上次修订日期：2018 年 3 月 1 日

Citrix 服务安全附件

本 Citrix 服务安全附件（下称“附件”）描述了针对 Citrix 许可证、订阅或服务协议下的 Citrix Cloud 服务、技术支持服务或咨询服务采取的技术和组织安全控制措施。本附件通过引用纳入此类服务协议（下称“协议”）。
本附件不适用于 Beta 或 Lab/Tech Preview 服务，包括 Citrix Cloud Labs。
本附件使用的术语采用本协议规定的或本附件（包括以下第 7 条“定义”）所述的含义。

第 1 条 Citrix 安全控制措施

本条款描述了 Citrix 为保护服务安全而采取的物理、逻辑和管理控制措施以及客户应承担的相关安全义务。Citrix 的服务安全计划遵循 ISO/IEC 27002 标准。

第 1.A 条规定的控制措施适用于所有服务。第 1.B 条规定的附加控制措施适用于所有公开发布的 Citrix Cloud Service（以下统称“云服务”）。

Citrix 保留修改第 1 条规定的控制措施的权利，但前提是，在客户已付款的服务期限内采取的控制措施应始终为客户内容提供至少与此类期限生效之日在第 1 条中规定的此类控制措施同等的保护。

1.A. 企业安全控制措施 – 所有服务

领域	控制措施
安全计划管理	**安全所有权**。Citrix 已指派一名或多名安全管理人员，负责协调和监控服务的安全控制措施。 **安全角色和责任**。有权访问客户内容的 Citrix 员工应履行保密义务。 **服务安全策略。**Citrix 已制定全面的全球安全框架 (GSF)，该框架提供了经 Citrix 执行管理层认可和批准的总体安全原则。这些策略清晰简明地描述了相关安全要求。这些标准定义了满足这些策略要求所需采取的流程或方法。GSF 安全计划会定期进行审查和评估。Citrix 会留存一份 GSF 计划摘要，必要时会提供给客户。 **产品风险管理。** Citrix 将对与服务相关的关键风险领域进行评估，包括隐私风险评估、开放源审查和导出控制分析等，此处仅为列举说明，具体依实际情况进行。
资产管理	**资产清单**。Citrix 会留存一份用于执行服务的 Citrix 托管设备（下称“资产”）的清单。经认可的系统所有者负责在必要时维护和更新此清单。

领域	控制措施
	资产和数据处理 Citrix 将对客户内容进行标识和分类，以确保访问受到适当限制。 Citrix 将对客户内容的打印以及包含客户内容的打印材料的处理实施限制措施。 Citrix 员工需获得授权方可将客户内容存储在便携式设备上、远程访问客户内容或在 Citrix 或其服务提供商管理的设施之外处理客户内容。
访问管理	**访问策略。** Citrix 会留存一份有关有权访问客户内容的个人的安全权限的记录，并遵循最低权限原则。 **访问授权** Citrix 会留存一份有权访问包含客户内容的 Citrix 系统的人员的记录，并对此记录进行更新。 如需重新授予对系统的访问权限，需经管理层审查和批准。 Citrix 将对用户帐户进行定期审查，并为关键系统分配相应权限。 Citrix 将对那些可授予、变更或取消经授权的数据和资源访问权限的人员进行认证。 Citrix 确保，如包含客户内容的系统可供多人访问，此类个人需具有独立的标识符/登录名。 **最低权限** Citrix 将对客户内容的访问权限进行限制，仅限那些需要此类访问权限以履行其工作职责的个人进行访问。 **安全和保密** Citrix 要求用户确保计算机和数据在无人照管的情况下获得安全保护。 Citrix 要求密码在其整个生命周期内始终无法被破解。 **身份验证** Citrix 采用行业标准做法来识别并验证访问信息系统的用户的身份。

领域	控制措施
	如采用密码进行身份验证，Citrix 遵循行业标准的密码处理和管理做法，其中包括： 按照系统要求和 Citrix 标准定期更新密码 密码必须符合长度和复杂性要求，包括长度最少为 8 个字符 禁止人员共享密码 停用或过期的标识符不会授予给他人 Citrix 已制定相关程序以停用已损坏或无意中披露的密码。 Citrix 将对使用无效密码反复尝试访问服务的情况进行监控。 Citrix 将采用经过专门设计的做法来确保密码在分配、分发和存储时的保密性和安全性。
预防损失	**恶意软件**。Citrix 将采用防病毒软件和其他控制措施以避免恶意软件（包括源自公用网络的恶意软件）在未经授权的情况下访问客户内容。 **介质处理。**Citrix 将通过分类并采用安全删除流程来处理不再需要的介质。
物理和环境安全（访问控制、可用性控制）	**对 Citrix 设施的物理访问。**Citrix 将对设施的访问权限进行限制，仅限经授权的个人进行访问。员工、承包商和访客在设施内均需佩戴 ID 徽章，并将其始终置于显著位置。Citrix 将通过多种方法监控设施入口，包括设立安保人员、入侵检测和 CCTV 摄像机。 **防止中断**。Citrix 将通过系统来防止因电源故障或线路干扰而导致数据丢失，包括在灾难恢复站点设置全局和冗余服务基础结构；评估数据中心和 Internet 服务提供商 (ISP) 以优化带宽、延迟和灾难恢复隔离方面的性能；将数据中心置于不受 ISP 运营商影响且能够提供物理安全性、冗余电源和基础结构冗余的安全设施中；以及与主要供应商签署正常运行时间协议。 **托管数据中心。**如 Citrix 使用第三方共存数据中心提供服务，Citrix 要求服务提供商满足或超过 Citrix 托管设施的物理和环境安全要求。最低安全要求包括但不限于： • 物理访问限制和安全保障措施（身份验证、日志、监控等） • 充分隔离环境 • 明火消除、检测和预防机制 • 气候控制系统（温度、湿度等）

领域	控制措施
	云计算。如 Citrix 使用 XaaS [基础结构即服务 (IaaS)、平台即服务 (PaaS)、软件即服务 (SaaS)] 提供服务，Citrix 将与 XaaS 提供商签署合同，以提供与 Citrix 托管数据中心实质类似程度的物理访问控制措施。
应用程序和开发安全	**系统开发和维护。**Citrix 已制定 Secure by Design（安全设计）流程，其中包括专门设计的标准和变更控制程序，用以满足信息系统、代码审查和测试以及与使用测试数据相关的安全性方面的安全要求。该流程由专业安全工程团队进行管理和监控，该团队还负责进行设计审查、威胁建模、手动代码审查和抽查以及渗透测试。 **开放源管理**。Citrix 将采用基于软件的系统来管理开放源审查和批准。 此外，Citrix 还将定期对其软件产品进行扫描和审核，以确认开放源合规性。 **变更管理。**Citrix 已制定变更控制程序，用以满足信息系统、测试、测试验收以及与使用测试数据相关的安全性方面的安全要求。软件和配置变更通过标准工单系统进行管理和追踪。
安全操作	**网络设计**。Citrix 将采用专门设计的机制来对服务实施访问管理策略和标准，包括对客户内容的访问权限实施网络控制。这些机制包括（视情况选用）：在 Internet 和内部网络之间配置一个不受信任的中间区域，通过一种安全机制来限制访问以及未经授权的流量；以及通过一个分层结构将 Web 和应用程序服务器与相应的数据库服务器分开，以限制各层之间的流量。
事件管理	**事件响应**。Citrix 专门设计了一个事件响应计划，用于保存、分析、修复以及传达影响 Citrix 托管网络和/或系统或客户内容的安全事件。 **事件通知**。如 Citrix 确定其控制下的客户内容受到安全事件的影响，客户将在适用法律要求的时间段内收到通知。 **事件记录**。Citrix 会留存一份有关已知安全事件的记录，其中包括事件描述、发生时间、事件后果、报告者姓名、事件报告的对象以及恢复数据和服务的程序（具体视情况而定）。
供应商管理	**加盟**。Citrix 将对有权访问客户内容以及/或者处理客户内容的服务组件的服务提供商进行安全评估。 Citrix 要求与服务相关的服务提供商遵守本条中适用于其所提供服务的安全级别。根据欧盟法律可访问客户内容的服务提供商必须自行通过欧盟-美国和欧盟-瑞士隐私保护计划的认证或履行标准合同条款。 **日常维护。** 根据服务提供商所提供服务的敏感性和风险，Citrix 将定期对服务提供商进

领域	控制措施
	行评估。 **退出。** 如供应商关系发生终止，服务提供商必须退回其拥有的所有客户内容，或者证明所有客户内容已被安全销毁。
业务连续性和灾难恢复	**业务连续性。** Citrix 已针对处理客户内容的 Citrix 信息系统设施制定应急计划。 **灾难恢复。**Citrix 的冗余存储及其数据恢复程序经过专门设计，可尝试重建客户内容，使其恢复到其原始状态或上次复制的状态。
客户安全义务	客户负责管理未在服务中明确规定的安全事项。其中包括但不限于： • 限制 Citrix 对客户内容的访问权限，使其仅能访问为客户提供服务所需的内容。 • 防止其网络和服务组件受到干扰，包括监控其网络和计算设备并保证其安全无虞。 • 在服务期限内或服务终止后，根据需要下载客户内容。 • Citrix 将默认对传输中的数据进行加密或向客户提供对传输中的数据进行加密的方法。有关更多详细信息，请参见适用于服务的产品文档。客户负责确保数据在传输过程中得到妥善保护。

1.B. 其他云服务安全控制措施

领域	控制措施
数据保护 （可用性控制、传输控制、数据删除）	**故障转移程序**。Citrix 将通过专门设计的机制来防止客户内容丧失可用性，包括将客户内容的副本存储在与处理客户内容的主计算机设备不同的位置。 **界外数据**。Citrix 将对通过在服务中提供的公用网络传输的客户内容进行加密，或者协助客户对此类内容进行加密。 **保留。** Citrix 可以出于法律的需要在服务期限过后保留客户内容，并对此类内容进行存档以供客户访问。Citrix 将始终遵守本附件中的要求，直至此类客户内容被永久删除。在符合下述“退还”规定的前提下，Citrix 没有义务在服务终止后保留客户内容。 **退还。** 在可用的前提下以及根据适用的服务说明，客户应在本协议期满后三十 (30) 天内下载客户内容。 **数据删除**。如不再需要将客户内容用于合法目的，Citrix 将安全删除此类内容。

领域	控制措施
安全操作	**事件日志记录**。在某些服务中，Citrix 会收集日志。此类日志可能包含访问 ID、时间、授予或拒绝的权限、诊断数据（如追踪和崩溃文件）以及其他相关活动。 这些日志 **(i)** 用于提供、保护、管理、衡量和改进服务和相关分析结果，**(ii)** 按照客户及其用户的指示或说明来使用，和/或 **(iii)** 用于遵守 Citrix 政策、适用法律、 法规或政府要求。其中可能包括监控服务以及相关组件的性能、稳定性、使用情况和安全性。客户不得阻止或干涉此类监控行为。 Citrix 可出于上述目的使用从第三方收集的信息对日志进行补充。 此类日志可用于本附件未规定之目的，但仅限于以汇总形式。
业务连续性和灾难恢复	**备份。**服务采用跨多个物理站点的高可用性双活群集进行维护，除非相应服务说明另有规定。未采用双活配置的系统将根据特定服务的服务级别目标进行备份。

第 2 条 个人数据的处理

个人数据指有关已识别身份或可识别身份的个人的信息。客户可决定要在其客户内容中包括哪些个人数据。在实施服务期间，对于客户内容中包含的任何个人数据，Citrix 为数据处理方，客户始终为数据控制方。根据本协议规定，Citrix 在处理此类个人数据方面将按照客户的说明进行操作。

有关依据《一般数据保护条例》处理个人数据的更多信息（包括此类数据的国际传输机制），详见《一般数据保护条例》条款附件 I。

第 3 条 服务地点

客户内容可能会被传输到美国或者 Citrix 和/或其服务提供商的其他运营国家/地区，并在此类国家/地区进行存储和/或处理。无论 Citrix 在何处存储或处理客户内容，本附件中规定的要求始终适用。

为了便于在 Citrix 提供服务过程中在国际间合法传输数据，双方可以就任何其他数据处理或数据传输协议开展善意协商。

第 4 条 客户内容的披露

根据本条中的规定，客户同意 Citrix 对客户内容进行披露。
Citrix 可以通过分包商和代理商来实施服务。任何分包商和代理商应仅出于实施服务的需要有权访问客户内容，并且应受必要的书面协议的约束，以提供与本附件对 Citrix 规定的数据保护水平相同的数据保护水平（如适用）。Citrix 始终负责确保其分包商和代理商遵守本协议中的条款（如适用）。

此外，Citrix 还可在下列情况下披露客户内容：(a) 出于与本协议一致的目的披露给附属实体；(b) 在发生任何预期或实际的兼并、收购、出售、破产或对其部分或全部业务的其他重组行为时，有义务根据本协议中的条款对客户内容进行保护；或 (c) 出于法律目的，包括行使其权利、发现和阻止欺诈行为、防止对 Citrix、

客户、用户或公众的权利或财产造成损害；以及 (c) 应法律要求，包括对传票、司法或行政命令或者其他有约束力的文书（以下均称“要求”）做出回应。除非法律予以禁止，否则 Citrix 将就任何要求及时向客户发出通知，并为客户提供合理必要的协助，使客户能够及时对要求做出回应。

第 5 条 客户义务

1. 一般条款。客户仅能在本协议允许的情况下使用和访问服务。客户将遵守与其使用服务相关的所有适用法律。

2. 权限。客户应负责取得 Citrix 实施服务所需的所有权限，包括提供任何通知，以及获得 Citrix 访问和处理本附件中规定的客户内容所需的任何同意或许可。

3. 监管。客户应负责确定是否存在需满足本协议（包括本附件）中规定的要求以外的其他监管或安全要求的任何客户内容。客户不得提交或存储任何受《美国国际武器贸易条例》(ITAR) 或任何限制进口或出口国防物品或国防服务的国家/地区的类似条例约束的客户内容。此外，客户不得提供或存储任何受其他监管要求约束的客户内容，例如受保护的医疗健康信息（“PHI”）、支付卡信息（“PCI”）或政府法规规定的受控分发数据，除非客户订单和适用服务说明另有规定，并且双方已事先就 Citrix 处理此类数据签署任何其他必要的协议（如业务伙伴协议 (BAA)）。ShareFile 服务的客户可通过 privacy@sharefile.com 与 Citrix 联系，以申请 BAA。

4. 客户安全环境。 根据服务设计，服务仅能在较大的客户安全环境中提供。客户应确保未明确由 Citrix 管理的所有组件均获得适当的安全功能，包括但不限于与服务配合使用的访问控制措施、防火墙、应用程序和网络。请参见上文第 1.A. 条“客户安全义务”。

5.安全通知。客户应负责按照下文第 VI 条“Citrix 联系信息”中的说明，就任何涉及服务和/或客户内容的安全事件及时向 Citrix 发出通知。

6. 用户合规性。客户应负责确保用户遵守订单和协议中的条款。

第 6 条 Citrix 联系信息

事项	联系信息
客户支持	https://www.citrix.com/contact/technical-support.html
事件上报	secure@citrix.com
Citrix 产品的可疑漏洞	secure@citrix.com

第 7 条 定义

本附件中的术语应采用本协议或下文规定的含义。如果本协议的其余条款与以下任何定义有冲突，本附件将采用以下定义。

客户内容指任何上载至客户帐户进行存储的数据，或者客户的计算环境中为便于 Citrix 实施服务而允许 Citrix 访问的数据。

日志指与服务相关的事件记录，包括衡量性能、稳定性、使用情况、安全性和支持的记录。

安全事件指未经授权访问客户内容而导致失去机密性、完整性或可用性的事件。