# 正文科技股份有限公司
# 資訊安全風險管理

## 一、 資訊安全政策：

本公司為強化資訊安全管理，確保資訊資產符合 ISO 27001 資訊安全管理系統之機密性、完整性與可用性，以杜絕毀損、失竊、洩漏、竄改、濫用與蓄意等風險，維持資訊系統與業務持續運作，並符合相關法令規範與內外部利害相關者之要求，所有人員應確實瞭解此政策，並遵循相關資安管制作業程序與規範。資訊安全政策如下:

1. 本公司內部所有正式員工、約聘與派遣人員等公司所聘用之人員，皆應清楚且遵循此資訊安全政策與規範。
2. 所有人員，均有責任及義務保護其所取得或使用之資訊資產，防止遭未經授權存取、篡改、破壞或不當揭露。
3. 員工之工作分派應考量職能分工，職務責任範圍須作適當區隔，僅授予工作所需之必要權限與必要資訊，避免資訊或服務遭未經授權修改或誤用。
4. 員工有義務保護公司機敏資料，禁止未經授權的情況下接觸、使用或將該資訊揭露、告知予業務無關之同仁、廠商及其它客戶。
5. 所有人員之個人電腦應安裝防毒軟體且定期更新病毒碼，並禁止於本公司資訊資產上安裝、使用、下載非法或未授權之軟體。
6. 各單位如發生資訊安全事件，應依據資訊安全事件管理程序進行通報。
7. 訂定資訊作業營運持續管理程序，重要設備應建置適當之備援或監控機制，並定期測試與演練，確保公司業務持續運作。
8. 新系統開發與資訊設備建置前，須將風險、安全因素納入考量，防範危害系統安全之情況發生。
9. 制訂資訊安全內部稽核與風險評鑑管理程序，定期進行稽核與資訊資產之風險評估，確保落實各項資安規定，使資安管理制度持續正常運作。
10. 任何危及資訊安全之行為，若涉及不法情事者，員工除須受行政處分外，並應自負相關法律責任。

## 二、 資訊安全組織：

為確保本公司資訊安全管理系統能持續有效運作，特設立資訊安全委員會，由資安單位最高主管擔任主任委員，定期召開管理審查會議，制訂與檢討資訊安全管理目標及政策，建立資訊業務永續運作計畫，執行符合相關法令或法規要求之資訊業務活動運作。

此為委員會負責資訊安全管理手冊之制訂、管理系統建置作業及相關活動之督導，內容包含：

1. 依照資訊安全策略方向及本公司之營運需求、法令異動、資訊安全需求、技術變遷及可接受風險水準等因素，審議與公布資訊安全管理手冊及規範。
2. 覆核資訊安全風險評鑑報告，並根據該報告之結果，決定資訊安全可接受風險水準。
3. 協商訂定資訊安全各項管制措施與處理程序。
4. 執行資訊安全管理系統之實際導入作業。
5. 檢討並改進現行資訊安全管理系統，以提高其運作效率及有效性。
6. 監控並檢討重大安全事件之應變處理與改善措施。
7. 針對新科技之導入或新資訊與通訊系統專案、評估可能之資訊安全衝擊。

## 三、 已實施之管制措施，如下：

| 類別 | 說明 | 相關措施 |
|---|---|---|
| 權限管理 | 人員帳號、權限管理與系統操作 | 1. 人員帳號權限管理與審核<br>2. 定期盤點人員帳號權限<br>3. 重要機房之出入權限管理 |
| 存取管制 | 人員存取內外部系統、資料傳輸管道安全措施 | 1. 系統存取權限管理<br>2. 管制資料檔案存取<br>3. 操作行為軌跡紀錄 |
| 外部威脅 | 內部系統潛在弱點、防毒防駭之保護措施 | 1. 系統弱點掃描、定期系統更新與弱點補強<br>2. 惡意行為偵測與防範，包含偵測病毒之防毒軟體與更新、MDR 威脅偵測應變代管服務、新世代防火牆(NGFW)第七層應用系統進階防護，內網防火牆設備，於主機網段進行加強防護..等<br>3. 郵件安全，包含垃圾郵件防堵與郵件病毒偵測<br>4. 透過第三方威脅偵測 SecurityScorecard，進行網路風險評估，本年度皆維持於等級 A |
| 系統可用 | 系統可用狀態與服務中斷時之處置措施 | 1. 監控系統與網路可用狀態與通報機制 |

| | | |
|---|---|---|
| | | 2. 資訊機房不斷電系統採用機架式模組擴充彈性高，可供電持續至少 90 分鐘<br>3. 採用新一代備份軟硬體，符合主流 3-2-1 備份原則，強化資料異地備份，並針對可能之破壞進行強化管控<br>4. 中斷服務之應變措施<br>5. 備援機制與資料異地備份<br>6. 定期災害還原演練與還原 |
| 其他強化 | | 1. 建立新日誌管理平台，記錄保存期間符合客戶與法規規定，並建立適當保護機制<br>2. 官網導入 WAF(應用程式防火牆)，避免駭客 DDos(分散式阻斷服務)攻擊 |

## 四、 ISO 27001 資訊安全管理系統證書

為符合資訊安全具體管理方案，相關管制措施需與國際資安管理系統接軌，並滿足利害關係人之資安需求，本公司已於 2010 年 8 月導入 ISO 27001 認證並取得證書，目前證書版本為最新版本 ISO 27001:2022，有效期為 2025 年 7 月至 2028 年 8 月，透過此資訊安全管理系統之導入，有效強化資訊安全管理與執行能力，並保護公司與客戶之資產安全。

# Certificate of Registration

INFORMATION SECURITY MANAGEMENT SYSTEM - ISO/IEC 27001:2022

This is to certify that: Gemtek Technology Co., Ltd.
No. 15-1, Zhonghwa Road
Hsinchu Industrial Park
Hukou
Hsinchu County
303035
Taiwan

Holds Certificate No: **IS 563508**

and operates an Information Security Management System which complies with the requirements of ISO/IEC 27001:2022 for the following scope:

The provision of development, operation and maintenance of information systems, service delivery, management of network, data center, and related supporting security activities within the IT Division.
This is in accordance with the Statement of Applicability, QP2415, version 1.6 dated 13 May 2025.

For and on behalf of BSI:

Michael Lam, Senior Vice President, APAC Assurance

Original Registration Date: 2010-08-02
Latest Revision Date: 2025-07-01

Effective Date: 2025-08-02
Expiry Date: 2028-08-01