以下译文仅供参考。如果本译文与英文版本之间存在差异、不一致或冲突（尤其是在译文延迟的情况下），以英文版本为准。

供应商安全政策

上次更新时间：2022 年 1 月 28 日

1. 范围；定义。

1.1 安全政策。供应商应全面遵守本政策（“**安全政策**”）中规定的亚马逊信息安全要求。本安全政策适用于供应商履行协议、对亚马逊信息的所有访问、收集、使用、存储、传输、披露、销毁或删除，以及与亚马逊信息相关的安全事件。本安全政策不限制供应商的任何其他义务，包括与亚马逊签订的任何其他协议项下或者适用于供应商、供应商在与亚马逊签订的其他任何协议项下的履约、亚马逊信息、许可目的的任何其他法律项下的义务。如果本安全政策与双方之间的任何保密协议或适用于双方的任何其他协议冲突，供应商应立即将冲突通知亚马逊，并遵守对亚马逊信息保护性更高的要求，除非明确规定保护性较低的要求优先于保护性较高的要求（可由亚马逊指定）。亚马逊可自行决定不时更改本安全政策，但是如果此类更改在商业上不合理，亚马逊将根据要求举行会议并商定适当的额外费用。

1.2 定义。

1.2.1 “**汇总**”是指将亚马逊信息与供应商或任何第三方的任何数据或信息合并或存储在一起。

1.2.2 “**协议**”是指引用本安全政策的任何协议。

1.2.3 “**亚马逊**”是指亚马逊公司及其关联公司。

1.2.4 “**匿名**”是指确保任何数据或信息（包括亚马逊信息）的使用、收集、存储、传输或转换方式或形式不会识别、不允许识别、不会以其他方式关联亚马逊或任何用户、设备标识符、来源、产品、服务、场景或其品牌。

1.2.5 “**亚马逊信息**”是指（单独和集体的）：(a) 所有亚马逊机密信息（定义见双方之间的保密协议或任何其他协议）；(b) 供应商或其关联方从亚马逊或代表亚马逊获取、访问、收集、接收、存储或维护的或者与本安全政策、服务、双方履行或行使协议项下权利或与之相关的所有其他数据、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。

1.2.6 “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。

1.3 许可目的。供应商仅可出于提供协议项下产品或服务之目的按照本安全政策项下授予的许可（如有）（“**许可目的**”）访问、收集、使用、存储和传输协议项下明确授权的亚马逊信息。除协议明确授权外，供应商不得访问、收集、使用、存储或传输任何亚马逊信息，也不得汇总亚马逊信息，即使是匿名的。除非事先获得亚马逊的明确书面同意，否则供应商不得 (a) 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亚马逊信息，或 (b) 将亚马逊信息与任何其他信息或数据（即使是匿名的）汇总在一起。

2. 亚马逊安全政策。

2.1 基本安全要求。供应商应根据当前最佳行业标准以及亚马逊根据亚马逊信息分类和敏感性规定的其他要求，采取物理、管理和技术保护措施以及其他安全措施：(a) 维护供应商访问、收集、使用、存储或传输的亚马逊信息的安全性和保密性，以及 (b) 保护此类信息免遭已知或合理预期的安全和完整性威胁或危害、意外丢失、篡改和披露以及所有其他非法形式的处理。对于供应商用于处理亚马逊信息或可访问亚马逊信息的任何系统（“**亚马逊信息系统**”），供应商应遵守（包括但不限于）以下要求：

2.1.1 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），保护任何亚马逊信息系统。供应商应安装并维护有效的网络安全解决方案（如防火墙），始终保护亚马逊信息。

2.1.2 更新。如美国国家标准与技术研究院（"NIST"）特别出版物（"SP"）800-40 第 3 版所述，供应商应及时对亚马逊信息系统进行升级、更新、错误修复和新版本应用以及任何其他必要修改，以确保亚马逊信息的安全性。

2.1.3 反恶意软件。供应商应始终使用反恶意软件或同等安全控制措施，以降低恶意软件的感染和传播风险。使用时，供应商应确保反恶意软件为最新版本。

2.1.4 加密。供应商应根据行业最佳实践对静态数据和通过开放网络发送的数据进行加密。

2.1.5 测试。供应商应定期测试其安全系统和流程，以确保其符合本安全政策或供应商与亚马逊商定的最新安全政策的要求。如果根据第 1.1 条对本安全政策进行了变更，则就本条而言，在供应商与亚马逊达成一致（电子邮件即可）之后这些变更才会生效。

2.1.6 访问控制。供应商应确保亚马逊信息的安全，包括遵守以下要求：

2.1.6.1 供应商将为每个能够通过计算机访问亚马逊信息或亚马逊信息系统的人员分配一个唯一的 ID。

2.1.6.2 供应商应仅允许出于许可目的"须知"的人员访问亚马逊信息。

2.1.6.3 供应商应定期审查有权访问亚马逊信息的人员和服务清单，并删除不再需要访问亚马逊信息系统的帐户。该审查必须至少每 90 天进行一次。

2.1.6.4 供应商不得在任何亚马逊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，规定并确保在所有亚马逊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。

2.1.6.5 帐户密码连续错误超过十 (10) 次时，供应商应通过禁用可访问亚马逊信息或亚马逊信息系统的帐户来维护和强制执行"帐户锁定"。

2.1.6.6 除非亚马逊以书面形式明确授权，否则供应商应始终（包括存储、处理或传输过程中）确保亚马逊信息在物理上或逻辑上与供应商和任何第三方信息隔离。

2.1.6.7 如果亚马逊书面要求采取额外的物理访问控制措施，供应商应实施并使用这些措施。

2.1.6.8 应亚马逊的合理要求，供应商应向亚马逊提供 (a) 有关出于许可目的提供给供应商之亚马逊帐户或凭证（如社交媒体帐户凭证）的所有使用情况（授权和未授权）的日志数据，以及 (b) 有关任何假冒或试图假冒有权访问亚马逊信息的亚马逊人员或供应商人员的详细日志数据。

2.1.6.9 供应商应定期审查访问日志，确定是否存在恶意行为或未经授权访问的迹象。

2.1.7 供应商政策。供应商应针对员工、分包商、代理商和供应商制定并执行符合本安全政策中所述标准的信息和网络安全政策，包括检测和记录政策违规的方法。应亚马逊的要求，如果供应商或亚马逊有理由怀疑违反供应商信息和网络安全政策的行为可能构成安全事件（定义见下文），供应商应向亚马逊提供有关违反供应商信息和网络安全政策的信息。

2.1.8 分包。未经亚马逊事先书面同意，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分包商或受托人（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和人员均具有约束力。供应商应 (a) 确保其分包商和人员遵守本安全政策，并且 (b) 对其分包商和人员的所有作为、不作为、过失和不当行为负责。

2.1.9 远程访问。供应商应确保对亚马逊信息系统的任何访问均需进行多因素身份验证（例如，需要至少两个单独的因素来确认用户身份）。

2.1.10 "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。除非亚马逊以书面形式明确授权，否则供应商自身不得，也不得允许他人"批量"访问亚马逊信息，无论亚马逊信息是在供应商或亚马逊控制的数据库中，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）中等。具体而言，本条禁止对亚马逊信息的任何访问，但出于许可目的而需访问个别记录除外。供应商应保留尝试或成功"批量"访问亚马逊信息的详细日志数据，并提供这些日志的报告，作为第 2.5 条（安全审查）规定的供应商义务的一部分。如果亚马逊向供应商提供"批量"访问亚马逊信息的书面授权，供应商应 (a) 将此类访问仅限于"须知"的指定员工，以及 (b) 使用限制访问的工具，并对所有访问明确授权且进行记录。

2.1.11 供应商人员。亚马逊可将供应商人员签署并向亚马逊交付个人保密协议作为访问亚马逊信息的条件，其形式由亚马逊规定。如果亚马逊有要求，供应商人员应签署个人保密协议。供应商应获得并向亚马逊交付有权访问亚马逊信息的供应商人员签署的个人保密协议（在向供应商人员授予访问权限或提供信息之前）。供应商还应保留一份曾在亚马逊信息系统上访问或接收亚马逊信息的所有供应商人员的名单，并应要求及时向亚马逊提供该名单。对于 (a) 不再需要访问亚马逊信息或 (b) 不再符合供应商人员资格条件的任何供应商人员（例如，从供应商离职的人员），供应商应立即（在 24 小时内）终止其访问亚马逊信息和亚马逊信息系统的权限。如果任何此类人员被授权访问亚马逊信息系统上的亚马逊信息，供应商也应在 24 小时内通知亚马逊。

2.2 访问亚马逊外联网和供应商门户。亚马逊可出于许可目的，授权供应商通过网站门户、其他非公开网站、亚马逊或第三方网站或系统上的外联网服务（均称为"**外联网**"）访问亚马逊信息。如果亚马逊允许供应商通过外联网访问任何亚马逊信息，供应商必须遵守以下要求：

2.2.1 许可目的。供应商和供应商人员只能出于许可目的访问外联网以及通过外联网访问、收集、使用、查看、检索、下载或存储亚马逊信息。

2.2.2 帐户。供应商应确保供应商人员仅使用亚马逊为每个人指定的外联网帐户，并要求供应商人员对其访问凭证保密。

2.2.3 系统。供应商只能通过计算或处理系统或者运行由供应商管理的操作系统的应用程序访问外联网，包括：(a) 符合第 2.1.1 条（网络安全）规定的系统网络防火墙；(b) 按照第 2.1.2 条（更新）进行的补丁集中管理；(c) 符合第 2.1.3 条（反恶意软件）规定且与操作系统兼容的反恶意软件；(d) 便携式设备的全磁盘加密。

2.2.4 限制。除非事先得到亚马逊的书面批准，否则供应商不得从任何外联网下载、制作镜像、永久存储任何亚马逊信息到任何介质中，包括任何机器、设备或服务器。

2.2.5 帐户终止。如果有权访问任何外联网的任何供应商人员 (a) 不再需要访问亚马逊信息或 (b) 不再符合供应商人员的资格条件（例如，该人员从供应商离职），供应商应终止其帐户，并在 24 小时内通知亚马逊。

2.2.6 第三方系统。

2.2.6.1 在使用存储或可能以其他方式访问亚马逊信息的任何第三方系统之前，供应商应事先通知亚马逊并获得亚马逊书面批准，除非 (a) 数据已根据本安全政策进行加密，和 (b) 第三方系统无法访问解密密钥或数据的未加密"纯文本"版本。亚马逊有权在批准前要求对第三方系统进行亚马逊安全审查（根据第 2.5 条（安全审查））。

2.2.6.2 如果供应商使用存储了未加密亚马逊信息或以其他方式可访问未加密亚马逊信息的任何第三方系统，供应商应对第三方系统及其安全控制措施进行安全审查，并以亚马逊要求的格式向亚马逊提供有关第三方系统安全控制措施的定期报告（例如，SAS 70 或其后续报告，或亚马逊批准的其他公认行业标准报告）。

2.3 数据保留和销毁。

2.3.1 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亚马逊信息。

2.3.2 归还或删除。如果亚马逊提出要求，供应商应立即（但最迟不超过 72 小时）根据亚马逊的归还和/或删除通知，向亚马逊归还所有亚马逊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安全政策终止或到期（以较早者为准）后 30 天内，以安全的方式永久删除亚马逊信息的所有实时（可在线或网络访问）实例。如果亚马逊有要求，供应商应以书面形式证明所有亚马逊信息均已销毁。为明确起见，本条不适用于第 2.3.3 条所述的存档副本。

2.3.3 存档副本。如果法律要求供应商出于税务或类似监管目的保留亚马逊信息的存档副本，则存档的亚马逊信息必须通过下列方式之一存储：

2.3.3.1 以"冷"或离线（即，不可即时或交互使用）备份的形式存储在物理安全设施中；或

2.3.3.2 加密，且托管或存储加密文件的系统无法访问用于加密的密钥副本。

2.3.4 恢复。如果供应商出于灾难恢复目的执行"恢复"（即备份恢复），供应商应制定并维护一个流程，以确保在恢复后 24 小时内根据本第 2.3 条重新删除或通过恢复数据而覆盖根据协议或本安全政策或与亚马逊签订的任何其他协议需要删除的所有亚马逊信息。如果供应商出于任何目的执行恢复，未经亚马逊事先书面批准，不得将亚马逊信息恢复到任何第三方系统或网络。亚马逊有权在允许将任何亚马逊信息恢复到任何第三方系统或网络之前要求对第三方系统或网络进行亚马逊安全审查（根据第 2.5 条（安全审查））。

2.3.5 数据清理标准。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》（详见 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf）附录 A 中包含的最低清理建议来删除所有亚马逊信息。如果 NIST SP 800-88 附录 A 中未提供相关指南，包含亚马逊信息的设备应通过以下方式之一销毁：(a) 在 10,000+ 高斯的电磁通量场中对磁介质进行消磁，(b) 粉碎或机械分解，使颗粒小于 2x2 mm，或 (c) 亚马逊根据亚马逊信息的分类和敏感性可能要求的其他标准。

2.4 取证销毁。在（以任何方式）处置包含或在任何时候包含过亚马逊信息的任何硬件、软件或任何其他介质之前，供应商应对硬件、软件或其他介质进行彻底的取证销毁，确保无法以任何形式恢复亚马逊信息。供应商应根据 NIST SP 800-88 附录 A 中包含的最低清理建议进行取证销毁，以销毁相关类型的设备。

2.4.1 供应商不得出售、转售、捐赠、翻新或以其他方式转让（包括出售或转让任何此类硬件、软件或其他介质，与供应商业务清算有关的任何处置，或任何其他处置）包含亚马逊信息并且尚未由供应商按照第 2.4 条的要求进行取证销毁的任何硬件、软件或其他介质。

2.5 安全审查。

2.5.1 亚马逊有权定期要求供应商参与亚马逊风险评估。

2.5.2 证明。根据亚马逊的书面要求，供应商应以书面形式向亚马逊证明，在风险评估过程中提供的信息符合供应商和亚马逊最后商定的本安全政策。如果根据第 1.1 条对本安全政策进行了变更，则就本条而言，在供应商与亚马逊达成一致（电子邮件即可）之后这些变更才会生效。

2.5.3 其他审查。亚马逊有权定期审查亚马逊信息系统的安全性，但每年最多一次，除非 (a) 在日历年内发现先前的重大缺陷，或 (b) 政府机构或其他监管机构要求亚马逊进行此类审查。供应商应予以配合，并在合理时间内（但应在亚马逊提出要求之日起 20 个日历日内）向亚马逊提供所有所需信息。

2.5.4 纠正。如果安全审查发现任何缺陷，供应商应自费采取所有必要的合理措施，在商定的时间内纠正这些缺陷。

2.6 安全事件。

2.6.1 供应商应尽快（但不得晚于获悉后 24 小时）将任何实际或可疑的未经授权访问、收集、获取、使用、传输、披露、损坏或丢失亚马逊信息或任何亚马逊信息系统数据泄露事件（"**安全事件**"）通知亚马逊。供应商应及时纠正每一起安全事件，并向亚马逊提供有关供应商对每起安全事件进行内部调查的书面详细信息。在适用法律允许的情况下，供应商同意不代表亚马逊通知任何监管机构或客户，除非亚马逊以书面形式明确要求供应商通知任何监管机构或客户，并且亚马逊保留在向任何一方发送通知之前审查和批准任何

通知的形式和内容的权利。供应商应配合亚马逊并与其共同制定和执行旨在纠正所有已确认安全事件的计划。

2.6.2 在适用法律允许的范围内，如果供应商收到政府机构要求其提供包含任何亚马逊信息之数据的要求或命令（如传票、法院命令或搜查令），供应商应向亚马逊提供充分通知，以便亚马逊寻求保护令或其他适当的救济。

2.7 一般条款。亚马逊保留作出本安全政策项下所有相关决定的自行决定权。“包括”或“例如”之后的任何示例列举是说明性的，并非详尽无遗。除非亚马逊另有规定，否则本安全政策项下提及的所有安全要求标准均指规定的标准及其各自的后续版本或等效版本（因可能进行更新）。