4.6 資通安全

資通安全攸關企業的營業秘密能否完善保護，中天生技由資訊部制定資通安全政策暨執行計畫，並推動落實與檢討改善；另外由稽核室成立內部稽核小組負責稽核，每年定期執行至少一次抽核資通安全檢查之控制情形，追蹤改善計畫執行成效。

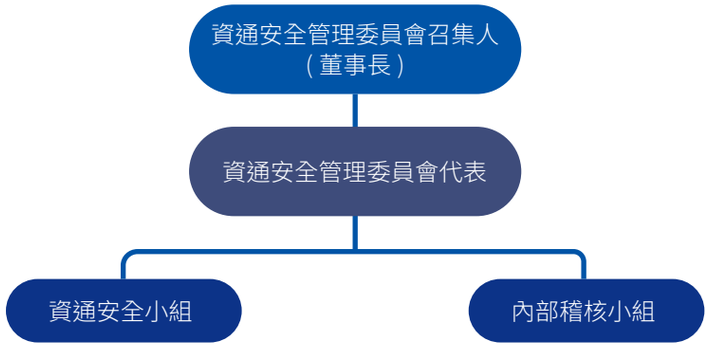
• 資通安全風險管理架構

中天生技針對資通安全管理責由資訊部成立資通安全委員會，由董事長擔任召集人，並設立資通安全管理代表一職，委員會下設資通安全小組及內部稽核小組，共同制定資通安全政策 (以下簡稱本政策) 暨執行計畫。

資通安全小組每季向資通安全管理代表報告公司資安管理現況，每年檢討資安政策。另外由內部稽核小組 (稽核室) 負責稽核，每年定期執行抽核資安政策執行情況，並追蹤缺失改善計畫執行成效。

2024 年資通安全小組設有 2 人，內部稽核小組設有 2 人，期間召開 1 次資通安全會議，年內並未發生重大資通安全違規事件。

資通安全風險管理架構



• 資通安全政策與方針

中天生技《資通安全政策》共包含下列四個方針：

一、制定管理辦法

以標準化規範同仁行為準則。

二、資訊技術

導入先進軟硬體，有效防止資安事件。

三、推廣與改善

提升同仁資安觀念與強化自我保護意識，並不斷修正日新月異的資安執行政策。

四、加入資通安全組織

參加官方或民間資通安全組織，強化資安情訊蒐整能量，提升主動防禦機制。

此外，中天生技《資通安全政策》亦明訂資訊安全管理的適用對象、範圍與原則，涵蓋全體員工、外部協力廠商、資訊資產、系統與應用服務。政策核心內容聚焦於強化公司整體資安治理能力，並落實下列關鍵管理承諾：

1. **持續改善資訊安全管理制度：**公司已建立資訊安全管理系統（ISMS），並定期進行管理審查與內部稽核，以持續精進資安制度並因應法規與業務需求調整作法。
2. **保障資訊資產的完整性與保護：**政策明定須落實資訊分類、權限控管、資料備份與還原等機制，防範未經授權的存取與資料遺失，確保資訊資產之正確性與可靠性。
3. **強化威脅監控與應變處置能力：**公司已建立資安事件通報及應變流程，定期辦理演練及通報教育，強化識別、回應及處置潛在威脅的能力。
4. **強化全員資安責任意識：**所有資訊使用人員皆應遵循本政策規範，並定期參與資安教育訓練與宣導，以提升整體資安防護意識。
5. **落實對第三方之資訊安全管理：**針對涉及資訊處理之供應商與外包單位，訂有相應的資安條款與權限控管措施，納入合約、風險評估與稽核管理，降低外部資安風險。

• 資通安全目標

為維護中天生技資訊資產之機密性、完整性與可用性，中天生技期藉由資通安全政策之實施以達成下列目標：

（一）建立安全及可信賴之資訊化作業環境，確保本公司資料、系統、設備及網路之安全，以保障本公司業務永續運作。

（二）保護本公司業務服務之安全，確保資訊需經授權人員才可存取資訊，以確保其機密性。

（三）保護本公司業務服務之安全，避免未經授權的修改，以確保其正確性與完整性。

（四）建立本公司業務永續運作計畫，以確保本公司資訊業務服務之持續運作。

（五）確保本公司各項業務服務之執行須符合政府相關法令（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）規範之要求。

（六）為保護本公司業務相關個人資料之安全，免於因外在威脅，或內部人員不當之管理與使用，致遭受竊取、竄改、毀損、滅失、或洩漏等風險。

（七）提升對資訊資產之保護與管理能力，降低營運風險。

• 資通安全具體管理措施

中天生技資安具體管理措施如下：

(一) 制定管理辦法

中天生技為健全資通安全管理制度，於 2022 年 10 月份通過 ISO 27001 認證，並已於 2022 年底取得證書，藉由國際資安管理標準落實相關管理制度，以提升同仁資通安全意識，建立正確的電腦網路使用準則。已分別制定資政策及相關管理程序書如下：資通安全政策、資通安全組織與目標管理程序書、資訊資產管理程序書、資通安全風險評鑑、實體安全、作業安全、存取控制、資通安全事件管理等相關程序書及說明書。

(二) 資訊技術

本公司在資訊安全防護上，加強軟體與硬體方面多層次防護，其中包含：帳號複雜性密碼驗證、主機與用戶端防毒、上網行為管理 / 惡意網站防護、防火牆阻擋、主機資料備份、資料加密、網路 IP 管理及 EDR(端點偵測與回應) 等防護措施。2023 年 EDR 部署範圍約為 30%，目前已完成核心主機 EDR 的部署，以防堵惡意攻擊。

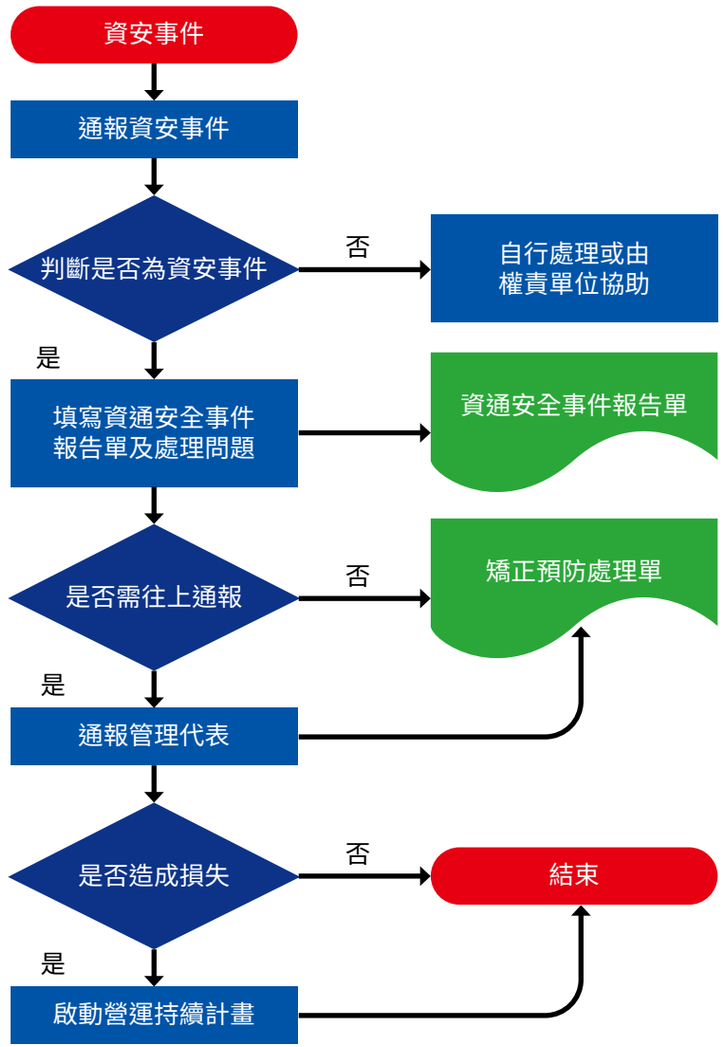
(三) 推廣與改善

為提升同仁資通安全觀念與強化自我保護意識，每年至少辦理 1 次資通安全管理審查會，針對年內相關資安制度與事件進行監督與管制，另每年至少舉行資通安全宣導 3 小時、資通安全事件通報演練 1 次以及不定期資安線上宣導。2024 年共計 3 場次員工資通安全教育訓練，並完成 14 次線上電郵資安宣導。此外，2024 年共計執行 4 次電子郵件社交工程演練，以提升公司人員資安意識。

(四) 加入資安聯防機制

中天生技已於 2022 年 9 月加入 TWCERT/CC 資安聯盟，並於 2023 年 8 月加入中華民國資訊軟體協會 - 資安長聯誼會，不定期透過上述平台進行網駭情資交換，期藉由聯防機制，網駭情資共享，擴大公司資安防禦廣度，及強化資安韌性。

資通安全事件通報與應變流程圖



2024 年中天生技資通安全教育訓練統計

資安訓練課程名稱	對象	參與人次	課程時數	涵蓋率
物聯網安全與近期資安案例剖析	全體員工	124	3	91%
資安災變時各單位分工及注意事項 (單位主管及稽核人員)	單位主管	13	1	100%
企業肅貪暨資安宣導	指定人員	9	1	100%

2024 年棉花田資通安全教育訓練統計

資安訓練課程名稱	對象	參與人次	課程時數	涵蓋率
ISO 27001 資訊安全課	總部全體員工	44 人	2.5	75%
物聯網安全與近期資安案例剖析	總部全體員工	49 人	3	83%

2024 年中天 (上海) 資通安全教育訓練統計

資安訓練課程名稱	對象	參與人次	課程時數	涵蓋率
資訊安全	全體員工	46	1	71%

註：涵蓋率 = 參與人次 / 應受訓人次

中天生技 (含子公司) 資通安全管理成效表

分類	2021	2022	2023	2024
重大資通安全事件發生件數	0	0	0	0
資料洩漏發生件數	0	0	0	0
因資訊洩漏致受影響的員工或客戶數 (人)	0	0	0	0
因資安事件被裁罰的金額 (新台幣)	0	0	0	0

註：重大資通安全事件係依據公司資通安全事件管理程序書之定義

• 導入 ISO 27001 ISMS 制度

為展現中天生技對於資安的重視程度，並期與國際資安標準接軌，中天生技已於 2022 年第二季導入 ISO 27001 Information Security Management System (ISMS)，並於 2022 年 8 月初成立資通安全管理委員會，由董事長為委員會召集人，授權管理代表推動資通安全管理及運作、重要資訊保護措施、災害演練與執行計畫等。

此次導入 ISO 驗證項目，包含系統與管理面，執行項目包含風險評估、弱點修復、安全防護、風險驗證、資產清查及風險評鑑及人員教育訓練等工作項目，期符合國際資訊安全管理規範。2022 年 10 月已完成 ISO 27001 資訊系統管理認證，並已於 2022 年 12 月取得證書，2023 年已由第三方驗證單位完成年度續評，證書有效期至 2025 年 12 月。


Certificat
Certificate
MICROBIO CO., LTD.
中天生物科技股份有限公司
NF EN ISO/IEC 27001:2017 (Europe) - ISO/IEC 27001:2013 + COR 1:2014 + COR 2:2016 (International)