**國光生物科技股份有限公司資通安全資理辦法**

1. **資通安全管理策略與架構**

國光生物科技股份有限公司自民國113年設立「資訊安全組暨個資管理委員會」，由總經理室、稽核部、人資部、行政管理處等各部處主管代表組成，主要業務包括研議資訊安全管理規範、推動資訊安全活動、辦理資訊安全教育訓練、建立風險管理制度，執行風險管理、建立安全事件緊急應變暨復原措施、追蹤內、外部資訊安全查核後之改善事項及矯正預防措施、就資訊安全事件之紀錄，分析事件發生頻率與研擬改善措施，彙整適用之資訊安全相關之法令規定，建立風險管理制度，執行風險管理。

**總經理**

**資訊安全暨個人資料管理委員會**

**執行單位(資訊部)**

**資安緊急應變小組**

**資安暨個資小組**

資訊安全管理組織定期召開會議檢討計畫執行狀況，每年由資訊部主管定期向董事會審計委員會彙報資安管理成效、資安相關議題及未來執行方向。

1. **資通安全政策**

我司資訊安全組織為有效落實資安管理，確保資料、系統、設備及網路安全，免於因外在威脅或內部人員不當之管理使用，至遭受竄改、揭露、破壞或遺失等風險，維繫營運系統的操作及保障使用者權益。

政策涵蓋範圍包括我司全體員工、委外人員及所有與資訊相關資產之安全管理內容，並透過定期召開例行會議，依據規畫、執行、查核與行動（Plan-Do-Check-Act, PDCA）的管理循環機制，檢視資訊安全政策適用性與保護措施，並定期與資訊安全組暨個資管理委員會回報執行成效。

而本公司於「規畫階段」著重資安風險管理，建立完整的 資 訊 安 全 管 理 系 統（Information Security Management System, ISMS)，從系統面、技術面、程序面降低企業資安威脅，建立符合客戶需求、最高規格的機密資訊保護服務。「執行階段」則建構多層資安防護，持續導入將資安防禦創新技術，將資安控管機制整合內化於軟硬體維運、供應商資安管理等平日作業流程，系統化監控資訊安全，維護國光生物科技股份有限公司重要資產的機密性、完整性及可用性。「查核階段」積極監控資安管理成效，依據查核結果進行資安指標衡量及量化分析，並透過定期模擬演練資安攻擊進行資訊安全成熟度評鑑。「行動階段」則以檢討與持續改善為本，落實監督、稽核確保資安規範持續有效。

1. **具體管理方案**
* 人員安全管理：
	+ 處理相關機密性資訊者，需經我司安全評估程序執行，若職務經異動，管理者將撤銷或移轉相關權限。
	+ 進行相關系統操作及資安概念教育訓練。
* 電腦系統安全管理：
	+ 運用稽核管理系統，確認是否有不當的使用行為。
	+ 使用電腦浮水印機制，防止重要機密文件外洩。
	+ 進行帳號權限管理，並留存相關登入及授權紀錄。
* 網路安全管理：
	+ 設立防火牆管控內外部網路資料傳輸及存取。
	+ 使用網路偵測系統，監控網路流量及相關未授權作業。
* 系統存取控制：
	+ 建置機密性/一般性權限控管機制電腦作業環境
	+ 以使用者帳號管控人員資料存取權限，並定期審查其權限及備份資料。
* 加密系統管理：
	+ 公司文件系統進行加密，以防止資料外流造成資安危害及公司損失。



**113年度投入資通安全管理情形**

* 設置人員：8名
* 軟體更新、授權支出及設備更新投入共計605萬元。
* 因應ERP、MAIL、流程系統，進行更新系統以達到資訊安全。
* 不同建物系統切換還原測試1次。
1. **資通安全風險與因應措施**

國光生物科技股份有限公司已建立全面的網路與電腦相關資安防護措施，仍有一定風險遭滲透或破壞公司製造營運及會計等重要企業功能來自任何第三方癱瘓系統的網路攻擊。

風險因子1

這些網路攻擊以非法方式入侵國光生物科技股份有限公司的內部網路系統，進行破壞公司之營運及損及公司商譽等活動。在遭受嚴重網路攻擊的情況下，國光生物科技股份有限公司的系統可能會失去公司重要的資料，生產線也可能因此停擺。

風險因子2

國光生物科技股份有限公司透過持續檢視和評估其資訊安全規章及程序，以確保其適當性和有效性，但不能保證公司在瞬息萬變的資訊安全威脅中不受推陳出新的風險和攻擊所影響。網路攻擊也可能企圖竊取公司的營業祕密及其他機密資訊，例如客戶或其他利害關係人的專有資訊以及國光生物科技股份有限公司公司員工的個資。

風險因子3

惡意的駭客亦能試圖將電腦病毒、破壞性軟體或勒索軟體導入國光生物科技股份有限公司的網路系統，以干擾公司的營運、對國光生物科技股份有限公司進行敲詐或勒索，取得電腦系統控制權，或窺探機密資訊。

風險因子4

網路攻擊可能導致公司因延誤或中斷訂單而需賠償客戶的損失；或需擔負龐大的費用實施補救和改進措施，以加強公司的網路安全系統；也可能使國光生物科技股份有限公司因涉入公司對其有保密義務之員工、客戶或第三方資訊外洩而導致的相關法律案件或監管調查，而承擔重大法律責任。

因應措施1

國光生物科技股份有限公司公司落實相關改進措施並持續更新，例如建置機台入廠掃毒機制以防止內含惡意軟體的機台進入公司；強化網路防火牆與網路控管以防止電腦病毒跨機台及跨廠區擴散；依電腦類型建置端點防毒措施；導入先進的解決方案以偵測與處理惡意軟體；設計開發資安強化個人電腦供員工使用；設計開發雲端應用安全政策；導入新技術加強資料保護；加強釣魚郵件偵測；建立一個整合的自動化資安維運平台，並定期執行員工警覺性測試及委託外部專家執行資安評鑑。雖然國光生物科技股份有限公司持續加強資訊安全防護措施，但仍無法保證公司免於惡意軟體及駭客攻擊。 此外，國光生物科技股份有限公司需要分享高度敏感及機密的資訊給部分其雇用提供國光生物科技股份有限公司及其全球關係企業服務的第三方廠商，以使其能提供相關服務。儘管國光生物科技股份有限公司在和第三方服務廠商簽訂之服務合約中，要求其遵守保密及／或網路安全規定，但不能保證每個第三方服務廠商都將嚴守這些義務。由上述服務廠商及／或其承攬商所維護的內部網路系統及外部雲端運算網路（例如伺服器），亦會有遭受網路攻擊的風險。若國光生物科技股份有限公司或其服務廠商無法及時解決這些網路攻擊所造成的技術性問題，或確保國光生物科技股份有限公司（及屬於本公司客戶或其他第三方）的數據完整性及可用性，或控制住公司或其服務廠商的電腦系統，皆可能嚴重損及國光生物科技股份有限公司對客戶和其他利害關係人的承諾，而公司營運成果、財務狀況、前景及聲譽亦可能因此遭受重大不利影響。

因應措施2

當員工違反相關規範及程序時，依據「資安事件通報及應變作業程序」進行處置；定期檢討及執行包含資訊安全措施、教育訓練及宣導等改善作為，確保國光生物科技股份有限公司重要機密資訊不外洩。

因應措施3

我司當資安問題產生後，由資訊部人員成立資訊緊急應變小組研判是否為資訊安全事件及是否需請外援單位支援協助研判，並做資安事件紀錄，釐清相關內容後進行追蹤調查且執行檢討改善會議， 依據資安事件檢討會議之結果，由負責人執行矯正措施，進行問題矯正的作業，以降低事件再發生的可能性。

1. **重大資通安全事件**

本公司113年度未發生重大資通安全事件，但仍秉持著防範未然之心態持續編列適當的預算強化資訊技術安全，以降低公司被惡意軟體攻擊的風險。