雲林科技大學

圖書資訊處

資通安全政策

機密等級：一般

文件編號：YUNTECH-ISMS-A-001

版　　次：2.6

發行日期：115.11.03

修　訂　紀　錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
1.0	98.02.23		謝政呂	初版
1.1	103.05.07	2	陳珮芸	增加5 管理指標。
1.2	103.10.13	3	陳珮芸	5.2.6 本校資訊系統開發應考量安全需求，修訂為本校資訊系統應考量安全需求...
2.0	107.01.17	1-13	陳珮芸	轉新版
2.1	107.10.24	3,6,8,11	陳珮芸	調整部分內容，使更符合新版規範要求
2.2	108.07.16		洪明賢	因應資通管理法修正相關用詞： 1.「資訊安全政策」修改為「資通安全政策」。 2.雲林科技大學資訊中心(以下簡稱「本中心」)修改為「本校」。 3.「資訊安全」修改為「資通安全」
2.3	110.04.30		賴國銓	修訂： 5.1 一般要求、5.3.1.1 過程簡要說明、5.4.1.6、7.1.1 原「教育體系資通安全管理暨個人資料規範」修訂為「國際標準ISO 27001:2013 資訊安全管理制度」。 增訂： 5.3.1.1.2、5.3.1.3、5.3.1.5、8.3.3 修訂部份陳述文字： 5.3.1.6、8.2.1 修訂「資訊安全委員會」為「資通安全暨個人資料保護推動委員會」(5.3.1.1.1、5.3.4.1.7、5.3.4.2、5.3.4.3、6.1.2、8.1) 修訂「資訊安全長」為「資通安全長」(5.2.1、5.2.2、

				5.3.3.3~5.3.3.8、11) 修訂「資訊安全小組」為「資通安全暨個人資料保護執行小組」(5.3.3.5)
2.4	113.04.30	P1、2、3、9、12	張瑋辰	依據 ISO/CNS27001:2022 本文及控制措施修正部分文件內容：2.2、2.3、5.1、5.3.1.1、5.4.1.6、7.1.1
2.5	114.02.05	封面、P7	張瑋辰	因應組織編制調整，機關名稱由「資訊中心」修正為「圖書資訊處」
2.6	115.11.03	P13	張瑋辰	依據 ISO27001 第三方稽核結果，增訂 8.2.3 與 ISMS 相關關注方之需要及期望的變更。

目錄

1 目的 1

2 適用範圍 1

3 目標 2

4 責任 2

5 資訊安全管理制度 3

6 管理階層責任 10

7 內部稽核 12

8 管理階層審查 12

9 改進 14

10 審查 15

11 實施 15

資通安全政策					
文件編號	YUNTECH-ISMS-A-001	機密等級	一般	版次	2.6

1 目的

為確保雲林科技大學（以下簡稱「本校」）所屬之資訊資產的機密性、完整性及可用性，以符合相關法令、法規之要求，使其免於遭受內、外部蓄意或意外之威脅，並衡酌本校之業務需求及達到以下之標的，訂定本政策。

1.1 落實資通安全管理政策。

1.2 導入資訊安全管理制度（ISMS）。

1.3 培訓資訊人力資通安全專業能力。

1.4 強化資通安全環境及資訊安全應變能力。

1.5 達成資訊安全管理政策量測指標。

2 適用範圍

2.1 本政策適用範圍為本校之內部人員、委外服務廠商與訪客等。

2.2 資訊安全管理範疇涵蓋四大項管理事項，避免因人為疏失、蓄意或天然災害等因素，導致資料不當使用、洩漏、竄改、破壞等情事發生，對本校造成各種可能之風險及危害，各領域分述如下：

2.2.1 組織領域控制措施。

2.2.2 人員領域控制措施。

2.2.3 實體領域控制措施。

2.2.4 技術領域控制措施。

2.3 資通安全運作包含 15 項治理事項

2.3.1 治理 (Governance);

2.3.2 資產管理 (Asset management);

2.3.3 資訊保護 (Information protection);資訊資產管理;

2.3.4 人力資源安全 (Human resource security);

2.3.5 實體安全 (Physical security);

2.3.6 系統與網路安全 (System and network security);

2.3.7 應用程式安全 (Application security);

2.3.8 安全組態 (Secure configuration);

2.3.9 識別與存取管理 (Identity and access management);

2.3.10 威脅與弱點管理 (Threat and vulnerability management);

2.3.11 持續性 (Continuity);

2.3.12 供應商關係安全 (Supplier relationships security);

2.3.13 法律與合規 (Legal and compliance);

2.3.14 資訊安全事件管理 (Information security event management);

2.3.15 資訊安全確保 (Information security assurance) ;

3 目標

為維護本校資訊資產之機密性、完整性與可用性，並保障使用者資料隱私之安全。期藉由本校全體同仁共同努力以達成下列目標：

3.1 保護本校業務服務之安全，確保資訊需經授權人員才可存取資訊，以確保其機密性。

3.2 保護本校業務服務之安全，避免未經授權的修改，以確保其正確性與完整性。

3.3 建立本校業務永續運作計畫，以確保本校業務服務之持續運作。

3.4 確保本校各項業務服務之執行須符合相關法令或法規之要求。

4 責任

4.1 本校應成立資通安全組織統籌資通安全事項推動。

4.2 管理階層應積極參與及支持資通安全管理制度，並透過適當的標準和程序以實施本政策。

4.3 本校全體人員、委外服務廠商與訪客等皆應遵守本政策。

4.4 本校全體人員及委外服務廠商均有責任透過適當通報機制，通報資通安全事件或弱點。

4.5 任何危及資通安全之行為，將視情節輕重追究其民事、刑事及行政責任或依本校之相關規定進行議處。

5 資訊安全管理制度

5.1 一般要求

本校因應「國際標準 ISO 27001:2022 資訊安全管理制度」之要求，特制訂本政策作為整體資訊安全管理制度之建置開發、實施操作、監控審查及持續維持改進之規範，並依據本校業務活動與風險，以建立資訊安全管理政策及目標。

5.2 組織全景之鑑別

5.2.1 本校應決定與本校營運目的相關，且會影響資訊安全管理制度（ISMS）預期成果之內部與外部議題，鑑別出與本校所提供服務相關之利害關係者，以及這些利害關係者對本校的需求與期望，並讓資通安全長知悉以取得共識，用以客觀決定本校資訊安全管理制度（ISMS）之範圍。

5.2.2 應制定組織全景鑑別管理作業程序，用以系統化地鑑別本校之核心業務與核心業務相關之利害關係者，以及這些利害關係者對本校核心業務之需求與期望，並判別若無法達到需求與期望會對本校造成何種程度之衝擊，並將上述評估及分析結果供資通安全長用以決策 ISMS 之導入及驗證範圍。

5.3 資訊安全管理制度之建立與管理

5.3.1 建立資訊安全管理制度

5.3.1.1 過程簡要說明

本校係依照「國際標準 ISO 27001:2022 資訊安全管理制度」

標準之步驟建立資訊安全管理制度（ISMS），其過程簡要說明如下：

5.3.1.1.1 依據標準建議與主管機關之要求，成立資通安全暨個人資料保護推動委員會，並經核准頒布。

5.3.1.1.2 本校資訊安全管理制度（ISMS）以全校為範圍，不因選擇之驗證範圍而有所差異。

5.3.1.1.3 頒布「資通安全管理政策」，以說明本校資通安全政策、目標與執行方式。

5.3.1.1.4 進行風險評估作業，發掘資產與組織之安全弱點及其威脅與影響，並評估其風險等級，彙整成『風險評鑑報告』後，執行及追蹤『風險處理計畫』。

5.3.1.1.5 依據資訊安全管理政策與風險評估的結果，設定風險管理之實施範圍。

5.3.1.1.6 選擇適合實施之資通安全管制目標與措施，並檢討確認其可行性與有效性。

5.3.1.1.7 將所選定之安全管制目標、管制措施、選用原因等資料記載於『適用性聲明』文件中。

5.3.1.1.8 為貫徹資訊安全並持續改善，本校將依實際需求適時檢討上述步驟，並做必要之變更修正。

5.3.1.2 所有正式與外部團體契約員工及第三方派駐人員均須遵循本校資通安全管理政策與資訊安全目標，恪守資訊安全管理制度(ISMS)各項作業流程、管理規範及相關法令法規之要求。故意或過失違反者，將視其違反情節及所造成之衝擊，依人事規章及法令法規予以懲處。

5.3.1.3 第三方承包廠商在執行本校委外業務時若有複委託之需求，

應評估複委託業務相關之資安風險，並要求承包廠商依資訊安全管理制度（ISMS）等相關規定對複委託廠商進行適當之監督與管理。

5.3.1.4 對內部及外部專案管理的過程中，應明訂及陳述與專案相關之各項資訊安全要求，並由風險評鑑之結果用以決定及實作資訊安全控制措施，確保內部及外部專案資訊之機密性、完整性及可用性，降低機敏資訊（含個人資料）外洩及違反法令之風險。

5.3.1.5 應決定及建立與資訊安全管理制度（ISMS）相關的內部與外部溝通之需求及準則，內容須包含：要溝通什麼、何時溝通、和誰溝通、應是誰溝通以及應實現哪種溝通過程，確保資訊安全管理制度（ISMS）各項資安業務在內部適度的溝通與傳達，以利資訊安全管理制度（ISMS）之推動與管理。

5.3.1.6 應制定管制區域之可攜式資訊設備(包含智慧型移動裝置)及可攜式儲存媒體之管理程序，要求同仁落實執行，並定期針對可攜式資訊設備（包含智慧型移動裝置）及可攜式儲存媒體進行風險評鑑，依據風險評鑑之結果選擇適切之控制措施，定期執行查核作業，確保使用可攜式資訊設備及儲存媒體之風險受到監控，降低機密資料外洩之風險。

5.3.2 資訊安全管理制度之實施及操作

5.3.2.1 應制定風險處理計畫，有系統地鑑別及陳述適當的管理措施、權責及優先順序，以便管理資訊安全風險。

5.3.2.2 實施風險處理計畫中所選定之控制措施，以對各項風險加以防禦，包含實施既定管理計畫，以達到所鑑別的安全目標，計畫內容包括投資的考慮及角色與責任的分派。

5.3.2.3 應擬定安全控制措施有效性之量測指標與使用方法，以判斷所選控制措施以達資安目標所要求之程度。

5.3.2.4 人員所需實施訓練與認知計畫參閱第 6.2.2 節。

5.3.2.5 各項作業需遵照作業程序執行或執行計畫，單位主管應不定期檢視與管理執行狀況。

5.3.2.6 須定期衡量各項計畫目標執行狀況，並依據衡量結果適時調整相關控制措施與目標。

5.3.2.7 執行時所需之各項資源管理參閱第 6.2 節。

5.3.2.8 單位主管利用不定期巡視、內外部稽核或是單位人員所提出之建議事項回報，加速偵知各種安全事件並予以回應處理。

5.3.3 資訊安全管理制度之目標設定、實現

5.3.3.1 各單位針對所負責之業務，訂定各項改善目標，並且定期檢討與改善,以持續改善及維持資訊安全管理系統之有效運作。

5.3.3.2 各單位主管應定期指派專人，蒐集單位內資訊安全相關之管理數據與資料，並加以統計分析，以作為資訊安全目標之設定及審核之參考依據。

5.3.3.3 各單位主管應指派專人依據如下之重點，設定可衡量之資訊安全目標，並填寫於「資訊安全目標設定表」,陳資通安全長審核。

5.3.3.3.1 資訊安全目標應考量各單位之特性及能力。

5.3.3.3.2 資訊安全目標應配合資通安全政策。

5.3.3.3.3 將重要之資訊安全管控流程尋找適當監測點，列入資訊安全目標持續監測。

5.3.3.4 經資通安全長核定之「資訊安全目標設定表」,由各業務承辦人員，依資訊安全目標之要求項目向單位同仁公布，並確實

要求單位同仁努力達成資訊安全之目標。

5.3.3.5 資通安全暨個人資料保護執行小組每季應針對上一季之資訊安全目標執行情形，於相關會議中提出檢討，並記錄於「資訊安全目標檢討表」，由圖書資訊處彙整後陳資通安全長審核。

5.3.3.6 每季定期檢討資訊安全目標，或單位主管發現資訊安全目標不適當時，均得重新提出「資訊安全目標設定表」，經資通安全長核定後，方得依新核定之目標執行及檢討。

5.3.3.7 若資訊安全目標多次無法達成，資通安全長得視需要，依「矯正及預防管理程序書」之規定，要求相關單位研擬及執行改善措施。

5.3.3.8 每年定期討論資訊安全目標，或單位主管發現資訊安全目標不適當時，均得重新提出「資訊安全目標設定表」，經資通安全長核定後，方得依新核定之目標執行及檢討。

5.3.4 資訊安全管理制度之監控及審查

5.3.4.1 本校採用下列監控方式確保資訊安全管理制度所涵蓋範圍皆能安全無虞：

5.3.4.1.1 人員應定期及不定期巡視檢查各項設備及環境是否皆屬正常狀態。

5.3.4.1.2 利用攝影機監視單位內人員出入狀況並錄影存證。

5.3.4.1.3 應設定、定期檢查及紀錄各項監控指標，以協助判斷安全事件，預防及立即處理安全事故之發生。

5.3.4.1.4 單位主管應隨時注意各項通報事件或人員工作執行狀況，進而決定相應的控制措施，必要時可將人員職務進行短期調動，避免發生系統失效或人為破壞事件。

5.3.4.1.5 配合定期執行之內部稽核，確認各種安全措施及控制程

序是否如預期般實施。

5.3.4.1.6 隨時注意本校所發生之資安事件，針對事件發生之成因及後果詳加評估，並配合矯正預防措施之執行，改善整體資安環境，降低資安事件發生之機率。

5.3.4.1.7 管理階層利用定期執行之資通安全暨個人資料保護推動委員會會議或內部會議，討論目前可能存在的安全漏洞，並決定解決之道。

5.3.4.2 於資通安全暨個人資料保護推動委員會會議中定期審查資訊安全管理制度之有效性，並考慮安全稽核、事件、有效性量測及利害關係團體之建議及反映意見。

5.3.4.3 於資通安全暨個人資料保護推動委員會會議中審查資安風險、殘餘風險與可接受風險等級，並考慮組織、技術、單位營運目標及程序、已鑑別之威脅與外部事件（包括法令法規、合約義務及社會環境）之變化。

5.3.4.4 每年執行內部稽核，以確定是否有依據作業流程執行，且是否達到預期功能。

5.3.4.5 每年至少召開一次資通安全管理審查會議，執行正式的資訊安全管理制度審查，以確保範圍適當及資訊安全管理制度過程之各項改善措施均已鑑別與實施。

5.3.4.6 應依據監視及審查結果，適時修訂資訊安全管理計畫，以符合資安政策、資安目標與各項資訊安全要求。

5.3.4.7 所有對資訊安全管理制度有效性或績效有衝擊之活動與事件均須加以記錄。

5.3.5 維持及改善資訊安全管理制度

本校將定期進行下述工作：

5.3.5.1 利用風險評鑑或是內外部稽核之結果進行整體資安環境改善。

5.3.5.2 採取適當矯正及預防措施，採用從其他單位或內部發生事件之安全經驗汲取教訓。

5.3.5.3 與相關機構就結果及各項措施進行溝通並徵詢意見。

5.3.5.4 必要時修改資訊安全管理制度。

5.3.5.5 確保各項修改措施達到預期目標。

5.4 文件要求

5.4.1 一般要求

本校資訊安全管理制度文件化包括下列各項：

5.4.1.1 安全政策與安全目標之書面聲明。

5.4.1.2 資訊安全管理制度適用範圍及各項作業程序。

5.4.1.3 風險評鑑報告。

5.4.1.4 風險處理計畫。

5.4.1.5 組織為確保有效規劃、操作及控制資訊安全過程所需之文件。

5.4.1.6 「國際標準 ISO 27001:2022 資訊安全管理制度」要求及上級主管單位要求之紀錄。

5.4.1.7 適用性聲明書。

5.4.2 文件管制

資訊安全管理制度所需之文件應受保護及管制。紀錄是文件之一種特殊型態，應依第 5.4.3 節所定的要求予以管制。並建立文件化程序，以界定所需之管制，用以：

5.4.2.1 在文件發行前核准其適切性。

5.4.2.2 必要時，審查與更新並重新核准文件。

5.4.2.3 確保文件之變更與最新改訂狀況已予鑑別。

5.4.2.4 確保在使用場所備妥適用文件之相關版本。

5.4.2.5 確保文件易於閱讀並容易識別。

5.4.2.6 確保文件於需使用時能隨時取用，並且於文件傳遞、保存及毀棄時皆能遵守文件管制規定辦理。

5.4.2.7 確保外來原始文件已加以鑑別。

5.4.2.8 確保文件分發有適當管制。

5.4.2.9 防止作廢（失效）文件被誤用，作廢文件為任何目的需保留時，應予以適當鑑別。

5.4.3 紀錄管制

5.4.3.1 為確保資訊安全管理制度符合本校要求及提供有效運作之證據，應建立及維持執行資訊安全管理制度各項作業程序之各項紀錄，並予以管制，並將相關法律法規及合約要求列入考量。

5.4.3.2 紀錄應清晰易讀，容易識別及檢索。紀錄之鑑別、儲存、保護、檢索、保存期限及作廢，應建立文件化程序，以界定所需之管制。

5.4.3.3 紀錄應妥善保存。

5.4.3.4 所需之紀錄及其範圍應由管理過程加以決定。該過程應記錄重大決定，並將紀錄之用途及缺少紀錄時相關之風險列入考量。

6 管理階層責任

6.1 管理階層承諾

為使資訊安全管理制度推動順利，管理階層應確實執行下列事項：

6.1.1 管理階層應積極參與及支持資訊安全管理制度，並透過適當的標準和程序以實施本政策。

6.1.2 成立資通安全暨個人資料保護推動委員會，以明訂及文件化資訊

安全之角色與責任。

6.1.3 管理階層應儘量藉由各種內部公開會議或集會時，向所有人員宣達符合資訊安全目標、法律及法規要求之重要性，以及持續改進之需求。

6.1.4 提供充分資源，確保能建立、實施操作、監控審查及持續維持改進資訊安全管理制度。

6.1.5 定期執行資訊安全管理制度之內部稽核作業。

6.1.6 定期召開資訊安全管理制度之管理階層審查會議。

6.1.7 決定風險評鑑後之可接受風險等級。

6.2 資源管理

6.2.1 資源提供

為確保資訊安全管理制度執行無礙，應決定並提供下列工作之必要資源：

6.2.1.1 提供建置與維護資訊安全管理制度時所需的人力與資源設備。

6.2.1.2 提供實施資訊安全管理制度時必要之協助。

6.2.1.3 確定各項安全程序可配合營運需求。

6.2.1.4 鑑別並提出法律與法規的要求以及於各項合約上之註明安全義務。

6.2.1.5 正確應用所有實施的控制措施，以維持適當之安全。

6.2.1.6 當需要時，進行審查並針對審查結果作適當因應。

6.2.1.7 當必要時，改進資訊安全管理制度之作業流程，以確保其有效。

6.2.2 訓練、認知及能力

為確保所有同仁皆有能力執行所要求之工作與符合各項安全要求，應藉由各種途徑取得協助同仁執行教育訓練，包括下列方式：

6.2.2.1 提供各種能力訓練以滿足該需求。

6.2.2.2 確保同仁認知其所從事的活動之相關性及重要性，以及他們如何對安全目標之達成有所貢獻。

6.2.2.3 應留下教育訓練、技能、經驗及評定資格等紀錄，紀錄保存之要求參閱第 5.4.3 節。

6.3 本校全體人員及委外服務廠商均有責任透過適當通報機制，通報資訊安全事件或弱點。

6.4 任何危及資通安全之行為，將視情節輕重追究其民事、刑事及行政責任或依相關規定進行議處。

7 內部稽核

7.1 每年定期執行內部稽核，確保資訊安全管理制度的各項管制目標、控制措施、運作過程以及各項程序是否皆：

7.1.1 符合國際標準 ISO 27001:2022 資訊安全管理制度與相關法令或法規之要求。

7.1.2 符合本校所制定之資訊安全目標及其他相關要求。

7.1.3 有效地實施與維持資訊安全管理制度。

7.1.4 符合上級單位的期待。

8 管理階層審查

8.1 概述

資通安全暨個人資料保護推動委員會至少每年召開一次會議，針對本校現行之資訊安全管理制度進行審查，以確保相關程序的適用性、適切性及有效性皆符合本校需求，並評估相關政策與目標的改進時機，或是其他的變更需求，且審查結果應留下相關文件與紀錄備查。

8.2 審查輸入（管理審查之範圍）

管理階層審查至少應包含（但不限於）下列項目：

8.2.1 先前管理審查決議事項之跟催狀況。

8.2.2 有關可能影響 ISMS 的外部與內部問題之變更。

8.2.3 與 ISMS 相關關注方之需要及期望的變更。

8.2.4 資訊安全的績效回饋，包含下列趨向：

8.2.4.1 不符合事項與矯正措施之執行狀況。

8.2.4.2 監督與量測結果。

8.2.4.3 內部稽核的結果。

8.2.4.4 資訊安全目標的實現。

8.2.5 利害相關團體的回饋。

8.2.6 風險評鑑的結果與風險處理計畫的狀態。

8.2.7 持續改進的機會。

8.3 審查輸出

8.3.1 管理審查的產出應包含和持續改進機會與資訊安全管理制度（ISMS）的變更需求有關之決定。

8.3.2 管理階層審查之產出建議包含但不限於下列事項之任何決策與措施：

8.3.2.1 ISMS 有效性之改進。

8.3.2.2 風險評鑑與風險處理計畫之更新。

8.3.2.3 影響資訊安全之程序與控制之必要時的修改，以回應可能衝擊 ISMS 之內部或外部事件，包括下列事項之變更：

8.3.2.3.1 各項營運要求。

8.3.2.3.2 各項安全要求。

8.3.2.3.3 影響既有各項營運要求之營運過程。

8.3.2.3.4 法律或法規各項要求。

8.3.2.3.5 契約的各項義務。

8.3.2.3.6 風險等級或風險接受準則。

8.3.2.4 資源需求。

8.3.2.5 控制措施的有效性如何量測之改進。

8.3.3 組織應保存文件化資訊及管理審查結果的證據。

9 改進

9.1 持續改進

本校經由資訊安全管理政策、安全目標、內外部資訊安全稽核結果、事件監控之分析、矯正與預防措施以及管理階層審查，由資通安全人員負責所有風險發生或不符合事項之監控，並追蹤相關業務承辦人之改善情形，以持續改進資訊安全管理制度之有效性。

9.2 矯正措施

本校採取適當的控管措施，以減低資訊安全管理制度在建置、操作及使用時所產生的不符合事項，以防止再度發生。矯正措施之內容應包含下列各項：

9.2.1 鑑別各項不符合資安要求之事項。

9.2.2 判定各項不符合事項發生之原因。

9.2.3 評估各項矯正措施之需求，以確保各項不符合事項不復發。

9.2.4 決定及實施所需之矯正措施。

9.2.5 需記錄所採矯正措施之結果，紀錄保存之要求參閱第 5.4.3 節。

9.2.6 審查所採取之矯正措施。

9.3 預防措施

本校應採取適當的控管措施，以預防及降低潛在不符合事項發生之機會，預防措施應能預防潛在問題所可能發生之影響。

9.3.1 鑑別潛在的各項不符合事項及其原因。

9.3.2 評估預防措施的需求，以防止不符合事項的發生。

9.3.3 決定及實施所需之預防措施。

9.3.4 記錄所採取措施之結果，紀錄保存之要求參閱第 5.4.3 節。

9.3.5 審查所採取之預防措施。

10 審查

10.1 本政策每年應至少評估檢討一次，以反映本校資通安全需求、政府法令法規、外在網路環境變化及資安技術等最新發展現況，以確保其對於維持營運和提供適當服務的能力。

10.2 本政策如遇重大改變時應立即審查，以確保其適當性與有效性。必要時應告知相關單位及合作廠商，以利共同遵守。

11 實施

本政策經資通安全長核准，於公告日施行，並以適當方式通知本校所屬職員及與本校連線作業之有關機關（構）、廠商，修正時亦同。