以下译文仅供参考。如果本译文与最后更新的英文版本之间存在差异、不一致或冲突（包括由于翻译延误），则以英文版本为准。

可根据以下规定进行变更。根据需要保存该版本的副本，以供内部记录使用。

# Amazon 供应商安全政策

## 最近更新日期：2024 年 9 月 11 日

**1. 范围**。供应商将遵守这些安全要求（“安全政策”）。 本安全政策不限制供应商的任何其他合同义务或法律义务。如果本安全政策与供应商和 Amazon 之间的其他协议之间存在冲突，供应商将遵守其中具有更强限制性要求的规定，以更好地保护 Amazon 信息。供应商与 Amazon 之间的其他协议中提及的“第三方安全要求”均应解释为对本安全政策的引用。

**2. 更新。**

2.1 Amazon 可能不时对本安全政策进行商业上合理的更新，更新将于本安全政策“最后更新”日期起 30 天后生效。供应商同意在更新生效后,受更新后的安全政策约束。

2.2 如果供应商希望在更新生效前收到此类更新的事先通知，可以使用本安全政策网页上提供的订阅表格订阅，以接收更新通知。供应商应确保为更新通知订阅所提供的所有供应商联系信息始终是最新和准确的。更新通知一经通过电子邮件发送，即视为供应商已收到，无论供应商是否实际收到该通知。

**3. 许可目的。**

3.1 **明确授权。**供应商仅可处理本协议项下明确授权的 Amazon 信息，且仅可将其用于提供本协议项下的产品或服务之目的（“许可目的”）。

3.2 **数据保留**。供应商应仅出于许可目的在实现许可目的所需期限内保留 Amazon 信息。

3.3 **明确限制**。供应商不得以其他方式：(a) 处理任何 Amazon 信息，即使是匿名处理；(b) 传输、出租、交换、交易、出售、出借、租赁或以其他方式向任何第三方分发或提供任何 Amazon 信息，即使是匿名处理；或 (c) 使用 Amazon 信息开发、训练或改进任何人工智能 (AI) 或机器学习 (ML) 模型，即使是匿名处理。

**4. 最低安全要求。**供应商应维持符合行业最佳实践的物理、管理和技术保障措施（包括国际标准化组织（“ISO”）27001 和 27002 标准、美国国家标准与技术研究院（“NIST”）网络安全框架或其他类似标准）。供应商维持的保障措施应包括下文第 4.1 – 4.18 条中所述的最低要求。

4.1 **书面信息安全计划**。供应商应制定书面信息安全计划，该计划应：(a) 包括符合本安全政策规定的适当政策、程序和标准；(b) 指定一名负责沟通和管理安全问题（包括安全事件）的安全联系人；(c) 至少每年审查一次，并根据需要更新；以及 (d) 适用于供应商人员。供应商应监督和执行其信息安全计划，并处理违规行为。

4.2 **补丁管理**。供应商应保持更新涵盖信息系统，安装最新升级、更新、错误修复和新版本。供应商应对无法用补丁修复的资产实施缓解措施。

4.3 **日志记录。** 供应商应收集、管理和保留审计、事件和安全日志，包括：(a) 有关出于许可目的向供应商提供的 Amazon 账户或凭证的所有使用情况（授权和未经授权）的日志数据，以及 (b) 任何冒

以下译文仅供参考。如果本译文与最后更新的英文版本之间存在差异、不一致或冲突（包括由于翻译延误），则以英文版本为准。

充或企图冒充有权访问 Amazon 信息或涵盖信息系统的 Amazon 人员或供应商人员的日志数据。此类日志应包含足够的数据，以识别每个记录事件的以下信息：(i) 发起该事件的人员或账户，(ii) 事件发生时间，以及 (iii) 受影响的系统、数据或其他资源。供应商应定期分析此类日志，以协助检测、调查未经授权的活动并从中恢复。

4.4 **恶意软件防护**。 供应商应：(a) 在所有涵盖信息系统中部署反恶意软件或同等安全控制措施；(b) 维护反恶意软件或同等安全控制措施的更新、特征码和配置；以及 (c) 配置系统以检测、防止和纠正恶意或未经授权代码的安装、传播和执行。

4.5 **风险管理计划**。 供应商应制定书面信息安全风险管理计划，该计划定义了风险分析、风险处理、风险接受和例外情况的流程。

4.6 **安全意识培训**。供应商将在人员入职时和之后至少每年为人员提供信息安全和数据隐私培训。供应商还应确保人员及时了解供应商安全和数据隐私政策的更新情况。

4.7 **数据清单**。 供应商将记录并维护有关以下方面的信息：(a) 其正在处理的 Amazon 信息，以及 (b) 该 Amazon 信息的处理方式和处理地点（例如，在最新的架构图中呈现）。应 Amazon 的要求，供应商应向 Amazon 提供此信息。

4.8 **安全测试。**

4.8.1 供应商应进行年度测试，以确保其符合本安全政策的要求。

4.8.2 供应商应至少每年对供应商的安全防御进行渗透测试。渗透测试应包括：(a) 从供应商网络内部和外部进行测试，(b) 社会工程学测试（例如，网络钓鱼模拟），以及 (c) 无线网络安全测试。供应商应将已识别的漏洞作为其漏洞管理计划的一部分加以处理。应 Amazon 的要求，供应商将向 Amazon 提供此类渗透测试和漏洞修复的结果。

4.9 **网络安全**。 供应商应限制未经授权的网络访问（尤其是来自外部互联网的访问），来保护涵盖信息系统。供应商应维护和配置防火墙或其他同等安全控制措施，以保护系统免受未经授权的访问，并至少每年审查一次防火墙规则集，以确保所有规则都存在有效、有文件记录的业务案例。

4.10 **适当环境**。供应商应仅在适合其目的的环境中处理 Amazon 信息，除非本协议允许，否则不得在测试环境中处理 Amazon 信息。

4.11 **加密**。供应商应根据行业最佳实践，对所有静态的 Amazon 信息和通过外部网络传输的 Amazon 信息进行加密。如果 Amazon 信息在内部供应商网络上传输，应通过符合行业最佳实践的加密协议传输。供应商应根据行业最佳实践来管理和保护加密密钥。

4.12 **管理特权的受控使用**。供应商应根据 NIST 网络安全框架或 ISO 27002 对管理职能进行管理。供应商应至少将管理账户与标准账户分开，并将管理账户的职能限制在履行管理职能所必需的范围内。供应商应以可追溯到单个用户的方式记录所有管理账户操作。授予标准账户的管理功能应基于最小权限原则，并以可追溯到单个用户的方式进行记录。

4.13 **访问控制。**

4.13.1 **唯一 ID**。供应商应向有权访问 Amazon 信息或涵盖信息系统的人员分配个人唯一 ID，包括具有管理访问权限的账户。

以下译文仅供参考。如果本译文与最后更新的英文版本之间存在差异、不一致或冲突（包括由于翻译延误），则以英文版本为准。

4.13.2 **仅“须知”。** 供应商应仅允许出于许可目的“须知”的人员访问 Amazon 信息和涵盖信息系统。

4.13.3 **用户访问权限审查。** 供应商应至少每 90 天审查一次有权访问 Amazon 信息和涵盖信息系统的人员和服务清单，并删除不再需要访问权限的账户。

4.13.4 **单点登录 (SSO)**。任何需要 Amazon 人员进行身份验证的供应商服务，必须与 Amazon 身份提供商（例如 Amazon Federate）集成以提供此类身份验证。此类服务不得使用供应商提供的或供应商管理的凭证进行身份验证。

4.14 **密码管理。**

4.14.1 **强密码。** 供应商不得在任何涵盖信息系统上使用制造商提供的默认系统密码和其他安全参数。供应商应根据 NIST SP 800-63B 中所述的最佳实践，规定并确保在所有涵盖信息系统上使用系统强制的“强密码”。供应商应要求对所有密码和访问凭证保密，不得与他人共享。

4.14.2 **锁定。**账户密码连续错误超过十 (10) 次时，供应商应通过禁用可访问 Amazon 信息或涵盖信息系统的账户，来维护和强制执行“账户锁定”。

4.15 **远程访问；多因素身份验证**。供应商应实施多因素身份验证（即，要求至少两个因素对用户进行身份验证），以远程访问任何供应商网络、系统、应用程序或其他资产。

4.16 **“批量”访问。** 就本条而言，“批量”访问是指通过数据库查询、报告生成或任何其他大量数据传输来访问数据。

4.16.1 除非协议中明确规定或 Amazon 以书面形式另有规定，否则供应商自身不得，也不得允许他人“批量”访问 Amazon 信息，无论 Amazon 信息是在 Amazon 或供应商控制的数据库中，还是以任何其他方式存储，包括存储在基于文件的档案（如平面文件）中。

4.16.2 如果 Amazon 授权“批量”访问，则供应商应：(a) 将此类访问限于仅“须知”的指定人员，以及 (b) 根据第 4.3 条的要求，需要明确授权和记录此类访问。应 Amazon 的要求并按照第 10 条“安全审查”或第 11 条“安全事件”的规定进行协调后，供应商应向 Amazon 提供本条中提及的“批量”访问的所有日志。

4.17 **数据隔离**。供应商应始终在物理或逻辑上将 Amazon 信息与供应商和任何第三方的信息隔离。如果无法隔离，供应商应出于记录、删除和事件响应目的，确保 Amazon 信息可与其他信息区分开来。

4.18 **供应商人员安全**。

4.18.1 供应商应采取一切合理的预防措施，确保被授予访问 Amazon 信息权限的人员对信息保密，并仅将其用于许可目的。这些预防措施必须包括通过保密协议或供应商政策而实施保密要求。

4.18.2 对于 (a) 不再需要访问 Amazon 信息或 (b) 不再符合供应商人员资格条件的任何人员，供应商应在 24 小时内终止其访问 Amazon 信息和涵盖信息系统的权限。如果任何人员在 (a) 或 (b) 情况发生超过 24 小时后仍保留对 Amazon 信息或涵盖信息系统的访问权限，供应商应在获悉该情况后的 24 小时内发送电子邮件至 security@amazon.com 通知 Amazon 该持续访问的相关情况。

以下译文仅供参考。如果本译文与最后更新的英文版本之间存在差异、不一致或冲突（包括由于翻译延误），则以英文版本为准。

**5. 支付安全要求。**如果供应商有权访问或即将处理支付卡持有人数据，供应商应遵守最新版本的《支付卡行业数据安全标准》(PCI DSS)。

**6. 分包商。**

6.1 未经 Amazon 事先书面同意，供应商不得将其在本安全政策下的任何义务分包或委托给任何第三方（统称为“分包商”）。即使存在任何分包或委托或者规定了任何分包或委托条款，供应商仍应负责全面履行其在本安全政策项下的义务。本安全政策的条款和条件对供应商的分包商及其人员均具有约束力。

6.2 如果供应商使用任何分包商涵盖信息系统，供应商应对分包商涵盖信息系统及其安全控制措施进行安全审查，并应 Amazon 的要求，按照 Amazon 要求的格式（例如，《鉴证业务准则公告第 16 号》(SSAE 16)）向 Amazon 提供关于分包商涵盖信息系统安全控制措施的定期报告。

**7. 访问 AMAZON 管理的信息系统。**Amazon 可授予供应商仅出于许可目的，通过门户网站或其他非公共网站或外联网（统称“Amazon 管理的信息系统”）处理 Amazon 信息的权利。如果 Amazon 允许供应商使用 Amazon 管理的信息系统处理任何 Amazon 信息，供应商及其人员必须遵守以下要求：

7.1 **账户**。供应商应确保供应商人员仅使用 Amazon 为每个人指定的 Amazon 管理的信息系统账户，并要求供应商人员对其访问凭证保密，不得共享。

7.2 **系统**。供应商及其人员应仅通过以下计算或处理系统或应用程序来使用 Amazon 管理的信息系统：(a) 运行由供应商管理并使用全盘加密的操作系统，以及 (b) 满足第 4.2 条（补丁管理）、第 4.4 条（恶意软件防护）和第 4.9 条（网络安全）的要求。

7.3 **限制**。 除非事先获得 Amazon 的书面批准，否则供应商及其人员不得从任何 Amazon 管理的信息系统下载、镜像任何 Amazon 信息或将其永久存储在任何介质上。

7.4 **账户终止**。对于 (a) 不再需要访问 Amazon 管理的信息系统或 (b) 不再符合供应商人员资格条件（例如，从供应商离职的人员）的任何人员，供应商应立即（在 24 小时内）终止其访问 Amazon 管理的信息系统的访问权限，或通知 Amazon 取消该访问权限。

**8. Amazon 域名 或 URL**。 供应商提供给 Amazon 专用的任何域名或 URL，在本协议终止后至少 5 年内，供应商不得向任何第三方发布或供任何第三方重复使用。

**9. 数据归还和删除；介质取证销毁。**

9.1 **数据归还和删除**。如果 Amazon 提出要求，供应商应立即（最迟不超过 72 小时）根据 Amazon 的归还和/或删除通知，向 Amazon 归还所有 Amazon 信息并以安全的方式将其永久删除。供应商还应在许可目的完成或者本协议终止或到期（以较早者为准）后 30 天内，以安全的方式永久删除 Amazon 信息的所有实时（可在线或网络访问）实例。如果 Amazon 有要求，供应商应以书面形式证明所有 Amazon 信息均已删除。为明确起见，本条不适用于第 9.3 条所述的存档副本。

9.2 数据清理。为清除相关类型的设备，供应商应根据 2014 年 12 月 18 日 的 NIST SP 800-88 修订版 1《介质清理指南》附录 A 中包含的最低清理建议来删除所有 Amazon 信息。若 NIST SP 800-88 中没有关于相关类型设备的指导，供应商应以下列方式之一销毁包含 Amazon 信息的设备：(a) 按照 NIST SP 800-88 的规定进行清除，(b) 按照 NIST SP 800-88 的规定进行销毁，或 (c) 根据 Amazon 信息的分类和敏感性，按照 Amazon 可能要求的其他标准进行处理。

以下译文仅供参考。如果本译文与最后更新的英文版本之间存在差异、不一致或冲突（包括由于翻译延误），则以英文版本为准。

9.3 存档副本。 如果法律要求供应商保留 Amazon 信息的存档副本，供应商不得将存档的 Amazon 信息用于任何其他目的，并且供应商
仍受其在本安全政策下所有义务的约束。任何存档的 Amazon 信息必须加密，并存储在托管或存储加密 Amazon 信息的涵盖信息系统无法访问其加密密钥的位置。任何离线或“冷”（即，不可即时或交互使用）的备份，都必须存储在物理安全设施中。

9.4 **介质取证销毁**。在处置包含或曾经包含 Amazon 信息的任何硬件、软件或任何其他介质之前，供应商应根据 NIST SP 800-88 附录 A 对硬件、软件或其他介质进行完全取证销毁。该销毁要求不适用于供应商没有物理访问或控制的存储介质。在这种情况下，供应商应确保按照行业最佳实践，在不再需要 Amazon 信息时将其安全删除。

> 9.4.1 除非供应商事先获得 Amazon 的明确书面同意，否则供应商不得出售、转售、捐赠、翻新或以其他方式转让任何曾包含 Amazon 信息的硬件、软件或其他介质，除非其已根据本条规定进行了取证销毁。

10. **安全审查**。 应 Amazon 的要求，供应商应：(a) 完成 Amazon 风险评估，(b) 提供 Amazon 要求的证据，以验证供应商是否遵守本安全政策，(c) 允许 Amazon 或其指定的第三方对供应商遵守本安全政策的情况进行审查，和/或 (d) 以开放网络安全框架 (OCSF) 格式向 Amazon 提供第 4.3 条中提及的所有日志。如果供应商要求亲自或以现场检查的方式审查任何证据，而不是将此类证据远程提供给 Amazon 以供审查，则供应商应承担与此类现场检查相关的差旅费和其他费用。如果任何评估或审查发现任何问题，供应商应自行承担全部费用，立即采取所有必要的合理措施，在双方商定的时限内以令 Amazon 合理满意的方式纠正这些问题。

11. **安全事件。**

11.1 **安全事件通知**。一旦供应商知晓或合理认为存在未经授权访问、收集、获取、使用、传输、披露、损坏或丢失 Amazon 信息或涵盖信息系统（“安全事件”）的情况，供应商应尽快通知 Amazon，不得迟于知晓后的 24 小时。供应商应将安全事件通知发送至 security@amazon.com。

11.2 **事件响应计划**。供应商应制定书面的事件响应计划，并根据要求向 Amazon 提供该计划的副本。供应商应根据其书面事件响应计划和行业最佳实践，及时补救每个安全事件。供应商应至少每年审查、测试和（如需要）更新计划。

11.3 **与 Amazon 合作**。供应商应 (a) 协助 Amazon 调查安全事件；(b) 为与安全事件或响应相关的人员和其他相关方的访谈提供便利；(c) 保留供应商对安全事件调查和响应的书面详细记录；以及 (d) 向 Amazon 提供 Amazon 要求的所有相关记录、日志、文件、数据报告、取证报告、调查报告和其他材料。

11.4 **第三方通知**。除非法律另有规定，否则供应商应在以下情况之前事先获得 Amazon 的书面同意：(a) 将任何安全事件通知任何第三方（包括任何监管机构或客户）；或 (b) 在有关任何安全事件的任何通知或公开声明中提及 Amazon。除非法律另有规定，否则 Amazon 将有权决定是否向任何第三方提供安全事件通知，以及此类通知的形式、时间和内容。

12. **法律程序通知**。法律程序通知。 除法律禁止的情况外，如果根据法律程序或其他适用法律要求提供 Amazon 信息，供应商应充分通知 Amazon，以便 Amazon 寻求保护令或其他适当的救济。

以下译文仅供参考。如果本译文与最后更新的英文版本之间存在差异、不一致或冲突（包括由于翻译延误），则以英文版本为准。

13. **定义**。

13.1 “**协议**”是指引用本安全政策的任何协议。

13.2 “**Amazon**”是指 Amazon.com, Inc. 及其关联方。

13.3 “**Amazon 信息**”是指：(a) 所有 Amazon 机密信息（定义见双方之间的任何其他协议）；(b) 供应商或其关联方从 Amazon 或代表 Amazon 获取、访问、收集、接收、存储或维护的，或者与本协议相关的任何形式的所有数据、记录、文件、内容或信息；和 (c) 源自 (a) 或 (b) 的信息，即使是匿名的。

13.4 “**匿名**”是指确保任何数据或信息（包括 Amazon 信息）的处理方式或形式不会识别、不允许识别、不会以其他方式关联 Amazon 或任何用户、设备标识符、来源、产品、服务、场景或其品牌。

13.5 “**涵盖信息系统**”是指供应商用于处理 Amazon 信息的任何系统。

13.6 “**人员**”是指供应商或分包商的员工、代理人、分包商及其系统和网络资源的其他授权用户。

13.7 “**处理**”是指对数据进行任何操作，例如访问、使用、收集、接收、存储、更改、传输、传播或以其他方式提供、删除或销毁。

13.8 “**供应商**”是指协议中定义的每个供应商、供货商或承包商以及受协议约束的任何其他提供商。