SAP Ariba 在线服务安全披露政策

SAP Ariba 承诺维护 SAP Ariba 在线服务（也称为 SAP Ariba 云服务）中所包含的客户信息的安全性和完整性。SAP Ariba 采用行业安全控制卓越实践保护所控制的信息免遭丢失、滥用或篡改。

为了防止未经授权的访问、维护数据准确性并确保正确使用信息，SAP Ariba 采取了适当的物理、电子和管理控制措施，确保我们在 SAP Ariba 在线服务中收集的信息安全。这些控制措施包括：

- 构建多级防火墙，基于系统角色隔离和保护网络段
- 使用 SSL 技术加密数据传输
- 使用服务器端和客户端数字证书
- 制定基于角色的管理访问政策和程序
- 一级和二级数据中心采用密码编码的访问胸卡、生物识别扫描以及 24 小时视频监控和保安员来控制访问
- 全面实施内部绩效、安全监控和审计
- 进行入侵检测和分析
- 制定详细的安全政策、流程和程序
- 由独立第三方评估人员执行安全审计

为了确保 SAP Ariba 在线服务中服务和信息的可用性，SAP Ariba 实施了以下组件：

- 灾难恢复计划
- 详细的备份策略
- 将数据写入一级数据中心内高度可用的基于磁盘的存储系统，并复制到位于二级（备用）数据中心的合作伙伴数据库
- 高可用性群集数据库服务器
- 冗余系统、电源和网络连接
- 与服务提供商达成服务水平协议，保证服务水平
- 全面的变更管理和测试策略
- 针对一级问题提供每周 7 天、每天 24 小时的支持服务

针对您正在使用的特定 SAP Ariba 在线服务的 SAP Ariba 云服务解决方案文档详细介绍了相关政策、程序和架构。此文档应客户要求提供，但需签署单独的保密协议。

如果您对上述任何信息有任何疑问，请联系 SAP Ariba Customer Support 服务。

请注意：如有任何冲突或非英文版本的翻译发生实质性变更，以本安全披露的英文版本为准。

*****

最后更新日期：2021 年 2 月 5 日