信息安全政策

1. 目的

好孩子国际集团信息安全政策的目的是定义好孩子国际集团及其子公司的整体信息安全方法。本政策支持：

- 检测和预防信息安全漏洞，例如滥用网络数据、应用程序和计算机系统
- 维护公司声誉，包括遵守道德和法律责任
- 尊重客户在个人数据分类、存储和处理方面的权利

2. 范围

本政策的适用范围是所有好孩子国际集团的雇员。

3. 信息安全目标

好孩子国际信息安全具有以下目标。在这些目标中，术语“数据”也用于指代存储、处理和传输数据的系统、应用程序和网络，以及这些系统上的任何信息。

- **保密性：** 确保只有授权用户和流程能够访问或修改数据
- **完整性：** 确保数据保持在正确状态，并且无人能够有恶意或无意地对其进行不当修改
- **可用性：**确保授权用户能够在需要时随时访问所需的数据

4. 信息安全原则

好孩子国际信息安全计划以六个核心原则为基础。这些原则将用于指导任何与集团或区域性 信息安全计划相关的决策。

a) 信息安全计划的存在是未来保护好孩子国际的信息和信息系统
b) 信息安全在流程、人员和技术方面的投资将与面临风险的信息和信息系统的价值相称
c) 信息安全保护信息和信息系统的方法将遵守所有必要区域的法律法规
d) 信息安全将以风险管理驱动的方法来应对实际和潜在的威胁
e) 信息安全服务将受益于服务管理原则中
f) 信息安全将利用国际公认的网络安全标准和良好实践

5. 信息安全方法

好孩子国际所采用的具体信息技术安全技术、流程和程序因子公司而异，但集团范围内的信息技术安全政策是统一的，概述如下。

5.1. 框架和最佳实践

好孩子国际采用了互联网安全中心 (CIS) 关键安全控制，以构建其信息安全方法并遵守国际标准和最佳实践。

5.2. 可接受的使用政策

将遵循一项可接受使用政策，描述雇员应如何使用 IT 资源。所有新雇员在入职过程中都需要阅读并签署此政策。

5.3. 访问控制

5.3.1. 用户认证

连接网络时，访问需要用户名和密码。将强制执行密码强度并定期更新密码。

5.3.2. 远程访问

从远程位置（即非专用好孩子国际办公室的地点）访问需要使用 VPN 解决方案，并通过多因素认证 (MFA) 进行保护，以访问公司内部系统。

5.3.3. 关键业务云服务

访问托管在云中的关键业务服务（例如 Office 365）时，从远程位置连接将使用 MFA 进行保护。

5.3.4. 物理访问控制

数据中心、服务器机房和网络机柜将始终上锁，仅向必要的 IT 工程师和支持人员提供访问权限。建议使用门禁卡或密钥扣控制进入建筑物。

5.4. 数据备份和恢复

对关键数据、系统和服务器进行每日备份。

5.5. 安全意识和培训

IT安全政策将与所有雇员共享。新雇员将在入职过程中接受介绍，并通过电子学习平台或课堂培训进行培训。这些课程将告知雇员在信息安全方面对公司的义务，并培训雇员识别社会工程学（网络钓鱼）攻击。

5.6. 系统和通信保护

5.6.1. 端点保护

所有端点（服务器和工作站）至少要安装防病毒和端点检测与响应 (EDR) 软件。

5.6.2. 数据丢失保护

实施控制措施以限制：使用云存储服务仅限于批准的提供商；使用可移动介质（例如 USB）仅限于授权的加密设备；最大电子邮件附件大小。

5.6.3. 数据加密

实施控制措施，根据数据保护政策确保对静态和传输中的公司数据进行加密。

5.7. 安全事件管理

维护安全事件响应程序，该程序定义发生不同类型安全事件后应采取的措施。

所有员工必须在发现系统漏洞、事件或可能导致安全事件的任何情况后，尽快向服务台报告，但最迟不得超过发现后24小时。

6. 风险管理计划

为了按照适用法规保护好孩子数据的机密性、完整性和可用性（CIA），好孩子 IT 团队根据 ISO27005 和 NIST 800-30 制定了网络安全的风险管理流程。好孩子次采用信息安全风险管理流程来识别风险并实施应对和管理计划，其中包括管理信息安全政策的意外情况和风险接受流程。

6.1. 已识别的 IT 风险

以下风险已被认定为对好孩子国际 IT 的基础设施和系统造成潜在威胁。

- **网络安全事件**：勒索软件、恶意软件或数据泄露。
- **IT 硬件故障**：服务器、存储设备或网络设备故障。
- **电力中断**：电力中断影响 IT 系统和数据中心。
- **自然灾害**：洪水、火灾或地震影响数据中心和关键 IT 基础设施。
- **人为错误**：人为意外删除或修改关键数据或配置错误。
- **应用程序停机**：由于软件漏洞或配置错误导致的关键软件故障。
- **第三方故障**：由服务提供商（包括云服务、备份服务和电信服务）引起的故障。

6.2. 预防措施

为降低风险并应对潜在的风险，采取以下预防措施：

- **网络安全措施**：采用多因素认证（MFA）、加密技术及网络安全控制措施，以降低网络威胁暴露风险。
- **基础设施冗余**：在关键数据中心部署冗余服务器、网络链路及电源供应系统。
- **数据备份策略**：遵循《数据备份与恢复政策》，定期将所有关键数据备份至异地存储位置及云环境。
- **常规维护**：定期对硬件和软件进行维护和升级，以防止故障发生。
- **服务级别协议（SLAs）**：与关键服务提供商签订 SLAs，以确保服务中断最小化并优先响应。

6.3. IT 应急计划

在发生中断的情况下，应急措施将包括：

- **数据中心切换**：激活配备镜像基础设施的备用数据中心，以确保关键服务正常运行。
- **云端恢复**：若本地系统故障，将关键应用程序迁移至云端服务。
- **远程访问支持**：确保员工可在办公场所受影响时，从远程位置安全访问 IT 系统。
- **第三方服务**：使用第三方备份和灾难恢复服务提供商，以确保持续访问 IT 资源。

7. 商业影响分析

7.1. 关键 IT 服务与应用程序

以下IT系统和应用程序对业务运营至关重要，必须优先进行恢复：

- **企业资源计划（ERP)**：用于财务管理、采购及供应链管理的核心业务应用程序。
- **客户关系管理（CRM)**：用于管理客户互动及销售流程的应用程序。
- **电子邮件与协作工具**：用于业务沟通的 Microsoft Exchange、Office 365 及 Microsoft Teams。
- **基于网页的平台**：对客户互动与销售至关重要的在线平台。
- **制造系统**：支持生产线及库存管理的 IT 系统。
- **供应链管理软件**：追踪从供应商到客户的货物与材料流动的应用程序。

7.2. IT 中断影响

IT中断的影响将根据中断类型和持续时间而有所不同：

- **财务损失**：系统停机时间过长可能导致销售损失和错失商机。
- **运营中断**：无法访问关键系统可能导致制造、客户服务和订单履行等业务流程停滞。
- **声誉损害**：长时间的系统中断可能影响客户信心和品牌形象。
- **监管与合规问题**：IT 中断可能导致违反数据保护法规（如 GDPR），从而引发法律处罚。

7.3. 恢复时间目标（RTO）与恢复点目标（RPO）

根据服务水平协议（SLA）确定RTO，并根据备份与恢复政策确定RPO。

8. 支持政策

政策和标准对于建立、维护和监控适当的信息安全实践至关重要。集团信息安全政策基于以下额外的IT安全政策：

可接受的使用政策 / 数据保护标准政策 / 访问控制政策 / 资产管理政策 / 配置管理政策 / 数据备份与恢复政策 / 特权账户管理政策 / 安全意识与培训政策 / 安全事件管理政策 / 安全监控政策 / 系统与通信保护政策 / 漏洞管理政策

9. 所有权与批准

在好孩子国际董事会的指导下，集团IT系统与服务副总裁和集团IT安全总监负责该政策的执行与遵守。