騏億鑫科技股份有限公司
資訊安全政策

騏億鑫重視資訊安全管理，致力建構安全、穩定且具韌性之資訊環境，以維護營運持續性、保障公司資訊資產，並降低外部攻擊及內部資料外洩風險。本公司資訊安全權責單位為資訊室，負責制訂內部資訊安全政策、推動與落實。

本公司資訊安全政策業已制訂，並經總經理核准公告實施。本公司全體人員、與本公司有業務往來之廠商及其員工或臨時雇員等應確實瞭解本資訊安全政策，以維護本公司所有業務之資訊安全與永續經營。於執行各項作業活動時，相關人員皆必須遵循規範，違者將依懲戒規定辦理。

資通安全檢查之控制作業

作業程序	管理措施說明
系統安全防護	● 設置專責人員負責資訊系統安全預防及危機處理 ● 建立網路安全控管機制，保護網路傳輸資料安全 ● 針對跨公司連網環境，加強防毒軟體及防火牆設置 ● 個人電腦及伺服器定期執行病毒掃描與更新病毒碼 ● 定期執行資通安全檢查，並就異常事項進行通報、紀錄及追蹤改善 ● 宣導合法軟體使用觀念，並教育員工正確認識電腦病毒及資訊安全威脅，提升整體資訊安全警覺
身分與存取控制	● 依業務範圍設定使用者帳號及權限，使用者職務異動或離職時，立即撤銷或調整帳號及權限 ● 要求使用者避免採用易遭猜測之密碼並定期變更 ● 每位使用者均配置個人專屬帳號及密碼，即使共用設備亦不得任意存取他人資料

	● 網路硬碟資料依使用者帳號設定存取權限，並定期審查權限及執行資料備份 ● 高權限系統如網路申報、網銀及海關付款系統，由權責主管審慎評估後指派可信賴人員管理
資訊系統復原	● 建置服務中斷通報及應變機制 ● 重要資料定期備份，並依日期、檔案及部門別分類保存，以利查詢與復原

個資保護

騏億鑫遵循《個人資料保護法》規定，於內部資訊安全相關辦法已明確規範，進行資訊處理時，若含有個人資料，應依照法令規定審慎處理，不得私自蒐集或洩漏業務資訊，非公務用途嚴禁調閱使用。資料存取、系統存取與網路存取等設定控制機制，透過分級分類管理制度，控管各式資料可接觸人員及設定其可處理方式，以提升個人資料保護。

如有職務異動、變更、離職、負責人調動等因素，應立即進行權限變更。若更換設備，重要資料應由電腦資訊處備份，再將儲存設備重新格式化後重新配置，以避免前一使用者資料留存。而設備報廢前應由電腦資訊處移除機密性、敏感性資料及授權軟體，並採安全覆寫、清除軟體或物理破壞方式銷毀儲存媒體，確保資料無法還原。如委託第三方銷毀，則額外要求第三方簽訂保密合約，以確保資料安全。

資安事件通報與因應

為即時掌控資通安全事件，並有效降低其所造成之損害，當內部人員發現資通安全事件時，應立即向電腦資訊處主管通報，若事件嚴重程度達中度或重度，應報告或通報總經理。電腦資訊處主管將與相關單位密切合作調查及處理事件，並適時掌握事件處理之進度及其他相關資訊。若資安事件導致利害關係人個資相關權益受損時，應適當地回應與處理。