

信息安全控制要求

1. 引言

美光管理层力求确保美光数据安全。

范围：

这些信息安全控制要求适用于所有处理或提供美光数据的供应商。

美光供应商（以下称为“**供应商**”）必须实施管理、物理和技术方面的保障措施，采用严格程度不亚于已知的行业实践方法（包括信息安全环境和治理方法），遵循国际标准化组织 (ISO) 27001 “信息安全、网络安全和隐私保护 - 信息安全管理系统 - 要求”的标准或其后续标准，来保护供应商可以访问、由供应商提供或为美光存储的任何归美光所有或由美光提供的有形或无形物品（简称“**IT 资产和美光数据**”），防止受到未经授权的访问、获取、披露、破坏、篡改、意外丢失、滥用或损坏。

这些信息安全控制要求的意图并非是取代供应商的标准政策和程序，而是阐明供应商必须纳入到供应商标准政策和程序中的最起码的控制措施。根据这些要求，供应商必须实施下文中进一步阐明的多个方面的控制措施。

2. 定义

“**IT 资产**”包括但不限于：计算机设备（例如笔记本电脑和台式机）、移动设备（例如移动电话/智能手机、平板电脑）、硬件、软件、操作系统、存储介质、网络资源、身份（如提供对电子邮件、在线浏览、文件传输协议和其他 IT 服务的访问权限），以及美光为开展业务而向其董事、高级职员、团队成员、承包商和其他第三方提供的计算环境（例如开发、测试、生产和备份应用环境）；

“**美光数据**”包括归美光所有的或第三方委托美光管理的知识产权以及其他机密及专有数据；

“**个人数据**”是美光数据的一部分，是指与已识别身份或可识别身份的自然人有关的任何信息；自然人是指可以直接或间接识别身份的人员，特别是提及标识（如姓名、识别码、位置数据、在线标识）或提及与其身体、生理、遗传、精神、经济、文化或社会身份有关的一个或多个特定因素时可以识别身份的人员；由适用的数据保护法律定义。

“**美光事件**”是指实际上损害或可能损害信息系统的保密性、完整性或可用性，或是损害系统处理、存储或传输的信息（美光数据），或构成违反安全政策、安全程序或合理使用政策的行为或迫在眉睫的威胁。

“**处理**”是对创建、收集、拥有、处置、处理、加工、接收、传输、存储、保留和披露美光数据的统称。

3. 信息安全政策

供应商必须管理和维持一套成文的安全政策和程序，对美光信息、资产和相关服务的接收、传输、处理、存储、控制、分发、检索、访问、展示和保护进行管理。

供应商必须通过符合 NIST 网络安全框架、ISO27001/27002 或任何后续行业认可标准或框架的信息安全政策框架，对 IT 资产实施全面保护，并明确其责任。

供应商的信息安全政策和程序至少应包含以下方面：

- a) 供应商对信息安全的承诺。
- b) 信息的分类、标记和处理，包括将美光数据与供应商或供应商其他客户的信息分开。

- c) 对计算系统、网络和消息传送工具等 IT 资产的合理使用（例如，在实施控制措施的情况下仅将其用于约定目的）。
- d) 信息安全事件管理，包括违规通知与配合以及证据收集程序。
- e) 基于主机和网络的安全控制措施，包括防病毒、入侵检测系统/入侵防御系统 (IDS/IPS)、防火墙和系统强化要求。
- f) 终端用户、管理员和系统的身份验证要求。
- g) 访问控制措施，包括远程访问和对访问权限的定期审查。
- h) 供应商生产环境的记录和监控，包括对处理或存储个人数据的 IT 资产的物理访问和逻辑访问。
- i) 为员工提供适当的隐私和信息安全培训。
- j) 端点安全，利用加密技术确保数据在静置状态下、传输过程中和使用过程中的安全。
- k) 物理安全和环境安全控制措施，目的是保护物理资产。
- l) 数据生命周期管理、记录留存，并应要求向美光提供此类做法的政策和文档。

在合理通知供应商后，美光可索取、审查和检查此类信息安全政策和程序，并要求对此类计划做出合理变更。

4. 谨慎标准

供应商承认并同意，在与美光合作期间，供应商可能会创建、接收或访问美光数据（包括个人数据）。供应商必须遵守本标准中规定的处理美光数据的条款和条件，并对供应商或控制美光数据的第三方未经授权或非法处理美光数据负责。

对于其用户和承包商或数据处理人员访问美光数据的行为和疏忽，供应商必须负责并承担责任，并且供应商必须以不亚于自身数据保护的方式来对待美光资产。鉴于上述情况，供应商同意并立约，必须做到以下几点：

- a) 严格保密和维护所有美光数据，采取适度谨慎措施，避免未经授权的访问、使用或披露。
- b) 不以违反法律的方式创建、收集、接收、访问或使用美光数据。
- c) 根据本标准的条款和条件，仅为美光数据或访问美光数据的目的而使用和披露美光数据，未经美光事先书面同意，不得出于供应商自身目的或为美光以外任何人的利益而使用、出售、出租、转让、分发或以其他方式披露或提供美光数据。
- d) 限制在 AI 聊天机器人、搜索引擎或可能导致未经授权披露的工具中使用美光数据。
- e) 未经美光事先书面同意，不得直接或间接向供应商以外的任何人披露美光数据；并以书面形式要求供应商处负责处理美光数据的所有承包商或数据处理人员遵守本文档中载明的义务。

供应商必须维护技术和网络安全风险管理计划，至少每年审查一次。供应商必须维护风险管理流程，定期甄别、评估和管理美光数据和 IT 资产的风险。

5. 个人数据保护和处理要求

- a) **美光个人数据的保密性。**对于在与美光开展业务的过程中收集的所有个人数据，供应商必须做到保密。“**个人数据**”是指单独提及时或与其他信息一起提及时能够合理地识别出特定人员身份的信息（例如姓名、联系信息、工作地点、购买记录、描述、喜好、照片、录音等）。所收集的此类信息为“**美光个人数据**”。
- b) **数据最小化原则和目的限制。**供应商对美光个人数据的收集和使用，应仅限于供应商在向美光提供商品或服务时，为履行相关权利和义务而合理需要的合法业务目的。未经美光事先书面许可，不得将美光个人数据用于其他用途。
- c) **传承隐私保护义务。**供应商应定期向其员工、承包商或处理美光个人数据的其他第三方说明对美光个人数据的保密义务，并且仅限于在为美光提供商品和服务的必要流程中收集和使用此类数据。供应商必须在合同中规定，处理美光个人数据的所有分包商或下级处理人员也必须履行这些数据保护义务。
- d) **隐私。**供应商应及时、透明地配合美光满足合法数据主体的隐私权要求。供应商应根据美光的书面指示，提供、修正或删除其记录中和数据存储库中的美光个人数据副本，但仅限于以原始形式保留此类美光个人数据的合法义务，且如若保留，保留时长仅限于法律要求的时限，之后应删除。未经美光事先书面授权，供应商不得分享或出售任何美光个人数据。
- e) **隐私事件通知和配合。**对于任何未经授权访问、收集、使用、更改、分享、复制或销毁美光个人信息的行为，供应商应及时告知美光并配合美光调查。涉及美光个人信息的事件通知必须发送至 security@micron.com。
- f) **合规证明。**供应商必须根据美光的要求及时提供充分的书面保证，证明其遵守了这些个人数据保护和处理要求。只要供应商或其代理持有美光个人数据，无论供应商目前是否在为美光提供商品或服务，这些保护美光个人数据的义务同样生效。

6. 人力资源安全

供应商必须维护多层次的人力资源安全计划。员工必须具备独特的身份识别形式（如工牌），签署保密协议，每年进行一次供应商《职业道德规范》或同等文件的审查和确认。在法律允许的情况下，员工还必须接受全面的背景调查，其中可能包括指纹、犯罪记录、信用记录、药物筛查和推荐人背景调查。

供应商必须要求全体员工完成有关妥善使用和处理机密信息与客户数据的年度信息安全培训，并且必须保留完成此类培训的员工的记录。供应商必须要求全体员工确认其理解并遵守供应商的信息安全政策。

7. 系统采购、开发和维护

供应商必须保持安全的开发方法，将安全纳入整个开发生命周期，其中包括应用程序开发政策、应用程序开发人员的安全培训以及对外 Web 应用程序的安全代码审查和渗透测试。

在系统采购、开发和维护流程中，供应商必须做到以下几点：

- a) 采取保护美光数据的机密性、完整性和可用性的方式，来开发和配置应用程序与数据库。
- b) 根据最佳安全做法（例如 Open Worldwide Application Security Project [OWASP] 十大漏洞）开发 Web 应用程序，并采取合理步骤验证 Web 应用程序的配置是否能够防止 OWASP 十大漏洞。
- c) 实施独立的生产、开发和测试环境。
- d) 使用自动扫描工具和手动分析方法，至少每年进行一次安全代码审查（包括开源审查）和渗透测试或同等测试。供应商必须确保根据成文的政策对查明的漏洞进行补救，政策中应根据风险状况来确定补救的轻重缓急；以及

e) 按照成文的程序管理源代码，程序中应限制访问权限并在部署前验证代码完整性。

8. 资产管理

供应商必须维护信息安全计划，该计划的目的是让员工了解，在从创建到处理、存储和处置的整个过程中，如何对信息和各类介质进行分类、标定、处理和处置。

供应商必须指导员工掌握妥善的信息处理方法，例如各类信息的分发、讨论、邮寄、复印、传真和存储。

供应商必须做到以下几点：

- a) 维护 IT 资产库存，管理相关资产的生命周期。确保资产仅用于商定目的。
- b) 在处理、加工和存储美光数据（包括个人数据）时，遵守行业标准和适用法规。
- c) 按照当前的行业标准（如国防部、NIST 800-88 或同等标准，或者相应的替代标准），执行对介质无害处理或安全销毁的程序。
- d) 在完成或终止供应商为美光所做的工作时，或应美光的要求，供应商必须对所有美光信息的所有副本进行无害处理和安全销毁（或应美光的要求将其归还美光），其中包括以任何电子或非电子形式提供的所有备份和存档副本，并且必须提供由供应商高级职员签署的证书，以美光接受的适当详细程度证明此类归还或销毁。

9. 访问控制

供应商必须维持合理的访问政策和控制措施（即身份和访问权限管理系统以及验证机制），确保只有经过授权的人员才能访问美光数据。必须通过正式的访问管理系统对访问请求进行跟踪和授权。访问权限的授予必须遵循最小权限和职责分离原则，并且必须仅限于有业务需求的人员。

在访问控制方面，供应商必须做到以下几点：

- a) 必须使用标识限制逻辑访问，防止供应商的其他客户查看或访问美光数据。
- b) 一经离职，或在公司内部调任到不再需要此类权限的职位后，尽快在商业上合理的时间内收回访问权限。
- c) 定期审查用户帐户及其权限，验证访问权限是否适合工作角色，并删除不再需要的访问权限。
- d) 限制执行系统管理或安全管理工作的授权员工使用特权帐户。
- e) 收集、监控和留存日志，以便跟踪对美光数据的访问。
- f) 仅将系统帐户用于系统间通信，并将其配置为防止用户进行交互式登录；以及
- g) 为远程访问 IT 资产实施安全的加密解决方案，且仅限授权人员访问。
- h) 收集、监控和留存日志，以便跟踪对美光数据的访问。

10. 加密技术

供应商必须实施符合最新版《联邦信息处理标准》(FIPS) 140 的密码政策，并将其用于保护美光数据和 IT 资产的所有密码技术。这包括行业标准算法和密钥长度、密钥生命周期管理要求以及密钥和证书核验要求。

供应商必须维护相关政策、流程和技术，对传输中和静置状态下的美光数据进行加密。这包括磁带、可移动媒体设备、笔记本电脑、网络文件传输和 Web 事务。加密术必须采用业界标准的商业级加密算法、协议和密钥强度。

供应商必须与美光合作，实施安全可靠的电子数据传输方法，来满足美光的要求。

11. 物理安全和环境安全

供应商必须维持物理安全措施，来控制 and 限制对 IT 资产的物理访问，这些 IT 资产包括全职的专业安全人员、覆盖用于处理和存储美光数据的安全和受限/关键空间的出入口的摄像头、停车区、入侵检测和警报能力、适当的访问控制系统、访客管理和日志。基础设施和环境控制措施可能包括但不限于电源、温湿度监控、消防系统、通用电源 (UPS)、符合当地法律和行业标准的应急或备用系统。

用于存储美光数据的所有数据中心必须位于美光批准的地理区域。即便供应商和美光签订的协议中有任何其他规定，但技术支持服务（包括但不限于软件开发、后台操作、质量保证和生产支持）可以在北美以外的地区进行。供应商必须保持实施相应的控制措施，且其严格程度应当不亚于美国境外业务所在地区的当地法规。

12. 运营安全

供应商必须保持实施妥善的安全运营计划，以保护美光数据和 IT 资产，且该计划必须经过测试并不断改进。在该计划中，供应商必须维护以下安全控制措施：

- a) 保护数据，防止数据丢失、恶意软件、恶意入侵或恶意下载。
- b) 及时更新反恶意软件和防病毒签名。
- c) 入侵检测和防御系统 (IDS/IPS)。
- d) 监控未经授权的访问、连接、设备和软件。
- e) 安全漏洞防御计划，包括定期扫描网络漏洞、补丁管理和根据风险的轻重缓急对已查明的安全漏洞进行修复。
- f) 收集和关联来自 IT 资产和传感器的安全事件，来检测和处理安全事件（如安全事故和事件管理 [SIEM]）。
- g) 使用标准化的强化构件实施系统和设备。
- h) 监控员工的联网情况；以及
- i) 按照经过测试的备份和恢复程序备份美光数据，以满足供应商对连续性的要求和有关恢复时间的目标，并保护备份，防止发生丢失、损坏和未经授权的访问。

13. 业务恢复能力

供应商必须保持全面的业务连续性和灾难恢复计划，其中包括技术和业务运营恢复。供应商必须将重点放在电信、系统和业务运营冗余，以及发生损失时的恢复策略上面，防止出现业务中断。业务连续性和灾难恢复计划必须遵守适用于提供服务的供应商的法律法规要求。

灾难恢复流程必须包括培训、规划和测试关键技术以及业务运营恢复，至少每年进行一次。必须开展业务影响分析，并针对不同的威胁情况制定恢复策略，涵盖场所、人员、技术或供应链的损失。供应商必须维

护在事件发生期间或之后可能执行的恢复计划，并且务必应要求与美光分享这些计划，以证明可以恢复受连续性事件影响的系统。在供应商业务连续性和灾难恢复计划的成果中，供应商的恢复时间目标（“RTO”）和恢复点目标（“RPO”）应与美光的 RTO/RPO 相一致，并作为双方服务水平协议的依据。

14. 信息安全事件管理

供应商必须维护并定期测试其成文的全面网络事件响应计划，该计划的目的是识别潜在威胁、评估风险敞口、向管理层报告风险并保护业务运营。在信息安全事件管理计划中，供应商必须采取以下行动：

- a) 评估安全事件和可疑事件。
- b) 通过控制和纾解事件，来做出应对。
- c) 确定行动方案，最大限度降低类似事件再次发生的风险；以及
- d) 根据保存证据的法律要求开展调查。
- e) 总结经验教训，提高整体上的事件管理能力。

15. 数据事故或泄露通知

如若美光数据发生丢失、毁坏、损坏、损毁、无法使用或被未经授权的个人或实体访问（如查看、复制、更改、披露或传输），供应商必须根据任何适用的合同或法律要求及时联系 security@micron.com 来告知美光。供应商必须自费恢复相应的美光数据。供应商必须根据任何适用的法律、法规或规章及时告知美光，不无故拖延，并且不得迟于知悉发生安全事故、未经授权或非法处理美光数据后 72 小时。在发生任何未经授权或非法处理美光数据后，双方必须立即配合调查事态。供应商必须配合美光处理事件，包括：

- a) 协助开展调查。
- b) 酌情向美光提供逻辑、物理和远程访问任何相关设施和操作的权限。
- c) 为采访供应商的员工、前员工、承包商、下级处理人员以及涉及此事的其他人员提供便利；以及
- d) 提供所有相关记录、日志、文件、数据报告以及为遵守所有隐私和数据保护要求而提供或美光合理要求提供的其他材料。

未经美光事先书面同意，供应商不得将任何安全事件告知任何第三方，除非法律或法规另有规定。供应商还同意，美光有权自行决定是否按照法律法规的要求或根据美光的自由裁量权向任何受影响的个人、监管机构、执法机构或其他方告知事件，包括告知的内容和告知方式；以及是否向受事件影响的个人提供任何类型的补救，包括此类补救的性质和范围。

与履行本节规定的义务相关的一切合理费用，均由供应商自理。对于供应商因作为或不作为而导致的损害，供应商还必须向美光补偿美光为应对和减轻损害而发生的合理费用，包括本节规定的所有通知和任何补救措施的费用。供应商同意维护和保存与任何安全事件相关的所有文件、记录和其他数据。此外，供应商同意在自理费用的情况下，在美光认为有必要的任何诉讼、调查或其他行动中充分配合，以保护美光在美光数据的使用、披露、保护和维护方面的权利。

16. 通信安全

供应商必须维护合理适宜的网络安全和信息传输控制措施，保障通过公共网络或无线网络传输的数据的保密性和完整性，确保各种 IT 资产受到保护，其中包括防火墙、入侵检测和防御系统、反恶意软件、代理服务和安全文件传输技术。

供应商必须：根据风险情况，对远程虚拟专用网络 (VPN) 访问和特定核心基础设施组件的管理实施多重身份验证；设计的所有网络要能保护网络完整性，并使用防火墙或同等设备分隔网络区域，仅使用授权的业务流量；每年审查一次防火墙政策。

17. 供应商关系

供应商必须维护第三方风险管理计划，该计划要纳入供应商侧采用供应商安全政策、ISO 27001 和其他行业标准做法得出的全面风险评估，来对美光数据（包括个人数据）进行处理的供应商。

美光承认供应商可能会利用云服务提供商，来提供与供应商和美光签订的协议项下规定的相关服务。供应商对处理或存储美光数据的供应商所提供的服务负责，其程度应与供应商自行提供服务的程度相当，并且必须与处理或存储美光数据的供应商签订书面协议，该协议应符合供应商的信息安全义务，并适用于此类供应商所提供的服务。

18. 安全保证和评估

应美光的要求，供应商必须每年以 ISO 27001 证书、SOC 2 Type II 报告或任何替代或同等标准报告的形式提供保证，证明已采取妥善的信息安全保障措施和控制措施。

应美光的书面要求，为确认遵守本标准以及任何适用的法律和行业标准，供应商必须及时准确地填写由美光或代表美光的第三方提供的信息安全调查问卷，问卷内容涉及供应商根据本标准处理所有美光数据和/或向美光提供服务的供应商业务做法和信息技术环境。供应商必须充分配合开展此类问询。美光应将供应商在安全问卷中提供的信息视为供应商的机密信息。

如果美光对供应商的场所、设施、系统（包括基础设施、软件、人员、程序和数据）以及据此或由此提供服务的系统组件（包括供应商的所有供应商、分包商和下级服务组织的系统组件）进行现场或远程安全评估（“安全评估”），美光必须在正常的营业时间内，在尽量不会对供应商的运营造成不便和干扰的情况下开展安全评估，且频度不得超过每年一次，并至少提前 90 天发出书面通知。供应商必须花费适当的时间，无偿参与美光的安全评估和审计。美光不得审查供应商其他客户或顾客的数据或信息、供应商的任何专有数据（可能损害用于保护供应商和供应商客户数据的控制措施的信息）或与安全评估目的无关的任何其他机密信息。此外，美光不得重新执行或观察控制措施的测试或实施。

安全评估的时长必须合理，范围由双方共同商定，美光应先查看现有的 SOC 2 II 型服务审计员报告、ISO 27001 证书或任何替代或同等的标准报告，证明已采取妥善的信息安全保障措施和控制措施，合理保证用于保护美光数据的控制措施。美光不得对供应商的网络和系统进行逻辑访问，也不得对供应商的设施和人员进行不受限制的物理访问。供应商必须提供安全人员来解决美光的合理问题。美光不得雇佣供应商的任何竞争对手（或根据供应商与美光签订的协议，不得雇佣供应商的任何重要分包商）或供应商的第三方服务审计员或 ISO 27001 审计员，来进行此类评估。美光的任何第三方代表必须执行保密协议，并遵守供应商的安全和保密要求。美光至少应采取程度不亚于美光在维护自身信息、数据和记录的预防措施，防止不当披露从供应商处收到的安全信息。未经供应商事先书面批准，美光不得向任何第三方披露从供应商处收到的任何安全信息，除非法律要求（在此情况下，美光应将要求书面通知供应商）。如果美光在安全评估过程中发现重大风险或缺陷，且双方同意需要针对该风险实施补救，美光和供应商必须立即共同商定补救计划，且供应商必须尽商业上合理的努力，对发现的任何缺陷或重大风险做出补救。