Power Integrations 供应商网络安全政策

修订日期：2026年1月

The online version of this manual is the updated version and takes precedence over any printed copy.
本手册的在线版本为最新版本，优先于任何印刷版本。

1. 目的与范围

本政策确立了处理 Power Integrations 机密数据 (PICD) 或连接到 Power Integrations 系统的所有供应商必须遵守的最低网络安全要求。这些要求旨在确保业务连续性，并保护 Power Integrations 供应链中的专有信息。

2. 违规通知要求

供应商必须在发现影响或可能影响 PICD 或 Power Integrations 系统的任何安全事件后，尽快且不得晚于 72 小时内通知 Power Integrations。

- **初步通知（24 小时内）**：初步事实和遏制措施。
- **详细更新（72 小时内）**：受影响范围、受影响系统、可能产生的影响及后续步骤。
- **所需信息**：发现日期/时间、事件类型、PICD 受影响状态（确认/疑似）以及主要事件联系人详细信息。

3. 数据加密与管理

供应商必须维护一套书面的加密与密钥管理政策。必须使用强效的现代加密算法保护 PICD：

- **传输中**：所有服务、API 和安全文件传输 (SFTP/FTPS/HTTPS) 均须使用 TLS 1.2 或 1.3。
- **存储中**：包含 PICD 的存储和备份必须使用 AES-256（或同等标准）。
- **密钥管理**：对加密密钥的访问必须受到限制、记录日志，并根据政策进行轮换。

4. 最低安全基准要求

供应商必须实施行业领先的管理、物理和技术防护措施。

- **身份与访问控制**：执行“最小权限”原则。
- 对于所有处理 PICD 的系统的特权访问、远程访问和面向互联网的访问，均要求进行 **多因素身份验证 (MFA)**。
- **漏洞与补丁管理**：保持例行漏洞扫描（建议每季度一次）。对于暴露在互联网上的系统，须在 72 小时内修复关键风险漏洞。
- **日志记录与监控**：安全日志至少保留 90 天，以便进行调查和审计。

修订日期：2026年1月

- **终端保护**：在所有访问 PICD 的系统上部署反恶意软件和终端检测与响应 (EDR) 控制措施。
- **人工智能 (AI)/生成式人工智能限制**：未经 Power Integrations 事先书面批准，供应商不得使用 PICD 训练 AI/ML 模型，或将 PICD 上传到公开 AI 工具中。
- **分包商问责制**：供应商在聘用分包商时仍需对合规性负责；
- 未经事先通知和批准，不得向第三方提供 PICD 访问权限。

5. 供应商确认与证明

供应商确认已收到并理解本政策，并证明已实施所需的控制措施。

A. **合规证明**
   - [ ] 已制定书面的事件响应计划。
   - [ ] 接受 72 小时违规通知期限。
   - [ ] 符合加密标准 (AES-256/TLS 1.2+)。
   - [ ] 执行 MFA 和最小权限访问。
   - [ ] 已实施漏洞扫描和及时补丁管理。
   - [ ] 已保留安全日志以备调查。

Power Integrations 事件报告联系方式：Breach-notify@power.com