
Cloud Software Group

服务安全附件

版本 3.0

生效时间：2022 年 9 月 30 日

目录

范围	3
安全计划与政策框架	3
访问控制	4
系统开发与维护	5
资产管理	5
人力资源安全	6
操作安全	7
加密	8
物理安全	8
业务连续性与灾难恢复	9
事件响应	10
供应商管理	10
合规性	11
客户审核与调查	12
联系方式	12

此 Cloud Software Group, Inc. (下称“Cloud Software Group”、“我们”或“我们的”) 服务安全附件 (下称“附件”) 描述已实施的安全控制措施, 这些措施与根据相关 Cloud Services Group 许可和/或服务协议及“服务”的适用规则 (统称“协议”) 履行向客户提供的 Cloud 服务、技术支持服务或咨询服务 (下称“服务”) 有关。“服务”交付过程中未涉及的 Beta 或实验室/技术预览服务 (包括 Cloud 实验室) 及我们的内部 IT 系统不在本附件的讨论范围内。

首字母大写的术语具有“协议”中规定的含义或此处定义的含义。“客户内容”是指我们访问或收到的任何数据, 或者为进行存储或处理由您发送或上载的任何数据, 以便我们提供服务。此外, 还包括与您的环境有关的专有技术信息, 例如系统或网络配置以及您选择的控件。“日志”是指与使用我们的产品或服务相关的性能、稳定性、使用情况、安全性、支持、硬件、软件、服务或外围设备的信息。

1. 范围

此“附件”描述我们为维持“服务”的机密性、完整性和可用性而采取的各种管理、物理和技术安全控制措施。这些控制措施适用于我们的操作和“服务”系统及环境。Cloud Software Group 采用 ISO/IEC 27002 作为其服务安全计划的基准, 并已获得特定服务的行业认证并通过评估。我们的信任中心的“隐私与合规性”部分中提供了更多信息。

我们致力于持续增强和改进其安全做法, 以便保留修改此处所述的控制措施的权利。任何修改均不会降低在相关服务期限内的安全级别。

2. 安全计划与政策框架

Cloud Software Group 的安全计划与政策框架是由代表整个公司不同业务领域的高级行政管理层制定和批准的。

2.1 安全风险监督

网络风险监督委员会 (CROC) 负责控制安全风险管理活动。CROC 由跨部门的管理层和领导层组成。行政领导团队负责每年审核委员会的成员资格, 以确认涵盖足够的业务和运营领域。

CROC 至少每个季度会晤一次, 并提供有关识别、评估和应对企业运营以及服务交付基础结构所面临的安全风险方面的指导、见解和指示。

2.2 安全风险理

Cloud Software Group 利用安全风险理 (SRM) 计划来识别我们的产品和服务以及我们的基础结构面临的潜在威胁，评估与这些威胁相关的风险的重要性，制定风险缓解战略，以及我们的产品和服务和工程团队合作实施这些战略。

2.3 信息安全

Cloud Software Group 已任命一位首席信息安全官 (CISO)，该人员负责安全监督和政策战略、合规性和战略执行。安全监控与响应主管负责主导事件响应流程，包括调查、控制和补救。

2.4 人身安全与环境安全

Cloud Software Group 安全团队负责监督我们设施的物理使用情况。

3. 访问控制

我们需要使用访问控制措施才能免遭潜在的损坏、折损或丢失，这些措施旨在确保分配和维持正确的特权以访问公司系统、资产、数据和设施。我们遵循最小特权原则或基于角色的安全，以限制用户只能访问履行工作职能或角色所需的内容。

经理负责设计各种角色来进行适当的职责分工，即将任务和特权分配给多个人，以预防徇私舞弊和差错。

3.1 新建帐户、角色和访问请求

Cloud Software Group 需要提出正式申请才能访问公司系统或数据。每个访问请求至少需要用户的经理批准，以确认用户的角色和访问权限。在授予访问系统或数据的权限之前，授权管理员会确认用户是否已获得必要的批准。将采用最小特权原则。

3.2 帐户审核

对于重要系统，我们将至少每年审核两次用户帐户和所分配的权限。如果审核后需要进行任何更改，则必须按照正式访问请求流程确认用户和用户的角色确实需要访问相关系统。

3.3 删除帐户、角色和访问权限

我们要求在用户的角色发生改变（如果适用）、终止、用户聘用期结束或从公司离职时，立即禁用、撤消或删除用户访问权限。

访问权限删除请求将被记录和跟踪。

3.4 凭据

Cloud Software Group 要求对员工进行多重身份验证，才能远程访问我们的系统，并采用以下密码处理和管理做法：

- 按照我们设定的系统要求，需要定期轮换密码

- 密码必须满足长度和复杂性要求，包括数字、特殊字符和大小写字母的组合、最少字符数以及不允许使用常用词或词典词汇
- 不得向其他人授予已停用或已过期的用户 ID
- 我们将按照相关过程停用被无意披露的密码
- 我们将监控使用无效密码反复尝试获取对“服务”的访问权限的行为，并自动采取相关措施以阻止此类反复尝试

Cloud Software Group 将按照以下做法操作，这些做法旨在分配、分发和存储密码时保持密码的机密性和完整性，例如：

- 要求密码在其整个生命周期内保持哈希和/或加密状态
- 禁止共享密码

4. 系统开发与维护

我们采用设计安全流程，其中包括标准和变更控制过程，旨在满足信息系统、代码审核和测试，以及测试数据的使用安全方面的安全要求。此流程由专业的安全团队进行管理和监控，该团队还负责设计审核、威胁建模、手动代码审核和抽查，以及渗透测试。

4.1 安全设计原则

Cloud Software Group 已采用规范化的系统开发生命周期 (SDLC) 方法，可管理计算机信息系统的开发、获取、实施和维护，以及相关技术要求。

我们使用基于软件的系统来管理开源代码审核和批准，其中包括定期执行其软件产品的扫描和审核。我们已就如何使用开源代码以及针对开源代码最佳实践对开发人员及其管理层展开培训制定了相关政策，并记录在案以供所有员工查看。

4.2 变更管理

我们的基础结构和软件变更管理流程可满足安全需求，并要求在部署到生产环境之前，先授权、正式记录、测试（如果适用）、审核和批准对软件和基础结构进行的更改。基础结构和软件变更是使用工作管理系统进行管理和跟踪的。

变更管理流程将被适当地分离开来，并且只有授权人员才拥有将变更迁移到生产环境的权利。

5. 资产管理

5.1 物理和虚拟资产管理

Cloud Software Group 将维护由我们管理的用于履行“服务”（“服务资产”）的物理和虚拟系统的动态库存清单。系统所有者负责根据我们的安全标准来维护和更新其“服务资产”。

制定的规范处置过程可以为安全处置 Cloud Software Group 和客户数据提供指导。我们会根据分类并使用删除流程来处理不再需要的数据，这些流程旨在防止数据被改造或读取。

当在指定或分配区域中不再需要我们的技术资产时，对其进行清理和处置。技术资产包括但不限于个人计算设备、多功能计算设备、存储设备、成像设备和网络设备。处置是通过全球安全风险服务与信息安全进行协调的。

5.2 应用程序和系统管理

应用程序和系统所有者负责审核他们存储、访问、删除或传输的数据并对其进行分类。在其他控制措施方面，员工和承包商需要执行以下操作：

- 在 Citrix 机密信息的两个最高类别之间对客户内容进行分类，并应用相应的访问限制
- 限制打印客户内容并在安全的容器中删除已打印的资料
- 在不满足 Citrix 安全政策和标准的任何装备或设备上，不要存储公司信息或机密信息
- 在无人值守时保护计算机和数据的安全

5.3 数据保留

在终止“服务”后的有限时间段内，作为我们 Cloud Services 的一部分而存储的客户内容将可供客户访问，但随后会在向客户发送删除确认后删除（备份副本除外）。其他详细信息在特定的服务文档中提供。如果出于法律目的需求，也可以在服务完成后保留客户内容。Citrix 将遵循此附件的要求，直到客户内容被永久删除为止。

6. 人力资源安全

维持客户内容的安全是所有员工和承包商的核心需求之一。我们的商业行为准则要求所有员工和承包商遵守我们的安全政策和标准，特别是要设法保护机密信息以及客户、合作伙伴、供应商和员工的个人信息。

所有员工和承包商都必须遵守保护客户信息的保密协议。此外，Cloud Software Group 安全组织还会就信息安全与物理安全方面的相关主题定期与员工进行交流，以保持对特定主题的安全意识。

6.1 背景筛查

我们当前使用背景筛查在全球雇用所有新供应商，并且要求采用相同的方法雇用其第三方供应商人员，受本地法律或雇佣法规限制除外。

6.2 培训

所有员工都必须参加有关数据保护和公司政策方面的培训，旨在保护我们机密信息的安全，这些机密信息包括我们的客户、合作伙伴、供应商和员工的机密信息。培训涵盖隐私保护做法和处理个人信息的员工需要遵守的法则，包括需要对使用、访问、共享和保留个人信息进行限制。工程组织的成员需要参加涵盖安全开发、架构和编码的特定培训。

6.3 执行

所有员工都必须遵守我们的安全和隐私政策及标准。如不遵守，则会受到纪律处分，甚至解除劳动合同。

7. 操作安全

7.1 网络和系统安全

Cloud Software Group 已将网络和系统强化标准记录在案，旨在确保网络和系统的配置是安全的。根据这些标准需要遵守的过程包括但不限于：

- 更改或禁用默认设置和/或帐户

- 有节制地使用管理访问权限
- 将服务帐户限制为仅用于创建时的目的
- 配置适用于审核的日志记录和警报设置

我们要求在服务器和工作站上实施反恶意程序软件，并扫描网络中是否存在恶意软件。

网络控制措施用于控制对客户内容的访问。这些措施包括（如果适用）：在 **Internet** 与内部网络（包含用于限制访问和未经授权的流量的安全机制）之间配置不受信任的中间区域；对网络进行分段，以防止对客户内容进行未经授权的访问；以及将 **Web** 服务器和应用程序服务器与分层结构（限制两个层之间的流量）中的相应数据库服务器分开。

7.2 日志记录

我们会收集日志以确认我们的“服务”正常运行，协助对系统问题进行故障排除，以及保护我们的网络和客户内容。日志可能包括访问 ID、时间、授予或拒绝的授权、跟踪文件和崩溃文件等诊断数据，以及其他相关信息和活动。

我们会出于以下目的收集和使用日志 (i) 用于提供、保护、管理、衡量和改进服务，(ii) 应客户或其最终用户的要求，(iii) 用于计费、帐户管理、内部报告和产品战略，和/或 (iv) 用于遵守协议、政策、适用法律、法规或政府要求。这可能包括监控“服务”和相关组件的性能、稳定性、使用情况和安全。日志可能包括访问 ID、时间、授予或拒绝的授权、跟踪文件和崩溃文件等诊断数据，以及其他相关信息和活动。客户可能无法阻止或干预此类监控。

有关客户内容和日志处理的详细信息，请参阅我们的信任中心[Cloud Assurance Data Protection & Security section](#)，其中包含多份有关 Citrix Cloud Services 日志记录的白皮书。

7.3 证书、凭据和密码管理

Cloud Software Group 制定的政策涵盖证书、凭据和密码的生命周期，可确保安全性、可用性和机密性。密码管理者必须记录在案，并正式承认他们愿意承担作为密码管理人员的职责。

其职责包括但不限于：

- 证书必须由经过批准的证书颁发机构颁发
- 加密密钥不得以纯文本形式存储或传输，并且必须使用经过严格批准的加密协议
- 凭据和密码必须至少每年轮换一次，并存储在经过批准的特许身份验证管理工具中

7.4 漏洞管理

我们会定期通过自动扫描漏洞和端口来监控应用程序和系统是否存在漏洞。

识别出的漏洞需要在一定时间内进行修复，具体取决于严重性级别和供应商建议。如果没有可用的修补程序、更新或永久性的修复措施，我们将采取相应的对策来降低漏洞利用风险。

8. 加密

8.1 保护传输中的数据

Cloud Software Group 已部署安全传输协议，以通过属于“服务”一部分的公用网络传输信息。“服务”通过加密进行保护，而通过 **Internet** 进行的访问则由 TLS

连接加以保护。

8.2 保护静态数据

我们要求使用最低 128 位全磁盘加密对所有用于提供服务的工作站进行加密。除非进行了加密，否则客户内容不能存储在任何便携式设备上。

某些 Cloud Services 会默认对特定的数据元素进行加密，还可能会提供其他供客户实施的加密功能。请参阅适用的 Cloud Services 文档以了解更多详情。

9. 人身安全

9.1 设施

我们会采用以下控制措施来防止未经授权便进出任何设施：

- 只有授权人员才能进出设施
- 访问者需要在数字访问者日志中注册，并且被护送或始终受到监测。
- 员工、承包商和来宾必须佩戴 ID 工卡，并且当他们未离开设施时必须始终佩戴工卡
- 下班时间进出设施时的安全管理和控制措施
- 保安、入侵检测和/或 CCTV 摄像头会监控公司大楼的入口、装卸码头及公共通道区域（用于监控通道的装置可能因设施而异，具体取决于设施和位置）

此外，Cloud Software Group 设施还提供：

- 灭火和火警探测系统或设备
- 气候监测系统或设备（温度、湿度等）
- 易于使用的水控断流阀或隔离阀
- 紧急出口和疏散路线

通过使用工卡进出保护办公室的数据储藏室。

9.2 数据中心

除了以上所述的设施控制措施之外，对于 Cloud Software Group 拥有和管理的设施，我们会在其用于提供“服务”的数据中心实施其他控制措施。

我们会使用旨在防止因电源故障或线路干扰而导致数据丢失的系统，包括使用灾难恢复站点进行设置的全局和冗余服务基础结构。对数据中心和 Internet 服务提供商 (ISP) 进行评估，以优化有关带宽的性能、减少延迟和灾难恢复隔离。

数据中心所在的设施为 ISP 运营商中立，并且由关键供应商提供物理安全、冗余电源、基础结构冗余和正常运行时间协议。

当我们使用第三方数据中心或云服务来交付“服务”时，我们会与满足或超过我们设施的物理和环境安全要求的提供商签订合同。

10. 业务连续性与灾难恢复

10.1 业务连续性

在出现不利或破坏性的情况下，Cloud Software Group 会制定战略计划以继续业务运营，并对系统进行设计以在出现此类事件时保持服务处于运行

状态。

我们将至少每隔两年执行一次部门级别的业务影响分析 (BIA)，并且每年审核一次。 BIA 将用于创建部门业务连续性计划 (BCP)，该计划将确定和记录每个部门的资源要求、恢复参数和方法、重新定位需求，以及整个流程所需的安全保护措施，以避免失败或产生差距。 每个部门的高级管理层将每年审核和批准一次 BCP，或者在发生重大组织变更时执行该操作。

我们为所有我们的设施制定了紧急和应急计划。 如果设施不可用，员工可以选择在其他 Cloud Software Group 设施或其选择的位置远程工作。其他恢复战略记录在 BCP 中（如果适用）。

10.2 灾难恢复

通过实施旨在确保有序、稳定地修复和恢复我们的业务系统和数据的流程和控制措施，我们将努力尽可能降低服务或运营中断产生的影响。 Cloud Software Group 将为所有任务关键型系统、数据和基础结构实施冗余。 灾难恢复计划 (DRP) 将使用上述 BIA 中执行的评估来识别和记录恢复事件参数、方法、优先级以及整个流程所需的安全保护措施，以避免失败或产生差距。

该计划概述了修复关键系统和数据的整体结构和方法，包括但不限于：

- 个人或团队的角色和职责
- 重要人员或第三方的联系信息
- 针对重要人员的培训要求和计划
- 恢复目标、修复优先级和成功标准
- 完全恢复和修复的架构

高级管理层将每年审核和批准一次 DRP，或者在发生重大组织变更时执行该操作。

11. 事件响应

Cloud Software Group 制定了网络安全事件响应计划，其中详细描述了检测、报告、识别、分析和响应安全事件的流程，这些事件影响我们管理的网络和/或系统或客户内容。 至少每年举行一次安全事件响应培训和测试。

“安全事件”是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。 如果我们确定在我们控制下的客户内容出现安全事件，则将在法律规定的时间内通知您。 我们的通知将描述（已知）事件的本质、时间段，以及对您产生的潜在影响。

我们将保留每个安全事件的记录。

12. 供应商管理

Cloud Software Group 可能会通过转包商和代理履行“服务”。 任何转包商和代理都只能根据需要访问客户内容以履行“服务”，并且应受到书面协议的约束，这些协议要求他们根据本附件至少提供我们所需级别的数据保护（如果适用）。 我们必须始终负责确保其转包商和代理遵守“协议”的条款（如果适用）。 有关能够访问客户内容的 Cloud Software Group 分包处理方的列表，请访问 [我们的信任中心](#)。

12.1 建立合伙关系

我们的第三方风险管理计划提供了系统方法来管理使用第三方供应商所产生的安全风险。在与采购此类第三方交涉采购事宜之前，我们会努力识别、分析和缓解安全风险。

Cloud Software Group 会与供应商签订协议，以记录符合本附件规定的相关安全措施和责任。

12.2 持续评估

我们会定期执行安全风险评估，旨在确保在整个供应商关系持续期间有现成的安全措施。对提供的服务进行更改或对现有合同进行更改需要评估安全风险，以确认变更不会产生其他或不合理的风险。

12.3 解除合作关系

在计划结束与供应商的合作关系前至少 90 天或与供应商签订的合同过期之前（除非需要提前终止），我们会尽力通知相关公司的采购组织。相关公司的采购组织应协调终止现有关系，以确保我们的企业数据和资产受到妥善处理和保护。

13. 合规性

13.1 处理个人数据

个人数据是指与身份已经过鉴定或可鉴定身份的个人的信息。客户内容中包含的个人数据由您决定。履行“服务”时，我们充当数据处理方，客户则始终充当客户内容中包含的任何个人数据的数据控制方。根据“协议”的规定，我们将在处理此类个人数据时按照您的指示行事。

Cloud Software Group [数据处理附件](#) 提供了有关根据《通用数据保护条例》（包括对个人数据进行国际传输时所采用的机制）处理此类数据的更多信息。

13.2 服务位置

Cloud Services 客户对其 Cloud Services 的地理位置拥有选择控制权。在适用的 Cloud Services 订阅期间，我们不得在未经您同意的情况下更改您所选的环境地理位置。请注意，某些 Cloud Services 可能不允许选择特定的地理位置，并且作为一般服务交付的一部分，可以将客户内容传输到美国或 Citrix 和/或其服务提供商将根据需要运营以提供“服务”的其他国家/地区。

13.3 客户内容披露

我们可能会在法律规定的范围内披露客户内容，包括响应传票、裁决令或行政命令，或者其他有约束力的文件（每种文件都称为“需求”）。除了法律禁止之外，我们还会及时通知客户任何“需求”，并为客户提供合理且必要的帮助，以便客户及时响应“需求”。

13.4 客户安全和法规要求

“服务”应在大型客户 IT 环境中交付，以便客户全权负责未明确规定由 Citrix 管理的安全的各个方面，包括但不限于与“服务”的技术集成、用户访问管理和控制，以及客户可能将其与“服务”结合使用的所有应用程序和网络。

您需负责确定他们对“服务”的使用（包括向我们提供访问作为服务一部分的任何客户内容的权限）是否需要遵守“协议”规定之外的法规或安全要求，包括本附件。因此，客户必须确保未提交或存储任何受法律（将实施本附件中不包含

的特定控制) 管控的客户内容, 本附件可能包括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, 受保护的健康信息 (“PHI”)、付款卡信息 (“PCI”) 或根据政府法规受限分发的数据, 除非可能根据我们的要求, “协议” 和适用的 “服务描述” 以及签订任何其他协议 (如 HIPAA 商业伙伴协议) 的相关方提前规定。

14. 客户审核与调查

Cloud Software Group 每年响应一次审核请求, 方式是响应客户风险评估。客户也可以随时访问我们的 Due Diligence Package, 以获取更新后的安全程序包和调查表。我们的 Due Diligence Package 是客户安全调查而创建的, 它提供随时可用的安全信息, 包括 Shared Assessments 公司针对我们的 Cloud Services 已填写的 Standardized Information Gathering (SIG) Lite 调查表。您可以从我们的[信任中心 \(云保证数据保护和安全性部分\)](#) 下载 Due Diligence Package。

15. 联系方式

职责	联系方式
客户支持	https://www.citrix.com/contact/technical-support.html
报告安全事件	secure@citrix.com
我们的服务中存 在可疑漏洞	https://www.citrix.com/about/trust-center/ (单击 “报告安全问题” 按钮。)

企业销售

北美洲 | 800-424-8749

Worldwide | +1 408-790-8000

位置

公司总部 | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States Silicon Valley |
4988 Great America Parkway Santa Clara, CA 95054, United States

©2022 Cloud Software Group, Inc. 保留所有权利。本文出现的所有标记均为 Cloud Software Group, Inc. 和/或其某个或多个子公司的财产, 并且可能已在美国专利与商标局及其他国家/地区注册。所有其他标记均为其各自所有者的财产。