软件支持、服务可用性和维护

我方对 **Innovative SAAS（软件即服务）订阅（例如：Vega、Innovative Mobile、Innovative Phone Alerts）**的软件支持、维护以及为之提供的服务的可用性概述如下。

支持

请求支持。支持包括问题分析、支持案例管理、问题优先级确定、问题跟踪和调查以及错误消息解释。贵方必须向我方提供解决问题所需的信息。这包括相关联系信息、问题详情、错误消息、用户 ID 以及任何其他必要信息。如果贵方在使用我方的软件时遇到问题，贵方的指定管理员可以在正常工作时间内联系我方。我方将向贵方的管理员提供一个内部门户网站，用于报告问题并查看问题状态。

响应。我方将尽商业上合理的努力，达到以下服务水平目标。确认接收和开始排除故障和诊断问题的目标响应时间如下所示。我方会尽一切努力尽快解决您的问题，但无法对解决时间作出保证。

优先级	响应	标准
严重等级 1	1 个工作小时	软件的一个主要组件处于无响应状态，严重影响图书馆的生产力或运行。对整个图书馆系统造成较大影响的问题。广泛系统可用，运行系统停机
严重等级 2	4 个工作小时	严重等级 1 中未涵盖的任何妨碍运行的组件故障或功能丧失，例如（但不限于）：响应时间过慢；功能下降；错误消息；备份问题；或影响模块或数据使用的问题
严重等级 3	2 个工作日	(a) 对业务流程没有直接、重大影响，(b) 只对某个细分用户群体产生影响，或 (c) 尚未破坏关键时间业务流程的问题（严重等级 1 或 2 除外）。
严重等级 4	在合理可行的情况下尽可能及时	与性能无关的事件，包括：一般问题、信息请求、文档问题、改进请求。这些事件会被记录，但不会立即采取措施。我方通常会监控相关情况，但没有义务提供任何解决方案。

上报路径。如果贵方在上述指定时间内未收到回复，请联系贵方的客户经理。

托管服务

服务可用性

我方努力确保 99.5% 的软件可用性，并在商业上做出合理努力，在合理通知的情况下，在周末或正常工作时间之外（即太平洋时间正常下班后和东部时间开始营业前）安排维护和系统升级。可用性的计算方法是将软件在测量期内可用的分钟数除以测量期内的分钟数总和减去任何排除的停机时间。

就此计算而言，(i) 测量期为日历年；及 (ii) 排除的停机时间包括系统维护和版本更新的计划停机时间，以及因以下原因而导致的服务不可用时间：贵方的违约、贵方或贵方用户的任何作为或不作为、我方控制范围之外的原因或者单独的不可用情况（每次均不到 5（五）分钟），前提是，此类情况不是持续性的。

如果可用性连续三个月均低于 99.5%，并且贵方已向 Clarivate 报告中断，则贵方有权获得抵免额，该抵免额等于根据软件在此三个月期间的任何不可用持续时间（但排除的停机时间除外）按比例分配的托管服务费金额。此抵免额为贵方对此类不可用的唯一救济。

安全控制措施

我方采取合理和适当的行政管理、技术和物理措施来保护贵方数据的机密性、完整性和可用性；但是，贵方应与 Clarivate 共同负责确保贵方数据的安全和合规。我方的责任（包括对 Clarivate 托管合作伙伴的托管服务的责任）如下文所述。贵方应根据任何适用的法律法规考虑任何特殊配置或第三方应用程序以及贵方的责任。

下表列出了我方的标准云托管方案的功能。高级支持可能需要额外付费。

功能	标准
7*24 小时网络监控	✓·
专用生产环境	✓·
保证 99.5% 的基础设施正常运行时间	✓·
专用公共 IP 地址和自定义 URL	✓·
操作系统安装和管理	✓·
Library software 安装和升级	✓·
数据备份	每天
存档数据备份保留	30 天

网络系统审计日志。将对所有网络登录活动以及对密码进行的更改进行记录、监控、控制和审计。所有入侵检测和防火墙日志监控均通过托管提供商提供的服务来完成。与客户托管的解决方案有关的相关日志文件和配置文件保留七天，并可在需要时根据要求提供，以便进行审计并解决问题。

加密。作为标准计划的一部分，对传输数据进行加密。

网络监控。将对所有网络系统和服务器进行 24/7/365 监控。我方将监控其系统是否存在安全漏洞、违规行为和可疑活动。包括可疑的外部活动（包括但不限于：未经授权的探测、扫描或入侵企图）和可疑的内部活动（包括但不限于：未经授权的系统管理员访问、对其系统或网络的未经授权的更改、系统或网络滥用或者程序信息被盗或处理不当）。如果 Innovative 得知任何涉及客户生产数据或环境的安全漏洞或可疑活动（包括但不限于：未经授权的访问和服务攻击，例如拒绝服务攻击），Innovative 将尽快通知客户。

物理安全。用于为产品（以及贵方从 Clarivate 购买的其他专业服务，视情况而定）提供支持的物理基础设施（包括服务器、存储设备、交换机和防火墙）由托管提供商提供。托管服务提供商会将出入权限仅限于授权人员，并将通过门卡和/或生物识别扫描来进行门禁控制。通过设于托管设施中的安全摄像头来进行视频监控。

审计和安全测试。托管提供商定期进行安全审计和测试。贵方不得自行对托管提供商进行审计。

安全评估。客户可以对 Innovative 的最佳安全实践进行供应商尽职调查审查。Innovative 将接受由独立事务所进行的年度审计，并应按照客户的要求以保密方式分享其安全认证和审计报告。

信息安全审计/合规。我方的托管提供商每年都会接受由独立第三方审计事务所进行的 SOC 1/SOC 2 类型 2/ISO 27001 审计。我方还为其用于支持托管解决方案的信息安全管理系统执行国际公认的 ISO 27001:2013 标准。我方与满足对安全最敏感的客户要求的托管提供商合作，这些托管提供商提供持续的监控、高度自动化、高可用性，并且高度符合各种全球安全标准认证，其中包括：PCI DSS 1 级、ISO 27001、FISMA 中级、FedRAMP、HIPAA 以及 SOC 1（以前称为 SAS 70 和/或 SSAE 16）以及 SOC 2。我方在美国、加拿大、英国、爱尔兰、澳大利亚和亚太地区的数据中心提供托管方案，但 Clarivate 保留随时增加、减少和/或迁移其数据中心的权利。

贵方的责任。客户负责正确实施访问和使用控制措施，并以客户认为足以确保其数据的适当安全、保护、删除和备份的方式来对客户可能选用的软件的某些特性和功能进行配置。

免责声明

支持服务不包括到访贵方的场所、第三方设备或软件的任何服务、贵方更改软件时产生的问题，或者与客户特定配置或实施相关的咨询服务（例如软件与硬件之间的互动、在贵方场所安装、验收测试协助、客户特定模板或报告等）。对于因贵方未能实施我方所建议并免费为贵方提供的第三方软件修改或更新而导致的任何错误，我方没有纠正义务。

如果中断的根本原因 (i) 系贵方违反协议；(ii) 贵方未能使用最低推荐浏览器标准访问和使用软件；或 (iii) 在我方的控制范围之外，包括但不限于贵方所在地的上游服务提供商的硬件或软件故障或软件的不当使用，我方对停机或任何其他未能满足可用性要求的情况不负责任。贵方可能要求且我方可能同意执行的任何额外服务，将根据当前适用费率按时间和材料收费。

支持政策的变更

我方可自行决定不时更新本政策。

最后更新日期：2022 年 12 月（版本 1.0）