中山华利实业集团股份有限公司

資訊安全政策	文件编号：HL-M-IT001	
	生效日期：2021 年 12 月 1 日	
	修订版本：1.0	页次： 1 OF 6

文件修订记录
Document Revision Record

版次 Revision	修订日期 Revise Date	变更内容 Description of Change	拟编者 Originator
1.0	2021/11/30	新订	周旭東
版次编号说明：a.b (a 为办法年次，b 为当年修订次数，未修订跨年续用为 a.0 版			

核准		复核		审核		制作	

一、目的

中山華利實業集團股份有限公司（以下簡稱本集團）為強化資訊安全管理，確保所屬廠區之資訊資產的機密性、完整性及可用性，以提供本集團資訊運作所需之環境與架構，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，特制定此政策。

二、適用範圍

1. 本政策適用範圍設定為本集團中國區總部及各廠、越南區各廠、多明尼加廠區、印尼廠區、緬甸廠區及後續因應集團業務需求於不同國家所建立的公司或工廠、香港分公司、台灣分公司、台北 IDC 機房、高雄機房相關部門與維運管理人員，以充份掌握資訊運作及管理過程，滿足各項安全要求。

2. 資訊安全管理系統範圍

2.1 本集團建置資訊安全管理系統，均應將內、外部單位對資訊安全方面之議題，包括系統服務的資訊安全及個人隱私保護，以及客戶方對資訊安全管理系統之期望與要求納入考量，並列入目標與成效評估範圍。

2.2 上述這些資訊安全相關議題、期望或要求，應列入風險評估及風險管理，以確保資訊安全管理系統能達成預期效果及持續改善。

3. 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，對本集團帶來各種可能之風險及危害。管理事項如下：

3.1 安全政策

3.2 資訊安全的組織

3.3 人力資源安全

3.4 資產管理

3.5 存取控制

3.6 加密

3.7 實體與環境安全

3.8 營運安全

3.9 通訊安全

3.10 資訊系統獲取、開發及維護

3.11 供應商關係

3.12 資訊安全事件管理

3.13 有關於資訊安全方面的營運持續管理

3.14 適法性

本集團資訊安全內、外部議題及關注事項對應表，如下：

內、外部利害關係方	期望及議題(資訊安全方面)	政策	對應事項及文件	目標及指標
1.集團資訊總處	確保業務系統及網路運作之資訊安全	1.資訊安全政策	1.資訊安全政策	A.1 資訊安全政策訂定與評估 (1)資訊安全政策審查次數 (2)資訊安全政策宣導次數
		2.資訊安全之組織政策	2.資訊安全組織程序書	A.2 資訊安全組織 (1)有否確實簽署保密協議 (2)管理審查會議召開次數
		3.資產管理政策	3.資訊資產管理作業程序	A.3 資訊資產管理 (1)資訊資產清冊更新 (2)資訊資產清冊符合分級與標示規定
		4.人力資源安全政策	4.人員安全與教育訓練作業程序	A.4 人力資源安全 (1)檢查入職和在職人員資安培訓時數 (2)檢查資安違規人員培訓時數 (3)離退人員帳號確實刪除
		5.存取控制政策	5.存取控制管理作業程序	A.5 存取控制安全 (1)定期審查重要系統存取權限 (2)未授權存取重要系統機敏性資料之次數 (3)定期變更電腦登入系統密碼
		6.實體與環境安全政策	6.實體安全管理作業程序	A.6 實體與環境安全 (1)檢查人員是否遵守機房門禁規定 (2)檢查消防設備是否定期保養 (3)檢查 UPS 是否定期保養
		7.通信與作業管理政策	7.通信與作業管理作業程序	A.7 通信安全 (1)內部網路斷線次數(年) (2)檢查重要系統時間是否同步

內、外部利害關係方	期望及議題(資訊安全方面)	政策	對應事項及文件	目標及指標
				(3)檢查防火牆設定是否與防火牆設定紀錄表相符 (4)弱點掃瞄次數及追蹤
		8.資訊系統獲取、開發及維護政策	8.系統開發與維護作業程序	A.8 資訊系統獲取、開發及維護 (1)重要系統更新上線前經過測試 (2)重要系統開發或變更時應更新系統文件 (3)重要系統上線具有緊急復原機制
		9.資訊安全事件管理政策	9.資訊安全事件管理作業程序	A.9 資訊安全事件管理 (1)發生資安事件未依規定通報之件數 (2)檢查資通安全事件通報單,統計重複發生相同資安事故件數
		10.營運持續管理政策	10.營運持續管理作業程序	A.10 營運持續管理(資安) (1)檢討營運持續計畫演練執行情形 (2)執行風險評鑑與營運衝擊分析
		11.遵循性政策	11.資訊安全稽核作業程序	A.11 營運安全 (1)定期監控網路重要伺服器執行作業之系統容量(例如 CPU 、RAM 、硬碟) (2)檢查病毒碼是否更新 (3)定期備份重要系統資料
			12.供應商管理作業程序	A.12 供應商關係 是否確實簽署保密協議
			13.矯正及預防管理作業程序	A.13 相關法規與施行單位政策之符合性
			14.風險評鑑與管理作業程序	(1)合法軟體之安裝 (2)矯正預防措施於規定時間內改善完成

內、外部利害關係方	期望及議題(資訊安全方面)	政策	對應事項及文件	目標及指標
2.客戶	1.業務資訊及網路管理安全 2.客戶隱私保護	1.實體安全管理政策	1.實體安全管理作業程序	A.6 實體與環境安全 (1)檢查是否遵守機房門禁規定 (2)檢查消防設備是否定期保養 (3)檢查 UPS 是否定期保養
		2.通信與作業管理政策	2.通信與作業管理作業程序	A.7 通信安全 (1)內部網路斷線次數(年) (2)檢查重要系統時間是否同步 (3)檢查防火牆設定是否與防火牆設定紀錄表相符 (4)弱點掃瞄次數及追蹤
		3.營運持續管理政策	3.營運持續管理作業程序	A.10 營運持續管理(資安) (1)檢討營運持續計畫演練執行情形 (2)執行風險評鑑與營運衝擊分析
		4.遵循性政策	4.資訊安全稽核作業程序	A.11 營運安全 (1)定期監控網路重要伺服器執行作業之系統容量(例如 CPU 、RAM 、硬碟) (2)檢查病毒碼是否更新 (3)定期備份重要系統資料

三、定義

資訊資產：維持本集團資訊業務正常運作之環境、硬體、軟體、資料及人員。

四、目標

維護本集團資訊資產之機密性、完整性與可用性，並保障使用者之個人隱私。藉由全體同仁共同努力來達成下列目標：

1. 落實本集團各項業務系統及相關部門與維運管理人員之標準作業程序，以確保本集團 IDC、各廠區機房及業務系統服務之機密性、完整性、及可用性，以符合利害相關團體之要求與期盼。
2. 保護本集團業務活動資訊，避免未經授權的存取及修改，確保其完整性。

3. 設置跨部門之「資訊安全長」，監督資訊安全部門推動及評估改進資訊安全管理事項，確保本集團具備可供業務持續運作之資訊環境。
4. 辦理資訊安全教育訓練，推廣員工資訊安全之意識與強化其對相關責任之認知。
5. 執行資訊安全風險評估機制，提升資訊安全管理之有效性與即時性。
6. 重要的資訊安全設施應視需要評估建立備援架構，以確保系統可用性。
7. 實施資訊安全內部稽核制度，確保資訊安全管理之落實執行。
8. 本集團之業務活動執行須符合相關法令或法規之要求。
9. 供應商提供之服務，應對其服務之項目及內容進行控管、查核及驗收管理。
10. 集團應建立內、外部溝通協調機制。
11. 集團應對資訊安全管理系統定期檢視並持續改善。
12. 針對業務系統服務資訊安全之要求，本集團必須妥予規劃與執行。
13. 本集團對業務系統服務內部授權人員， 須做妥善之風險管理。
14. 本集團業務系統服務對於供應商與客戶之間、客戶與客戶之間，須妥予區隔。
15. 業務系統服務之存取控制人員，其權責須做完善之規定與管理。
16. 當業務系統之相關管理及作業規定有變動及影響服務時，須告知客戶。
17. 業務系統服務之客戶資料，須予以妥善保存。
18. 應針對業務系統服務之客戶，做好生命週期管理。
19. 當業務系統服務有事件或事故發生時，須有明確之調查及處理規範，並通知主管單位及受影響之利害關係方。
20. 業務系統服務之作業過程，個人資料處理及管理者，須負個人隱私之保護責任。
21. 資訊安全政策為「資訊安全管理系統(ISMS)」的第一階文件，第二~四階文件為資訊安全的各項作業程序、管理說明及表單(四階文件一覽表如附件)，按照本政策原則及實施範圍另行制定。

五、責任

1. 本集團的資訊總處建立及審查此政策，有關各部門主管及成員之資訊安全職責另於「資訊安全組織程序書」訂定。
2. 資訊安全管理者透過適當的標準和程序以實施此政策。
3. 所有人員和供應商均須依照資訊安全管理程序，以維護資訊安全政策。
4. 所有人員有責任報告資訊安全事件和任何已鑑別出之弱點。
5. 任何危及資訊安全之行為，將視情節輕重追究其法律責任或依本集團之相關規定進行懲處。