



最后更新日期：2022 年 6 月 16 日

“通用条款”的本云服务附件适用于购买云服务的客户。

## 1. 云服务。

- 1.1. 客户可根据本协议和《云服务指南》在订阅期限内使用云服务。VMware 应根据《服务级别协议》提供云服务。
- 1.2. 如果云服务包含软件权利，则该软件受“软件附件”中相应条款的约束。

## 2. 可接受的使用。

- 2.1. 客户不得：(a) 以法律禁止的方式或可能会违反法律的方式使用云服务；(b) 在使用云服务时侵犯他人的权利；(c) 使用云服务以试图未获授权访问任何服务、设备、数据、帐户或网络、测试任何服务、设备、数据、帐户或网络的漏洞或破坏任何服务、设备、数据、帐户或网络；(d) 使用云服务分发垃圾邮件或恶意软件；(e) 以可能会损害或妨碍任何人使用服务的方式使用云服务；(f) 以避免服务的技术限制、定期费用计算或用量限制的方式使用云服务；或 (g) 使用云服务从事高风险活动。
- 2.2. 客户不得上传：(a) 任何可能会对任何人或财产造成损害风险的内容；(b) 任何可能会构成或促成犯罪或侵权的内容；(c) 任何非法、违法、有害、色情、诽谤、侵权的内容或侵犯个人隐私或公开权的内容；(d) 客户无权上传的任何内容；(e) 受 HIPAA 约束的信息（除非客户已与 VMware 签署业务伙伴协定）；(f) 任何需要出口许可或受适用出口管制法律限制的内容；(g) 任何需要分类或列入美国军需品清单或为适用数据中心所在司法管辖区发布的类似清单中的内容；(h) 任何含有 ITAR 相关数据的内容；或 (i) 本协议禁止的任何其他内容。

## 3. 安全措施。

- 3.1. VMware 必须实施和保证适当的技术和组织安全措施，以保护客户内容的机密性、完整性和安全性。VMware 不得访问或披露客户内容，除非出于提供云服务的需要，如产品或服务特定说明所述或“通用条款”第 9.4 条（必需的披露）所述。将客户内容上传至云服务不是向 VMware 披露客户内容。
- 3.2. 客户必须：(a) 采取适当措施保护客户内容；(b) 向其用户提供任何必要的声明，并依据法律要求获得其用户的同意；(c) 如客户认为其账户被盗用，尽快通知 VMware；以及 (d) 与 VMware 合理地合作，以解决与客户使用云服务相关的问题。客户应负责确保云服务适合客户的预期用途。客户应对在其登录凭据下发生的任何服务产品的使用负责。

## 4. 修改和终止提供。

- 4.1. VMware 可能会对云服务、《云服务指南》或《服务级别协议》进行商业上合理的修改。任何改变将自在发布之日起生效。
- 4.2. 如果 VMware 进行的修正会对客户使用云服务产生重大不利影响，则 VMware 须在此项改变生效日期之前通知客户。客户可在通知之日起 30 天内决定是否终止其云服务权利。客户可依据本第 4.2 条通过向 VMware 发送载明有效终止日期的通知来终止其云服务权利。在终止提供某项云服务之前，VMware 须至少提前六个月发出通知。
- 4.3. 客户应负责承担云服务有效终止日期或终止提供云服务之前已发生的所有费用。VMware 将按比例退还自有效终止日期或终止提供日期起的任何预付的费用。

5. **支持请求。** VMware 将根据支持政策（见 [www.vmware.com/cn/support/policies](http://www.vmware.com/cn/support/policies)）为云服务提供支持服务。VMware 可能需要对客户的云服务实例进行有限访问，以处理客户的支持请求。

6. **数据删除。** 根据《云服务指南》的相应规定，当客户的云服务权利到期或终止后，客户内容将被删除。客户应负责确保在其云服务权利到期或终止之前已保留客户内容的必要副本。

## 7. 定义。



**高风险活动：**指失败后可能导致人身伤害、死亡或环境破坏的活动相关的工作负载或应用，包括操控飞机或其他公共交通工具、核设施或化学设施、生命支持系统、植入式医疗设备、机动车辆、武器系统或任何类似场景。

**HIPAA：**指经修订和增补的美国 1996 年《健康保险流通和责任法案》，以及根据该法案颁布的条例。