資通安全政策

Information Security Policy

1. 目的

為確保和康生物科技股份有限公司(以下簡稱本公司)之資訊資產的機密性、完整性、可用性及法律遵循性，保護業務安全，避免未經授權的存取、修改及破壞，維護企業永續經營，特訂定本政策。

2. 適用範圍

2.1 本政策適用於本公司之全體員工、外部廠商及訪客。

2.2 為避免因人為疏失、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，本公司資通安全管理範疇涵蓋「組織」、「人員」、「實體」及「技術」等四大面向控制措施，以因應本公司造成各種可能之風險。

3. 目標

3.1 保護資訊資產之機密性，防止未經授權存取，並保障使用者資料與營運資訊之隱私。

3.2 保護資訊資產之完整性，防止未經授權之異動，確保資料與作業流程之正確性。

3.3 依 ISO/IEC 27001 要求執行風險管理，並透過 PDCA 循環持續提升資訊安全管理系統之有效性。

3.4 建立並維護本公司之業務持續運作計畫（BCP），確保機房、網路及資訊作業流程在中斷情境下仍能維持可接受之運作。

3.5 確保資訊安全管理、機房與網路維運、雲端使用及資訊作業流程之執行，均符合相關法規與契約要求。

4. 責任

4.1 本公司應設置資通安全組織，統籌規劃與推動資通安全相關事項，並明確界定各角色之職責與權限。

4.2 管理階層應積極參與並支持資通安全管理制度之推動，提供必要資源，並確保透過適當之標準與程序有效落實本政策。

4.3 本公司全體同仁、委外服務廠商、資料保管者與資料使用者，以及經授權之訪客，均應遵守本政策。

4.4 本公司全體同仁、委外廠商、資料保管者及資料使用者，均有責任依本公司之通報程序回報資通安全事件或弱點。

4.5 任何危及資通安全之行為，將依情節嚴重程度，依本公司相關規範處理，並得依法追究民事或刑事責任。

5. 管理指標

5.1 為評量資通安全管理目標之達成情形，本公司應訂定管理指標並定期監督、評估與改善。

5.2 本公司應定期檢視資通安全相關人員之角色與職責，以確保資通安全工作得以有效推動。

5.3 本公司應依員工職務與責任，提供必要之資通安全教育訓練，以符合主管機關及標準之要求。

5.4 本公司應確保資訊資產所處環境之安全，包括機房、網路及雲端環境之適當保護與權限管理。

5.5 本公司應確保資訊不被未經授權之人員或第三方取得、使用或揭露。

5.6 本公司應強化存取控制措施，防止未經授權之存取，確保資訊資產受到適當保護。

5.7 本公司之資訊系統維運應納入資通安全需求，並定期執行弱點掃描或安全檢測，以降低安全風險。

5.8 本公司應確保所有資通安全事件或弱點均依通報程序回報，並予以調查、處理與追蹤改善。

6. 管理審查

6.1 本公司應至少每年實施一次管理審查，評估資訊安全管理系統之適切性、充分性與有效性。

6.2 當組織、業務、技術或法規發生重大變動時，本公司應檢視並更新相關資通安全政策與程序，以維持其持續適用性。

7. 聲明

資訊為本公司重要資產，應採取適當之資通安全管理措施予以保護，防止因內外部威脅造成未經授權之存取、使用、洩漏、竄改或損害。

8. 實施

本政策經本公司「資通安全管理委員會」核定後實施，修訂時亦同。

9. 歷史資料

Issue #	Prepared By	Effective Date	Change
(END)			