Clarivate™

# Software Support, Service Availability and Maintenance

This document outlines our Software support, maintenance and service availability for **Innovative SAAS subscriptions (ex: Vega, Innovative Mobile, Innovative Phone Alerts)**.

## Support

**Requesting support**. Support includes issue analysis, support case management, prioritization of issues, tracking and investigation of issues and explanation of error messages. You must provide us with the information we need to resolve your problem. This includes relevant contact information, details about the problem, error messages, user IDs, and any other necessary information. If you have problems using our software, your designated administrators can contact us during normal hours. Your administrator will be provided an internal portal to report issues and review their status.

**Response**. We will use commercially reasonable efforts to meet the service level objectives stated below. Target response times to confirm receipt and begin troubleshoot and diagnosis of the problem are below. Resolution times cannot be guaranteed, although we undertake every effort to resolve your issues as soon as possible.

| Priority | Response | Criteria |
|---|---|---|
| Severity 1 | 1 Business hour | A major component of the software is in a non-responsive state and severely affects library productivity or operations. A high impact problem that affects the entire library system. Widespread system availability, production system is down |
| Severity 2 | 4 Business hours | Any component failure or loss of functionality not covered in Severity 1 that is hindering operations, such as, but not limited to: excessively slow response time, functionality degradation; error messages; backup problems; or issues affecting the use of the module or the data |
| Severity 3 | 2 Business Days | An issue (other than a Severity 1 or 2) which (a) has no direct and material impact on business processes, (b) has an impact only on a segment of users, or (c) does not yet disrupt time-critical business processes. |
| Severity 4 | as promptly as is reasonably practical | Non-performance related incidents, including: general questions, requests for information, documentation questions, enhancement requests. These will be logged but no immediate action will be taken. We will generally monitor the situation but will not be obliged to provide any solution. |

**Escalation Path**. If you do not receive a response within the timeframe designated above, please reach out to your Account Manager.

## Hosting Services

### Service availability

We endeavor to ensure 99.5% availability of our software and make commercially reasonable efforts to schedule maintenance and system upgrades during the weekends or outside regular business hours (i.e. after regular end of business Pacific Time and before start of business Eastern Time) with reasonable notice. Availability is calculated by dividing the number of minutes the software was available during the Measured Period by the total sum of the minutes in the Measured Period less any Excluded Downtime.

For the purposes of this calculation, (i) the Measured Period is a calendar year and (ii) the Excluded Downtime includes scheduled downtime for system maintenance and release updates, as well as any service unavailability attributable to your breach, any actions or omissions by you or your users, causes beyond our control, or separate instances of unavailability of less than 5 (five) minutes duration each, provided such instances are not of a persistent nature.

If availability falls below 99.5% in a month for three consecutive months, you will be entitled to a credit equal to the prorated amount of the fees for hosting services for any time during such three-month period in which the software was unavailable (other than Excluded Downtime). This credit will be your exclusive remedy for such unavailability.

**Security Controls**

We take reasonable and appropriate administrative, technical and physical measures to protect the confidentiality, integrity and availability of your data; however, security and compliance is a shared responsibility between you and Clarivate. Our responsibilities, including those managed by Clarivate hosting partners, are described below. You should take into consideration any special configurations or third-party applications and your responsibilities depending on any applicable laws and regulations.

The table below sets forth the features of our standard cloud-based hosting option. Premium support may be available for an additional cost.

| Feature | Standard |
|---|---|
| 24x7 network monitoring | ✓▪ |
| Dedicated production environment | ✓▪ |
| 99.5% guaranteed infrastructure uptime | ✓▪ |
| Dedicated public IP address and custom URL | ✓▪ |
| Operating system installation and management | ✓▪ |
| Library software installation and upgrades | ✓▪ |
| Data backups | Daily |
| Archive data backup retention | 30 days |

*Network Systems Audit Logging*. All network logon activity and password changes are logged, monitored, controlled and audited. All intrusion detection and firewall log monitoring is done through services provided by the Hosting Provider. The pertinent log files and configuration files related to customer's hosted solution are retained for seven days and can be made available upon request for audit and problem resolution, as may be required.

*Encryption*. Encryption for data-in-transit is provided as a part of the Standard Plan.

*Network Monitoring*. All network systems and servers are monitored 24/7/365. We will monitor its systems for security breaches, violations and suspicious activity. This includes suspicious external activity (including, without limitation, unauthorized probes, scans or intrusion attempts) and suspicious internal activity (including, without limitation, unauthorized system administrator access, unauthorized changes to its system or network, system or network misuse or program information theft or mishandling). Innovative will notify Client as soon as reasonably possible of any known security breaches or suspicious activities involving Client's production data or environment, including, without limitation, unauthorized access and service attacks, e.g., denial of service attacks.

*Physical Security*. The physical infrastructure used to support the product (and other professional services purchased by you from Clarivate, as applicable), including the servers, storage, switches, and firewalls, are provided by the hosting provider. The hosting provider limits access to only authorized personnel, and badge and/or biometric scanning controls access. Security cameras placed in the hosting facilities provide video surveillance.

*Audit and Security Testing*. Hosting providers perform regular security audits and testing. You may not perform own audits of hosting providers.

*Security Assessments*. Client may perform vendor due diligence reviews of Innovative's security best practices. Innovative undergoes annual audits by independent firms and will share its security certifications, and audit reports under Non-Disclosure, as requested by Client.

*Information Security Auditing/Compliance*. Our hosting providers undergo SOC 1/SOC 2 Type 2/ISO 27001 audits each year by independent third-party audit firms. We also hold the internationally-recognized ISO 27001:2013 standard for its information security management system supporting the hosting solutions. We partner with hosting providers who are designed to satisfy requirements of most security sensitive customers with constant monitoring, high automation, high availability, and highly accredited to global security standards, including: PCI DSS Level 1, ISO 27001, FISMA Moderate, FedRAMP, HIPAA, and SOC 1 (formerly referred to as SAS 70 and/or SSAE 16) and SOC 2. We offer hosting options in datacenters located in the United States, Canada, United Kingdom, Ireland, Australia and the Asia-Pacific region, however, Clarivate reserves the right to increase, decrease and/or relocate its datacenters at anytime.

*Your responsibility*. Client remains responsible for properly implementing access and use controls and configuring certain features and functionalities of the software that Client may elect to use in the manner that Client deems adequate to maintain appropriate security, protection, deletion, and backup of its data.

## Disclaimer

Support services do not include visits to your site, any services for third party equipment or software, problems stemming from a change you made to the software, or consulting services related to client specific configurations or implementation (such as interactions between the software and your hardware, installations at your site, assistance with acceptance testing, client specific templates or reports, etc). We have no obligation to correct any error resulting from a failure by you to implement a third-party software modification or update recommended by us and provided to you at no charge.

We are not responsible for downtime or any other failure to meet the availability requirement if the root cause of the disruption is (i) your breach of the agreement; (ii) your failure to use minimum recommended browser standards for access to and use of the software; or (iii) outside of our control including, but not limited to, failures of hardware or software of upstream service providers or at your location or improper use of the software. Any additional services which you may request and we may agree to perform will be billed on a time and materials basis subject to our current applicable rates.

## Changes to Support Policy

This policy may be updated by us from time to time, in our sole discretion.

Last Updated: December 2022 (version 1.0)