭露或修改的法律要求、價值、重要性與敏感性加以分級。

**A.8.2.2 資訊標示**

*控制措施*

應依照組織所採用的分類法，發展與實作一套適當的資訊標示程序。

**A.8.2.3 資產處置**

*控制措施*

應依照組織所採用的分類法，發展與實作一套適當的資產處置程序。

***A.8.3 媒體處理***

目標:：避免存放於媒體的資訊受到未授權揭露、修改、移除與破壞。

**A.8.3.1 可移除式媒體的管理**

*控制措施*

應依照組織所採用的分類法，實作可移除式媒體管理程序。

**A.8.3.2 媒體的汰除**

*控制措施*

媒體不再需要時，應加以安全地汰除。

**A.8.3.3 實體媒體輸送**

*控制措施*

應保護含有資訊的媒體在傳輸時，避免未經授權的存取、誤用或毀損。

**A.9 存取控制**

***A.9.1 存取控制之營運要求***

目標：限制資訊與資訊處理設施的存取。

**A.9.1.1 存取控制政策**

*控制措施*

應基於營運與資訊安全要求，建立、文件化及審查存取控制政策。

**A.9.1.2 網路與網路服務存取**

*控制措施*

應僅提供使用者經特定授權可存取的網路與網路服務。

***A.9.2 使用者存取管理***

目標：確保授權使用者得以存取，並避免系統與服務的未授權存取。

**A.9.2.1 使用者註冊與註銷註冊**

*控制措施*

正式的使用者註冊與註銷註冊流程應加以實作，以確保存取權限的指派。

**A.9.2.2 使用者存取提供**

*控制措施*

正式使用者存取提供流程應加以實作，以指派或撤銷所有系統與服務之各項使用者類別的存取權限。

**A.9.2.3 特殊存取權限管理**

*控制措施*

應限制與控制特權的配置與使用。

**A.9.2.4 使用者秘密鑑別資訊的管理**

*控制措施*

秘密授權資訊的配置應透過正式管理流程加以控制。

**A.9.2.5 使用者存取權限的審查**

*控制措施*

資產擁有者應定期審查使用者的存取權限。

**A.9.2.6 存取權限的移除或調整**

*控制措施*

所有員工與外部國體使用者對資訊及資訊處理設施的存取權限，在其聘僱、合約或協議終止時，或因變更而調整時，均應予以移除。

***A.9.3 使用者責任***

目標:讓使用者對保護其授權資訊安全負起責任。

**A.9.3.1 秘密鑑別資訊的使用**

*控制措施*

應要求使用者於使用秘密授權資訊時，遵循組織實務。

***A.9.4 系統與應用程式存取控制***

目標：防止系統與應用程式的未授權存取。

**A.9.4.1 資訊存取限制**

應根據存取控制政策，限制對資訊與應用系統功能之存取。

**A.9.4.2 保全登入程序**

*控制措施*

當有存取控制政策要求時，應由保全登入程序來控制系統與應用程式的存取。

**A.9.4.3 通行碼管理系統**

*控制措施*

管理通行碼的系統應為互動式，並應確保通行碼嚴謹。

**A.9.4.3 特權公用程式的使用**

*控制措施*

可能篡越系統與應用控制措施的公用程式之使用，應加以限制與嚴密控制。

**A.9.4.5 程式源碼的存取控制**

*控制措施*

應用程式原始碼的存取應加以限制。

**A.10 密碼措施**

***A.10.1 密碼控制措施***

目標：確保適當有效地使用密碼措施，以保護資訊的機密性、鑑別性與/或完整性。

**A.10.1.1 使用密碼控制措施的施政策**

*控制措施*

使用密碼控制措施以保護資訊的政策應加以發展與實作。

**A.10.1.2 金鑰管理**

*控制措施*

加密金鑰使用、保護與存續期間的政策，應加以發展與實作於整個生命週期。

**A.11 實體與環境安全**

***A.11.1 安全區域***

目標：防止組織資訊與資訊處理設施遭未經授權的質體存取、損害及干擾。

**A.11.1.1 實體安全周界**

*控制措施*

安全周界應加以界定與使用，以保護含有敏感或重要

資訊及資訊處理設施的區域。

**A.11.1.2 實體進入控制措施**

*控制措施*

安全區域應藉由適當的入口控制措施加以保護，以確保只有經授權人員方可允許進出。

**A.11.1.3 保全辦公室、房間及設施**

*控制措施*

應設計辦公室、房間及設施的實體安全並施行之。

**A.11.1.4 對外部與環境的威脅的保護**

*控制措施*

應設計並施行實體保護，以避免天然災害、惡意攻擊或意外。

**A.11.1.5 在安全區域內工作**

*控制措施*

安全區域內工作的程序應加以設計與施行。

**A.11.1.6 收發與裝卸區**

*控制措施*

諸如收發與裝卸區及其他未經授權人員可進入作業場所之進出點宜加以控制；若可能，並宜與資訊處理設施隔離，以避免未經授權的存取。

***A.11.2 設備***

目標：防止資產的遺失、損害、竊盜或破解，並防止組織作業的中斷。

**A.11.2.1 設備安置與保護**

應安置或保護設備，以降低來自環境之威脅與危害造成的風險，以及未經授權存取之機會。

**A.11.2.2 支援的公用設施**

應保護設備不受電源失效及其他支援的公用設施失效所導致中斷的影響。

**A.11.2.3 佈纜的安全**

*控制措施*

應保護傳送資料或支援資訊服務之電源與電信佈纜，以防止竊聽、干擾或損害。

**A.11.2.4 設備維護**

*控制措施*

應正確地維護設備，以確保其持續的可用性與完整性。

**A.11.2.5 財產的攜出**

*控制措施*

未經事前授權，設備、資訊或軟體不應帶出場外。

**A.11.2.6 場所外設備的安全**

*控制措施*

安全應適用於場外的設備並考慮其在組織場所外工作的各種不同風險。

**A.11 .2.7 設備的安全汰除或再使用**

*控制措施*

含有儲存媒體的設備，其所有項目在汰除前應加以檢核，以確保任何敏感性的資料與有版權的軟體已被移除或安全地覆寫。

**A.11.2.8 無人看管的使用者設備**

*控制措施*

使用者應確保無人看管的設備有適當保護。

**A.11.2.9 桌面淨空與螢幕淨空政策**

*控制措施*

應採用對紙本媒體與可移除式儲存媒體之桌面淨空政策，及資訊處理設施的螢幕淨空政策。

**A.12 作業安全**

***A.12.1 作業程序與責任***

目標：確保正確與安全地操作資訊處理設施。

**A.12.1.1 文件化作業程序**

*控制措施*

作業程序應加以文件化，並讓所有需要的使用者均可隨時取得。

**A. 12.1.2 變更管理**

*控制措施*

影響資訊安全的組織、營運流程、資訊處理設施與系統變更應加以控制。

**A.12.1.3 容量管理**

*控制措施*

各項資源的使用應加以監視、調諧(tune)，並對未來容量要求預作規劃，以確保所要求的系統效能。

**A.12.1.4 開發、測試及運作環境的分隔**

*控制措施*

開發、測試及運作之環境應加以分隔，以降低對運作之環境未經授權存取或變吏的風險。

***A.12.2 防範惡意碼***

目標：確保資訊與資訊處理設施受到防範惡意碼的保護。

**A. 12.2.1 惡意碼的控制措施**

*控制措施*

防範惡意碼的偵測、預防及復原控制措施，應加以實作，並應結合適切的使用者認知。

***A.12.3 備份***

目標：防範資料損失

**A. 12.3.1 資訊備份**

*控制措施*

應依據所議定的備份政策，定期進行資訊、軟體與系統影像檔的備份與測試。

***A.12.4 存錄與監視***

目標：紀錄事件與產生證據

**A.12.4.1 事件存錄**

*控制措施*

事件存錄係紀錄使用者活動、例外情形、錯誤及資訊安全事件，應加以產生、保存並定期審查。

**A.12.4.2 日誌資訊的保護**

*控制措施*

存錄設施與日誌資訊應加以保護，以避免竄改與未經授權的存取。

**A.12.4.3 管理者與操作者日誌**

*控制措施*

系統管理者與操作者的活動應加以存錄、保護、及定期審查。

**A.12.4.4 鐘訊同步**

*控制措施*

組織或安全領域內所有相關資訊處理系統的鐘訊，應與單一參考時間來源同步。

***A.12.5 作業軟體的控制***

目標：確保作業系統的完整性。

**A.12.5.1 作業系統上的軟體安裝**

*控制措施*

應實作程序來控制作業系統上的軟體安裝。

***A.12.6 計數脆弱性管理***

目標:防止技術脆弱性被利

**A.12.6.1 技術脆弱性管理**

*控制措施*

應及時取得關於使用中資訊系統的技術脆弱性資訊、評估組織對此等脆弱性的暴露，以及採取適當的措施以因應相關的風險。

**A. 12.6.2 軟體安裝的限制**

*控制措施*

使用者軟體安裝的管理規則應加以建立與實作。

***A.12.7 資訊系統稽核的考量***

目標:將稽核活動對作業系統的影響降至最低。

**A.1 2.7.1 資訊系統稽核控制**

*控制措施*

有關作業系統查核的稽核要求與活動，應謹慎規劃及議定，使營運與程中斷之風險降至最低。

**A.13 通訊安全**

***A.13.1 網路安全管理***

目標:確保網路與其支援資訊處理設施上的資訊的保護。

**A. 13.1.1 網路控制措施**

*控制措施*

網路應適切地加以管理與控制，以保護系統與應用程式的資訊。

**A.13.1.2 網路服務的安全**

*控制措施*

所有網路服務的安全機制、服務水準及管理要求，應加以識別並納入網路服務協議中，不論此等服務是由內部或委外所提供。

**A. 13.1.3 網路區隔**

*控制措施*

資訊服務、使用者及資訊系統等各群組使用的網路應加以區隔。

***A.13.2 資訊轉移***

目標:維護組織內及與任何外部單位資訊轉移的安全。

**A.13.2.1 資訊轉移政策與程序**

*控制措施*

應備妥適當的正式轉移政策、程序及控制措施，以保護經由使用所有型式通訊設施的資訊轉移。

**A. 13.2.2 資訊轉移協議**

*控制措施*

組織與外部團體問協議應說明安全的營運資訊轉移。

**A.13.2.3電子傳訊**

*控制措施*

電子傳訊涉及的資訊應適當地加以保護。

**A.13.2.4 機密性或保密協議**

*控制措施*

反映組織對資訊保護之需求的機制或保密協議要求，應加以識別、定期審查與文件化。

**A.14系統取得、開發及維護**

***A.14.1 資訊系統之安全要求***

目標：確保資訊安全是整體資訊系統生命週期的一部分。此也包含透過公共網路提供服務的資訊系統之安全要求。

**A. 14.1.1 資訊安全要求分析及規格**

*控制措施*

資訊安全相關要求應包含於新資訊系統或現有資訊系統提升的要求事項中。

**A.14.1.2 公共網路的安全應用服務**

*控制措施*

公眾網路上傳輸而涉及應用服務的資訊，應加以保護免於詐欺行為、契約爭議及未經授權的揭露與修改。

**A.14.1.3 保護應用服務交易**

*控制措施*

涉及應用服務交易的資訊，應加以保護以防止不完整的傳輸、選路錯誤(mis-routing) ，以及未經授權的訊息修改、揭露、訊息複製或重演。

***A.14.2 開發及支援過程的安全***

目標：確保資訊安全在資訊系統開發生命週期中加以設計與實作。

**A.14.2.1 安全開發政策**

*控制措施*

軟體與系統開發規則應加以建立與應用於組織的系統開發中。

**A.14.2.2 系統變更控制程序**

*控制措施*

系統開發生命周期中的變更，應使用正式變更控制程序加以控制。

**A.14.2.3 作業平台變更後的應用系統技術審查**

*控制措施*

作業平台變更時，營運關鍵應用系統應加以審查與測試，以確保對組織作業或安全無不利的衝擊。

**A.14.2.4 套裝軟體變更的限制**

*控制措施*

應不鼓勵軟體套件之修改， 且僅限於必要的變更，所有的變更並應嚴格管制。

**A.14.2.5 安全系統設計原則**

*控制措施*

設計安全系統的原則應加以建立、文件化、維護並應用於所有資訊系統實作成果。

**A.14.2.6 安全開發環境**

*控制措施*

組織應建立並適切地保護涵蓋系統開發與整合生命周期活動的安全開發環境。

**A.14.2.7 委外開發**

*控制措施*

組織應監督與監視委外系統開發的活動。

**A.14.2.8 系統安全測試**

*控制措施*

安全功能的測試應於開發中執行。

**A.14.2.9 系統驗收測試**

*控制措施*

新資訊系統、系統升級及新版本的驗收測試方案與相關準則應加以建立。

***A.14.3 測試資料***

目標：確保用於測試的資料受到保護。

**A.14.3.1 測試資料的保護**

*控制措施*

測試資料應加以小心選擇、保護及管制。

**A.15 供應商關係**

***A.15.1 供應商關係中的資訊安全***

目標：確保供應商可存取的組織資產受到保護。

**A.15.1 .1 供應商關係的資訊安全政策**

*控制措施*

為降低供應商存取組織資產相關風險的資訊安全要求事項資訊，應取得供應商的同意並加以文件化。

**A.15.1.2 供應商協議的安全說明**

*控制措施*

所有相關的資訊安全要求事項，均應加以建立，並取得涉及存取、處理、儲存、溝通或管理組織資訊提供的IT基礎設施元件供應商的同意。

**A.15.1.3 資通訊技術供應鏈**

*控制措施*

供應商協議應包含說明資訊與通信技術服務與產品供應鏈有關資訊安全風險。

***A.15.2 供應商服務交付管理***

目標：維持適切等級之資訊安全及服務交付，並能與供應商協議一致。

**A.15.2.1 供應商服務監視與審者**

*控制措施*

組織應定期監視、審查與稽核供應商的服務交付。

**A.15.2.2 供應商服務變更的管理**

*控制措施*

供應商所提供服務的變更，包括維持與改進現有的資訊安全政策、程序及控制措施均應加以管理，並考量所涉及之營運系統與過程的重要性以及風險的重新評鑑。

**A.16 資訊安全事故管理**

***A.16.1 管理資訊安全事故與改善***

目標：確保包含資安事件與弱點溝通的資訊安全事故管理採用一致與有效的作法。

**A.16.1.1 責任與程序**

*控制措施*

管理責任與程序應加以建立，以確保對資訊安全事故做迅速、有效及依序的回應。

**A.16.1.2 通報資訊安全事件**

資訊安全事件應循適切的管理管道盡速通。

**A.16.1.3 通報資訊安全弱點**

*控制措施*

使用組織資訊系統與服務的所有員工與契約人員，應被要求注意並通報系統或服務之任何觀察到或可疑的安全弱點。

**A.16.1.4 資訊安全事件評估與決策**

*控制措施*

資訊安全事件應加以評估與決策其是否應歸類為資訊安全事故。

**A.16.1.5 因應資訊安全事故**

*控制措施*

資訊安全事故應依據文件化程序加以因應。

**A.16.1.6 從資訊安全事故中學習**

*控制措施*

由分析與解決資訊安全事故所獲得的知識，應利用來降低未來事故發生可能性與衝擊性。

**A.16.1.7 證據的收集**

*控制措施*

組織應制訂並應用程序來進行可作為證據資訊的識別、蒐集、取得與保存。

**A.17 營運持續管理的資訊安全層面**

***A.17.1 資訊安全持續性***

目標：資訊安全持續性應植基於組織營運持續管理。

**A. 17.1.1 規劃資訊安全持續性**

*控制措施*

組織應決定資訊安全與資訊安全管理在危急情況，如危機或災害期間，的持續性要求。

**A.17.1.2 實行資訊安全持續性**

*控制措施*

組織應建立、文件化、實作與維護流程、程序與控制措施，以保障資訊安全在危急情況時達成所要求的持續性等級。

**A. 17.1.3 查核、審查與評估資訊安全持續性**

*控制措施*

組織應定期查核己建立與實作的資訊安全持續性控制措施，以確保其在危急情況的可用與有效性。

***A.17.2 複式措施***

目標：確保資訊處理設施的可用性。

**A. 17.2.1 資訊安全處理設施的可用性**

*控制措施*

資訊處理設施應以複式措施來實作，以充分符合可用

性要求。

**A.18 遵循性**

***A.18.1 遵循法規與契約要求***

目標：避免違反任何資訊安全相關的法律、法令、法規或契約義務，以及任何安全要求。

**A.18.1.1 識別適用之法條與契約要求**

*控制措施*

對每個資訊系統與組織，所有相關法律、法令、法規與契約要求及組織用以符合此等要求之作法，均應加以明確界定、文件化及維持最新。

**A.18 .1.2 智慧財產權**

*控制措施*

適當程序應加以實作，以確保遵循智慧財產權與所使用的專屬軟體產品的相關法律、法規及契約要求。

**A.18.1.3 紀錄的保護**

*控制措施*

紀錄應依據法令、法規、契約及營運要求，加以保護，以免於遺失、毀損、偽造、未授權存取與未授權發行。

**A.18.1.4個人識別資訊的隱私與保護**

*控制措施*

個人識別資訊的隱私與保護應加以確保符合相關適用法令法規的要求。

**A.18.1.5 密碼控制措施的規定**

*控制措施*

密碼控制措施的使用應遵循所有相關的協議、法律及法規。

***A.18.1 資訊安全審查***

目標：確保資訊安全依據組織的政策與程序進行實作與運作。

**A.18.2.1 資訊安全的獨立審查**

*控制措施*

組織對管理資訊安全的作法與其實作（例如：資訊安全的各項控制目標、控制措施、政策、過程及程序），應依所規劃的期間或當安全實作發生顯著變更時，進行獨立審查。

**A. 18.2.2 安全政策與標準的遵循性**

*控制措施*

管理者應、定期審查其適當的資訊安全政策、標準與其他安全要求責任範圍內資訊處理與程序的遵循性。

**A .18.2.3 技術遵循性審查**

*控制措施*

資訊系統應定期審查組織資訊安全政策與標準的遵循性。