長榮大學

資訊安全政策

機密等級：一般
文件編號：IS-A-0100
版　　次：2.5
發行日期：112.12.28

修 訂 紀 錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
2.0	106.08.04		俞怡中	106.05.22 經「智慧財產權與資訊安全暨個人資料保護宣導及執行委員會」會議通過 106.08.04 完成各階文件修訂後，簽請校長公布施行
2.1	107.01.17	4	俞怡中	統一名詞，將「關注方」修正為「利害相關者」
2.2	107.05.28	4	俞怡中	經 107.05.28 106 學年度第 2 學期「智慧財產權與資訊安全暨個人資料保護宣導及執行委員會」修正通過 對應國際標準，將「利害相關者」修正為「關注方」 核定方式修正 8.1 本政策經「智慧財產權與資訊安全暨個人資料保護宣導及執行委員會」會議決議或簽請召集人
2.3	109.12.17	2	俞怡中	經 109.12.17 109 學年度第 1 學期「智慧財產權與資訊安全暨個人資料保護宣導及執行委員會」修正通過 刪除 6..1.1 確保本校資訊系統維運服務達全年上班時間 96%以上之可用性。
2.4	112.05.25	2	俞怡中	經 112.05.25 111 學年度第 2 學期「智慧財產權與資訊安全暨個人資料保護宣導及執行委員會」修正通過。 6.1 定量化指標 6.1.1 因資通安全事件、異常事件、其他安全事故所造成核心系統異常而中斷營運服務之情事，每季不得超過 4 次。 6.1.2 因資通安全事件、異常事件、其他安全事故所造成核心系統異常而中斷營運服務之情事，每次最長不得超過 4 工作小時。
2.5	112.12.28	2	俞怡中	經 112.12.28 112 學年度第 1 學期「智慧財產權與資訊安全暨個人資料保護宣導及執行委員會」修正通過。 6.1 定量化指標 原 6.1.3、6.1.4 均為資安事件發生次數之指標，故刪除。 原 6.1.5、6.1.6、6.1.7，調次調整為

				6.1.3、6.1.4、6.1.5 新的調次修正 6.1.4 為確保本校資訊安全措施或規範符合現行法令、法規之要求，每年至少需辦理內部稽核 1 次，受稽核單位包含核心系統維運單位，並應分年完成全校各單位之稽核作業。 6.1.5 針對所有核心資訊系統每 2 年至少執行 1 次業務永續運作演練，以確保本校核心資訊業務服務得以持續運作。 8.1 本政策經「智慧財產權與資訊安全暨個人資料保護宣導及執行委員會」會議決議或簽請召集人核准，修訂時亦同。

以下紀錄為原 CJCU-ISMS-A-0100 修訂紀錄

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	2008/9/22		張文瑩	初版
1.1	2009/8/14	2,3	張文瑩	增列「定量/性化管理指標」
1.2	2010/8/27	2,3	張文瑩	修訂 4.5 將本中心改為本校
1.3	2012/3/28	2,3	張文瑩	修訂「目標」、「責任」及「定量化指標」內容
1.4	2012/9/12	1	張文瑩	「目標」增列資訊資產之合法性
1.5	102/01/03		俞怡中	更改文件編號
1.6	103/01/09	1,2,3	俞怡中	修改 「計算機與網路中心」→「圖書資訊處」 本中心→本處

目錄

長榮大學資訊安全政策

1 目的

確保長榮大學（以下簡稱本校）所屬之資訊資產的機密性、完整性與可用性，並符合相關法規之要求，使其免於遭受內、外部的蓄意或意外之威脅，進而保障全校教職員工生之權益。

2 適用範圍

本校之教職員工生、接觸本校業務資料之外機關人員、委外服務廠商與訪客等皆應遵守本政策。

3 資訊安全管理事項

資訊安全管理涵蓋 14 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，對本校帶來各種可能之風險及危害。管理事項如下：

3.1 資訊安全政策訂定與評估。

3.2 資訊安全組織。

3.3 人力資源安全。

3.4 資產管理。

3.5 存取控制。

3.6 密碼學(加密控制)。

3.7 實體與環境安全。

3.8 運作安全。

3.9 通訊安全。

3.10 資訊系統取得、開發及維護。

3.11 供應者關係。

3.12 資訊安全事故管理。

3.13 營運持續管理之資訊安全層面。

3.14 遵循性。

4 資訊安全目標

維護本校資訊資產之機密性、完整性、可用性與適法性，並保障使用者資料隱私。藉由全體同仁共同努力來達成下列目標：

4.1 保護本校業務服務資訊，避免未經授權的存取，確保其機密性。

4.2 保護本校業務服務資訊，避免未經授權的修改，確保其正確性與完整性。

4.3 建立資訊業務永續運作計畫，以確保本校業務服務之持續運作。

4.4 確保本校之業務服務執行符合相關法令或法規之要求。

5 責任

5.1 本校已成立資訊安全組織統籌資訊安全事項推動。

5.2 管理階層積極參與及支持資訊安全管理制度，並授權資訊安全管理組織透過適當的標準和程序以實施本政策。

5.3 本校所有人員和委外服務廠商均須依照相關安全管理程序以維護本政策。

5.4 本校所有人員和委外服務廠商均有責任報告資訊安全事件和任何已鑑別出之弱點。

5.5 任何危及資訊安全之行為，將視情節輕重追究其民事、刑事及行政責任並依本校之相關規定進行議處。

6 管理指標

為評量資訊安全管理目標達成情形，特訂定資訊安全管理指標如下：

6.1 定量化指標

6.1.1 因資通安全事件、異常事件、其他安全事故所造成核心系統異常而中斷營運服務之情事，每季不得超過 4 次。

6.1.2 因資通安全事件、異常事件、其他安全事故所造成核心系統異常而中斷營運服務之情事，每次最長不得超過 4 工作小時。

6.1.3 應適當保護本校資訊資產之機密性、完整性、可用性與適法性，每年至少需進行 1 次風險評鑑及風險管理。

6.1.4 為確保本校資訊安全措施或規範符合現行法令、法規之要求，每年至少需辦理內部稽核 1 次，受稽核單位包含核心系統維運單位，並應分年完成全校各單位之稽核作業。

6.1.5 針對所有核心資訊系統每 2 年至少執行 1 次業務永續運作演練，以確保本校核心資訊業務服務得以持續運作。

6.2 定性化指標

6.2.1 應定期審查本校資訊安全組織人員執掌，以確保資訊安全工作之推展。

6.2.2 應符合主管機關之要求，依員工職務及責任提供適當之資訊安全相關訓練。

6.2.3 應加強本校資訊機房設施之環境安全，採取適當之保護及權限控管機制。

6.2.4 應確保資訊不因傳遞過程，或無意間之行為，透漏給未經授權之第三者。

6.2.5 應加強存取控制，防止未經授權之不當存取，以確保資訊資產已受適當之保護。

6.2.6 本校資訊系統開發應考量安全需求，並定期稽核安全弱點。

6.2.7 應確保所有資訊安全事件或可疑之安全弱點，均依循適當之通報機制向上反應，並予以適當調查及處理。

7 審查

本政策應每年至少審查乙次，以反映政府法令、技術、業務等最新發展現況以及關注方之關注議題，以確保本校資訊安全管理制度之運作。

8 實施

8.1 本政策經「智慧財產權與資訊安全暨個人資料保護宣導及執行委員會」

會議決議或簽請召集人核准，修訂時亦同。

8.2 本政策公告實施後需以適當方式公告全體人員周知以落實執行運作。