國際中橡投資控股股份有限公司資訊安全政策

版次：1.0

公佈日期：2021.04.21

一、目的

定義國際中橡投資控股股份有限公司(以下簡稱本公司)的資訊安全政策，使全體同仁能遵守並有所依循，輔助使用者之各項業務作業順利運行，並確保各項資訊媒體之安全，以達成本公司資訊安全之目標。

二、範圍

適用範圍包括本公司及國內外子公司、合資公司及其他具有實質控制能力之集團關係企業組織之所有正式員工、約聘員工、派遣人員等公司所聘用之人員及外來的訪客和廠商等。

三、名詞定義

(一) 資訊安全

即確保資訊的機密性(Confidentiality)、完整性(Integrity)、可用性(Availability)，使資訊能安全地、正確地、適切地及可靠地運用於達成本公司經營目標之規劃、執行、管理及相關作為上。

(二) 資訊安全管理制度整體管理系統的一部分，以營運風險導向為基礎，用以規劃、建立、實施、運作、監督、查核、維護與改善資訊安全之管理制度。

(三) 機密性

確保只有獲得合法授權的使用者可以存取資訊。

(四) 完整性

保障資訊與資訊處理方法的正確與完整性。

(五) 可用性

確保獲得授權的使用者於有需求時能適時存取資訊及相關資產。

(六) 資訊資產

與資訊處理相關之資產皆屬之，包括擁有或使用之硬體設備、軟體、電子資料、文件及人員等，皆視為資訊資產。

四、權責

本公司之資訊安全治理，委由臺泥資訊股份有限公司代為管理。

五、內容

(一) 管理責任

1. 公司應建立內、外部溝通協調機制，並成立資訊安全管理專職單位，負責資訊安全制度之建立及推動事宜。
2. 組織內部人員應定期接受適當之資訊安全認知教育，並宣導資訊安全政策，以及與工作權責相關之組織程序及資訊安全規定。

(二) 法規遵循

本公司各項資訊安全管理規定及業務活動執行須遵循相關法令或法規之要求，如：資通安全管理法、刑法、國家機密保護法、專利法、商標法、著作權法、個人資料保護法等。

(三) 員工職責

1. 本公司全體員工應遵守此資訊安全政策及相關管理規定，並盡其資訊安全責任及義務，以減少因人員惡意、疏忽或對資訊安全認知不足所引發之資訊安全事件。
2. 違反相關資訊安全規範者，應依本公司相關獎懲規定予以處分，如涉有相關刑責或法律責任者，如營業秘密法、著作權法、個人資料 保護法等，將衡量並依情追訴其法律責任。

(四) 資訊安全管理制度

1. 概述資訊安全管理制度已依照 ISO/IEC 27001：2013 標準之要求建立、記載、
實施及維護之資訊安全管理系統，旨在強化資訊安全管理機制與防禦能力，建立安全及可信賴之電腦化作業環境，確保系統、資料、設備及網路安全，以保護公司重要資訊資產及資訊系統作業正常運作。
2. 運作機制

運作機制依照 ISO/IEC 27001：2013 標準，採用"Plan-Do-Check-Act" PDCA 之循環運作模式，建立與實施資訊安全管理系統，並維繫其有效運作與持續改

進。

(五) 資訊安全管理要點

1. 公司應識別資訊資產並定義適當的保護責任，妥善保護組織內資訊資產且訂定及落實相關規範。
2. 為避免各類資訊設備遭受未經授權之存取、威脅及破壞，應對存取機制及權限管理訂定作業程序與相關規範。
3. 組織內應建立保護資訊資產之政策以保護資訊的可用性、機密性及完整性，並降低資料洩漏之風險。
4. 對內部及外部專案管理的過程中，應考量專案相關之各項資訊安全要求，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. 公司應針對實體與環境安全管理並訂定相關規範，確保組織內所屬各區域之實體安全，預防資訊資產之損失、破壞或竊取，以及企業營運中斷。
6. 公司應對作業及通訊安全進行管理，並規範網路相關系統、設施之使用、授權、監督等各項作業程序，以避免不當作業導致營運中斷、資料遺失、弱點暴露等風險。
7. 公司應針對系統取得、開發及維護納入資訊安全設計及考量，並有對應之管控及要求以降低內系統開發生命週期中不利之衝擊及風險。
8. 公司應確保委外及第三方作業之資訊安全及風險，並針對與其作業與服務設有相關作業及審查程序。
9. 公司應對資訊安全事件建立管理責任與程序，並做出迅速、有效之應變措施，以降低對組織之損害並能確保關鍵性業務持續運作。

(六) 定期審查

資安政策之評估與審查應至少每年評估及審查一次，以反映管理政策、政府法令、及公司業務等之最新發展現況，確保資訊安全管理制度的可行性及有效性，以維持營運和提供適當服務的能力。

六、附件無。