Goodbaby International

資訊安全政策

1. 目的

好孩子國際集團資訊安全政策的目的是定義好孩子國際集團及其子公司的整體資訊安全方法。本政策支持：

- 檢測和預防資訊安全性漏洞，例如濫用網路資料、應用程式和電腦系統
- 維護公司聲譽，包括遵守道德和法律責任
- 尊重客戶在個人資料分類、存儲和處理方面的權利

2. 範圍

本政策的適用範圍是所有好孩子國際集團的雇員。

3. 資訊安全目標

好孩子國際資訊安全具有以下目標。在這些目標中，術語“資料”也用於指代存儲、處理和傳輸資料的系統、應用程式和網路，以及這些系統上的任何資訊。

- **保密性：** 確保只有授權使用者和流程能夠訪問或修改資料
- **完整性：** 確保資料保持在正確狀態，並且無人能夠有惡意或無意地對其進行不當修改
- **可用性：**確保授權使用者能夠在需要時隨時訪問所需的資料

4. 資訊安全原則

好孩子國際資訊安全計畫以六個核心原則為基礎。這些原則將用於指導任何與集團或區域性 資訊安全計畫相關的決策。

a) 資訊安全計畫的存在是未來保護好孩子國際的資訊和資訊系統
b) 資訊安全在流程、人員和技術方面的投資將與面臨風險的資訊和資訊系統的價值相稱
c) 資訊安全保護資訊和資訊系統的方法將遵守所有必要區域的法律法規
d) 資訊安全將以風險管理驅動的方法來應對實際和潛在的威脅
e) 資訊安全服務將受益於服務管理原則中
f) 資訊安全將利用國際公認的網路安全標準和良好實踐

5. 資訊安全方法

好孩子國際所採用的具體資訊技術安全技術、流程和程式因子公司而異，但集團範圍內的資訊技術安全政策是統一的，概述如下。

5.1. 框架和最佳實踐

好孩子國際採用了互聯網安全中心 (CIS) 關鍵安全控制，以構建其資訊安全方法並遵守國際標準和最佳實踐。

5.2. 可接受的使用政策

將遵循一項可接受使用政策，描述雇員應如何使用 IT 資源。所有新雇員在入職過程中都需要閱讀並簽署此政策。

5.3. 存取控制

5.3.1. 用戶認證

連接網路時，訪問需要用戶名和密碼。將強制執行密碼強度並定期更新密碼。

5.3.2. 遠端存取

從遠端位置（即非專用好孩子國際辦公室的地點）訪問需要使用 VPN 解決方案，並通過多因素認證 (MFA) 進行保護，以訪問公司內部系統。

5.3.3. 關鍵業務雲服務

訪問託管在雲中的關鍵業務服務（例如 Office 365）時，從遠端位置連接將使用 MFA 進行保護。

5.3.4. 物理存取控制

資料中心、伺服器機房和網路機櫃將始終上鎖，僅向必要的 IT 工程師和支援人員提供存取權限。建議使用門禁卡或金鑰扣控制進入建築物。

5.4. 資料備份和恢復

對關鍵資料、系統和伺服器進行每日備份。

5.5. 安全意識和培訓

IT安全政策將與所有雇員共用。新雇員將在入職過程中接受介紹，並通過電子學習平臺或課堂培訓進行培訓。這些課程將告知雇員在資訊安全方面對公司的義務，並培訓雇員識別社會工程學（網路釣魚）攻擊。

5.6. 系統和通信保護

5.6.1. 端點保護

所有端點（伺服器和工作站）至少要安裝防病毒和端點檢測與回應 (EDR) 軟體。

5.6.2. 資料丟失保護

實施控制措施以限制：使用雲存儲服務僅限於批准的提供商；使用可移動介質（例如 USB）僅限於授權的加密設備；最大電子郵件附件大小。

5.6.3. 資料加密

實施控制措施，根據資料保護政策確保對靜態和傳輸中的公司資料進行加密。

5.7. 安全事件管理

維護安全事件回應程式，該程式定義發生不同類型安全事件後應採取的措施。

所有員工必須在發現系統漏洞、事件或可能導致安全事件的任何情況後，儘快向服務台報告，但最遲不得超過發現後24小時。

6. 風險管理計畫

為了按照適用法規保護好孩子資料的機密性、完整性和可用性（CIA），好孩子 IT 團隊根據 ISO27005 和 NIST 800-30 制定了網路安全的風險管理流程。好孩子次採用資訊安全風險管理流程來識別風險並實施應對和管理計畫，其中包括管理資訊安全政策的意外情況和風險接受流程。

6.1. 已識別的 IT 風險

以下風險已被認定為對好孩子國際 IT 的基礎設施和系統造成潛在威脅。

- **網路安全事件**：勒索軟體、惡意軟體或資料洩露。
- **IT 硬體故障**：伺服器、存放裝置或網路設備故障。
- **電力中斷**：電力中斷影響 IT 系統和資料中心。
- **自然災害**：洪水、火災或地震影響資料中心和關鍵 IT 基礎設施。
- **人為錯誤**：人為意外刪除或修改關鍵資料或配置錯誤。
- **應用程式停機**：由於軟體漏洞或配置錯誤導致的關鍵軟體故障。
- **協力廠商故障**：由服務提供者（包括雲服務、備份服務和電信服務）引起的故障。

6.2. 預防措施

為降低風險並應對潛在的風險，採取以下預防措施：

- **網路安全措施**：採用多因素認證（MFA）、加密技術及網路安全控制措施，以降低網路威脅暴露風險。
- **基礎設施冗餘**：在關鍵資料中心部署冗餘伺服器、網路鏈路及電源供應系統。
- **資料備份策略**：遵循《資料備份與恢復政策》，定期將所有關鍵資料備份至異地存儲位置及雲環境。
- **常規維護**：定期對硬體和軟體進行維護和升級，以防止故障發生。
- **服務級別協定（SLAs）**：與關鍵服務提供者簽訂 SLAs，以確保服務中斷最小化並優先回應。

6.3. IT 應急計畫

在發生中斷的情況下，應急措施將包括：

- **資料中心切換**：啟動配備鏡像基礎設施的備用資料中心，以確保關鍵服務正常運行。
- **雲端恢復**：若本地系統故障，將關鍵應用程式遷移至雲端服務。
- **遠端存取支持**：確保員工可在辦公場所受影響時，從遠端位置安全訪問 IT 系統。
- **協力廠商服務**：使用協力廠商備份和災難恢復服務提供者，以確保持續訪問 IT 資源。

7. 商業影響分析

7.1. 關鍵 IT 服務與應用程式

以下IT系統和應用程式對業務運營至關重要，必須優先進行恢復：

- **企業資源計畫（ERP)**：用於財務管理、採購及供應鏈管理的核心業務應用程式。
- **客戶關係管理（CRM)**：用於管理客戶互動及銷售流程的應用程式。
- **電子郵件與協作工具**：用於業務溝通的 Microsoft Exchange、Office 365 及 Microsoft Teams。
- **基於網頁的平臺**：對客戶互動與銷售至關重要的線上平臺。
- **製造系統**：支援生產線及庫存管理的 IT 系統。
- **供應鏈管理軟體**：追蹤從供應商到客戶的貨物與材料流動的應用程式。

7.2. IT 中斷影響

IT中斷的影響將根據中斷類型和持續時間而有所不同：

- **財務損失**：系統停機時間過長可能導致銷售損失和錯失商機。
- **運營中斷**：無法訪問關鍵系統可能導致製造、客戶服務和訂單履行等業務流程停滯。
- **聲譽損害**：長時間的系統中斷可能影響客戶信心和品牌形象。
- **監管與合規問題**：IT 中斷可能導致違反資料保護法規（如 GDPR），從而引發法律處罰。

7.3. 恢復時間目標（RTO）與復原點目標（RPO）

根據服務水準協定（SLA）確定RTO，並根據備份與恢復政策確定RPO。

8. 支持政策

政策和標準對於建立、維護和監控適當的資訊安全實踐至關重要。集團資訊安全政策基於以下額外的IT安全政策：

可接受的使用政策 / 資料保護標準政策 / 存取控制政策 / 資產管理政策 / 配置管理政策 / 資料備份與恢復政策 / 特權帳戶管理政策 / 安全意識與培訓政策 / 安全事件管理政策 / 安全監控政策 / 系統與通信保護政策 / 漏洞管理政策

9. 所有權與批准

在好孩子國際董事會的指導下，集團IT系統與服務副總裁和集團IT安全總監負責該政策的執行與遵守。