HP 安保措施概要

为了保护客户数据，HP 遵循包括政策、做法、程序和组织结构在内的一整套健全的信息安全控制措施，以保障自身信息和客户信息（包括如 HP 客户和数据处理附录所定义的个人数据）的保密性、完整性和可用性。以下概述 HP 在整个公司采取的技术/组织安保措施。

1. 安保政策

   HP 制定全球适用的政策、标准和程序，旨在保护 HP 和客户的数据。HP 安保政策的细节保密，以保护 HP 数据和系统的完整性。不过，下文概述了我们的关键政策。

2. 信息安全组织

   HP 的信息安全方案旨在指导和维护组织的信息安全策略和控制措施。这一体系确保在整个企业范围内遵守 HP 的安保政策和控制措施，并遵守客户的安保要求。遵照行业标准的网络安全框架、法律和法规精心设计该框架，并且每年审查一次该框架以适应 HP 遭遇的多变威胁态势。

3. 网络安全风险管理

   HP 的网络安全风险管理方案旨在维护其信息资产的保密性、完整性和可用性。该方案提供一种始终如一的方法，以供发现、评估、优先考虑、处理、补救、跟踪和报告网络安全风险。HP 将其风险偏好定义为遭受损失的可接受程度，将其风险承受能力定义为从这种偏好产生的差异程度。使用经过定义的方法评估风险，这样使 HP 可将信息安全风险降低到可接受的程度。此方案与 HP 的企业风险管理流程一致。

4. HR 安保

   HP 人力资源安保政策通过建立访问设施、信息系统和其他资产的流程，在员工的整个工作周期内确保信息安全。其中包括通过保密和非披露协议获得书面确认以及开展背景审查程序。所有应聘 HP 职位的人员都必须根据相关法律、法规和道德规范完成背景核查。

5. 资产管理

   HP 制定了一个流程，以供发现技术信息资产、为关键资产分类以及为每种信息分类类型（包括那些含有个人数据的类型）维护成文的处理程序。这些程序涉及存储、传输、通信、访问、日志记录、留存、销毁、处置、事故管理和违规通知。HP 安保政策和标准还规定要安全处置各种介质。

上次更新时间：2024 年 9 月

6. 数据安全

HP 的数据安全方案概述为保护数据的机密性、真实性和完整性而必须执行的安保做法和技术控制措施。法律要求、价值、关键性和对未经授权的披露或修改的敏感性是决定如何根据 HP 的数据安全策略为信息分类的一部分因素。该政策除了数据处理程序之外，还概述数据加密、删除、收集和处理、留存、备份以及数据丢失防护。

7. 访问控制

HP 将最小权限原则用于逻辑访问控制，通过唯一用户 ID 和密码提供用户访问。密码政策定义复杂性、强度、有效期和是否不准设置用过的密码。定期审查访问权限，并在人员离职时吊销访问权限。执行商定的用户账户创建和删除程序，以便在聘用期间授予和吊销对客户端系统的访问权限。

8. 密码学

HP 规定了一整套健全的密码学流程以确保信息资产的保密性、完整性和可用性。获批的协议要求加密某些资产，包括那些含有个人数据的资产。我们的密码学方案涉及使用多种数学方法保护信息和通信，从而确保只有获得授权的各方可访问数据。HP 的信息安全方案的一个重要组成部分是保护数据免遭未经授权的访问和篡改。

9. 实物和环境安保

使用多种实物和电子访问控制措施，包括安保人员、电子访问控制措施和闭路电视 (CCTV) 保护 HP 设施。还为设施配备必要的基础设施支持，包括温度控制措施和备用电源，其中使用 UPS 和/或柴油发电机支持关键服务。所有 HP 人员都登记在册，并且必须佩戴适当的身份识别标牌。

10. 操作管理

HP 针对包括工作站、服务器和网络设备在内的技术基础设施制定了最低加固要求。这些设备使用预先加固的操作系统映像，并且其要求因操作系统和执行的控制措施而异。此外，HP 还部署了全年无休受监控和管理的网络入侵检测/预防系统 (NIDS/NIPS)。

11. 通信安全

通信安全确保信息在公司网络中受到保护。其中包括安装和管理网络安全组件（如防火墙）、网络隔离以及 Web 过滤和电子邮件处理控制措施。此外，它还涉及监控和管理通信渠道以检测和防止未经授权的访问或数据泄露。

12. 系统安全

HP 的政策规定，对于系统和软件在其生命周期内必须采用安全的开发方法。软件开发生命周期涵盖启动、开发/获取、实施、操作和处置。评估所有系统组件对整体安全性的影响。HP 针对应用程序服务事务制定了多种控制措施，包括用户凭证验证、数字签名、加密、安全通信协议以及将事务详细信息存储在适当的网络安全区域中。还定期执行内部漏洞扫描。

上次更新时间：2024 年 9 月

13. 第三方和分包商

HP 通过相应的流程选择符合详尽的合同安全要求的分包商。HP 网络安全部门对处理 HP 或客户数据或访问 HP 网络的适用供应商开展风险评估，以核实制定了具有实物、技术和管理保护措施的信息安全方案。供应商必须接受此评估后方可访问 HP 信息。

14. 信息安全事故管理

HP 有一套详尽的网络事故管理流程，该流程概述用途、范围、角色、责任、管理层承诺、组织协调、执行程序和合规检查。每年审查并更新一次此流程。包括接受过事故应对和危机管理培训的 HP 网络安全人员在内的网络事故应对小组定期对该流程和任何事故或事件进行模拟审查。

15. 业务连续性管理

HP 的全球运营连续性方案通过协作、标准化和记录在案的规划流程，确保端到端连续性。公司定期执行业务连续性计划以确保其有效性，并且每年至少测试和更新一次所有计划。此外，所有参与业务连续性计划的人员都接受适当的培训。

16. 合规性

合规性决定了 HP 如何制定方法以满足法律、合同和内部对有效的信息安全方案的期望。定期信息安全审查确保将协议融入到每个业务团体的运营中。随着要求不断变化，审查过程还不断更新文档以反映当前的法律义务。

17. 支付卡行业

支付卡行业 (PCI) 框架指导 HP 制定实现 PCI 合规性的方法，并概述与 PCI DSS 一致的商业责任和安全控制措施。通过安装和维护防火墙等网络安全控制措施，HP 确保符合 PCI 合规性要求。

18. HP 产品安全

HP 产品安全包括用于保护 HP 产品的基本做法，如代码签名、管理产品安全漏洞、发布安全公告和报告产品安全问题。这些措施确保 HP 产品对用户始终安全而可靠。产品安全是 HP 的重中之重，因为它有助于保持客户信任和防范潜在威胁。

19. HP 服务安全

HP 服务安全包括用于保护为 HP 客户提供的服务的基本做法。此政策涉及服务安全的多个方面，包括 HP 基础设施托管、第三方托管、合作伙伴托管和客户托管的环境。这些措施确保 HP 服务对用户始终安全而可靠。通过实行健全的安全做法，HP 确保其产品和服务的安全和完整性，从而为所有用户创造一个安全和值得信任的环境。

上次更新时间：2024 年 9 月