远程终端访问请求远程代操作服务产品政策

本政策补充并规定了申请高鸿提供远程终端访问时所应遵守的附加条款和条件。本政策中未定义的任何术语均具有订单或客户协议中赋予的含义。

1. 服务描述

客户可以申请提供远程代操作（Smart Hands） 支持服务，以便将笔记本电脑设备远程连接至高鸿数据中心的公共 Wi-Fi，以及连接至桥接这两个连接的客户系统的串行端口，以帮助客户远程终端访问其系统（“**远程终端访问**”）。

出于安全和可用性原因，高鸿建议客户使用配备了相应安全软件的高鸿自有设备来安全地远程访问客户的系统，满足客户的远程终端访问要求。但是，如果客户无法使用高鸿自有设备，在某些情况下，高鸿可以在客户设备上支持实现远程终端访问要求。这时，客户必须提供：(a) 硬件（笔记本电脑或其他支持设备以及电源线）；(b) 所有必备软件（含安全软件）；(c) （通用或客户创建的）登录凭证；及 (d) 支持使用笔记本电脑/设备的说明。

如果客户使用其自有设备，则必须在申请远程终端访问支持前，把笔记本电脑（或其他支持设备）提交到数据中心。客户提供的笔记本电脑必须：(i) 拥有标准以太网或串行端口，或者包含支持连接的合适适配器；(ii) 有线和无线连接（Wi-Fi、宽带和蜂窝网络）；及 (iii) 已安装网络会议或远程连接软件。此外，客户还必须提供笔记本电脑以及网络会议的访客访问权限或通用登录凭证，或者远程连接软件。高鸿不支持使用高鸿信息或高鸿员工信息创建账户。在数据中心进行远程终端会话后，客户可以选择将其提供的笔记本电脑存放在数据中心内客户上锁的机笼/机柜中（用于未来远程会话），也可将该笔记本电脑寄回给客户或寄至其他数据中心。

2. 其他

高鸿已经对其现有实践进行了一次审核。根据审核结果，高鸿认为该实践对客户造成潜在的网络安全风险。客户确认通过公共 Wi-Fi 访问其系统实施远程连接存在相关风险，并同意接受和承担与该远程终端访问有关的全部风险。

为了减少与远程终端访问请求有关的任何未经授权访问客户数据或客户数据丢失，客户将制定、实施、维护和应用适当的管理和技术防护措施，这些措施经过合理适当设计，旨在保护客户设备和该设备上存储的数据（“**客户数据**”）安全，包括但不限于：(i) 对客户数据加密；(ii) 使用侵入检测和监控、防火墙、杀毒保护软件以及符合当时行业标准的其他相关安全措施；及 (iii) 定期备份客户数据并存储该备份。客户不得向高鸿提供客户数据的任何访问权限。

客户确认并同意，虽然高鸿将尽合理努力正确且安全地提供远程终端访问，但可能无法遵守与惯常提供相关非标准请求的企业所适用的相同行业标准。高鸿将尽合理努力把任何高鸿设备还原到上一次注销时的状态，客户则负责从高鸿提供的任何设备中删除其任何格式的专有信息（例如，文本文件、PDF、Word 文档），以避免潜在的安全问题。

在法律允许的最大范围内，对于与远程终端访问和相关远程代操作服务有关的任何行为或不作为直接或间接引致的任何损失或损害，高鸿不承担任何责任和义务。高鸿概不作出并且在此否认作出任何及一切明示或默示的保证，包括但不限于适销性保证或特定用途适用性保证，且客户进一步确认所有非

标准请求均“按现状”提供。在任何情况下，无论是基于合同、侵权（含疏忽）或其他，高鸿概不对任何原因导致的间接、附带、特殊、信赖、惩罚性或后果性损害赔偿承担责任，即使已被告知此等损害赔偿的可能性也是如此。

如果本政策所述的任何其他责任限制因任何原因失效，双方同意，考虑到高鸿执行的是非标准请求，与远程终端访问服务有关或由此引致的高鸿全部责任在任何情况下均不超过五百美元 (USD 500) 或等值当地货币。