This Support & Maintenance Policy is part of the Subscription Agreement by and between Subscriber and iCIMS. In the event of a conflict between this Policy and the Agreement, unless otherwise expressly provided, the Agreement will control. All capitalized terms not defined herein have the meaning ascribed to them in the Agreement.

This Policy applies to the support and maintenance practices for the Application. Support and maintenance practices specific to Power-Ups are set forth in our then current Power-Up Support & Maintenance Policy, incorporated into this Policy by reference and available at Power-Up Support & Maintenance Policy 8.8.2014.

Definitions

- **“Application Availability”** means the availability of the Application at the Demarcation Point for use without Severity 1 Issue by Subscriber 24 hours per day, 7 days per week, 365 days per year (24x7x365) less the Maintenance Period and Disaster recovery period, and represents the combined availability of networks and servers supporting the Application.

- **“Backup”** means an encrypted backup of the servers, including Subscriber and User Data, log files, configurations, and any control files required to restore Subscriber’s configuration of the Application in the event of a Disaster.

- **“Data Center”** means the physical location of the iCIMS applications, networks, and servers supporting the Application. Specific details regarding the Data Center are available at www.icims.com/gc/ITdocumentation.

- **“Demarcation Point”** means iCIMS’s border router which is used to establish connectivity from the Data Center to the public Internet.

- **“Disaster”** means any act of God (e.g., earthquake, natural disaster), act of government (e.g., war, terrorism, embargo), or any other act or circumstance that is beyond the reasonable control of such Party that results in partial or total failure or destruction of computer hardware, communications capabilities, or facilities of the Data Center.

- **“Issue”** means one of the following:
  
  (i) a question regarding the use and/or operation of the Application;
  
  (ii) a requested seat assignment, report scheduling, or other change to an existing configuration that iCIMS generally performs as part of SMP as opposed to under a new Order Form; or
  
  (iii) a condition that inhibits the use and/or performance of the Application, including, but not limited to, an event that results in performance degradation, function unavailability, errors, security exposure, or other defects, such that the Application does not operate substantially as described in its documentation.

- **“Issue Resolution”** means one of the following:
  
  (i) As to (i) above, a correct answer to the question regarding the configuration, use, and/or operation of an Application;
  
  (ii) As to (ii) above, a configuration change consistent with the Application documentation that substantially meets the request;
  
  (iii) As to (iii) above, a patch, correction, or bug fix such that the Application substantially conforms to its documentation; or
  
  (iv) As to (i), (ii) or (iii) above, notice that an Issue is caused by a non-iCIMS provided Program or Service.

- **“Maintenance Period”** means the time period during which the Application may not be available because of required system maintenance, upgrades, and other Data Center requirements.

- **“Normal Business Hours”** means 9am ET Monday - 6pm ET Friday, excluding iCIMS recognized holidays.¹

- **“Updates”** means updates, enhancements, revisions, fixes, patches, or other changes to the Application that iCIMS makes generally available to all Subscribers with an active Subscription, but does not include additional modules or components and other applications separately sold under an Order Form. Each Update is deemed an Application once placed in a production environment.

¹ A listing of iCIMS recognized local holidays for an applicable year is available on the iCIMS Care site at iCIMS Holiday Schedule.
“Uptime Percentage” means 99.9%.

Support

Subscriber shall designate a primary point of contact (“POC”) for all support Issues under this Agreement. Subscriber may establish a secondary POC by request. All support issues should be directed to an iCIMS Support Contact via the iCIMS Helpdesk at the following contact information during Normal Business Hours:

Phone: 855-666-8150
Email: helpdesk@icimsnow.com

The iCIMS Helpdesk can also be reached directly through the Application by clicking the Help button at the top right corner. This will direct the POC to the iCIMS Customer Care Site and allow the POC to submit tickets, view past tickets, and access the iCIMS Knowledgebase of training, tips & tricks, and FAQs.

Hosting

Application Availability, measured on a calendar month basis, will be greater than or equal to the Uptime Percentage. Notwithstanding Subscriber/User-side network issues, the Application will respond to User requests in an average of less than one (1) second.

In support of the foregoing performance standards, iCIMS is connected to the Internet backbone via multiple ultra-high-speed fiber optic connections. State-of-the-art routers provide autonomous load-balancing and fail-over. These routers are configured to instantly fail over if any given connection goes down. Each connection follows a different path to the Internet backbone, such that the route automatically fails over to the best available connection.

Issues

Whenever a call is placed by the POC to iCIMS Support Contact, the following information must be provided:

- POC name, Subscriber identification number, email address, telephone number, and FAX number (including area code);
- Information about the nature of the Issue;
- Information about the location of the Issue;
- Any Application error messages associated with the Issue and the steps leading up to the Issue occurrence;
- Detailed description of the Issue;
- Impact of the Issue (in classifying Issues, iCIMS takes into consideration the impact on Subscriber and Users).

In the event iCIMS becomes aware and/or Subscriber notifies iCIMS of an Issue, iCIMS shall address the Issue based on its severity, as determined by iCIMS in its reasonable discretion. iCIMS shall use commercially reasonable efforts to respond to Subscriber within the timeframe specified for the respective severity level, acknowledging receipt of the Issue notification and the status of an initial action plan to accomplish Issue Resolution. iCIMS shall use commercially reasonable efforts, in light of the severity and complexity of the Issue, to provide an Issue Resolution within the time frames specified for the respective severity level.
Severity Definitions and Response Times\(^2\)

These times reflect the targeted time period between the receipt of the iCIMS Support Contact’s notification of an Issue to the initial response and the Issue Resolution, respectively, by iCIMS.

<table>
<thead>
<tr>
<th>Issue Severity</th>
<th>Definition</th>
<th>Initial Response</th>
<th>Status Update</th>
<th>Escalation (as set forth in the table below)</th>
<th>Work Around (if available)</th>
<th>Issue Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity 1</td>
<td>Any Issue that (i) compromises the integrity or security of the Application or Data, or (ii) (a) completely prevents the operation of the Application or precludes work by a User from reasonably continuing, and (b) for which there is no reasonable work-around.</td>
<td>Thirty (30) Minutes</td>
<td>Every Hour</td>
<td>To the Highest Escalation Contact Within Eight (8) Hours</td>
<td>Four (4) Hours</td>
<td>One (1) Day</td>
</tr>
<tr>
<td>Severity 2</td>
<td>Any Issue that (i) substantially restricts the operations of the Application, but for which an alternative solution or work-around exists, or (ii) does not substantially restrict the operations of the Application, but for which an alternative solution or work-around does not exist.</td>
<td>Two (2) Hours</td>
<td>Every Day</td>
<td>To the Next Escalation Contact on a Daily Basis</td>
<td>One (1) Day</td>
<td>One (1) Week</td>
</tr>
<tr>
<td>Severity 3</td>
<td>Any Issue that does not substantially restrict the operations of the Application and for which there is an alternative solution or work-around.</td>
<td>Eight (8) Hours</td>
<td>Every Week</td>
<td>To the Next Escalation Contact on a Quarterly Basis</td>
<td>N/A</td>
<td>Next Update</td>
</tr>
<tr>
<td>Severity 4</td>
<td>Any Issue that is (i) a requested change to an existing configuration, (ii) a question regarding usability, documentation, training, or another knowledge enhancement question or (iii) an enhancement request.</td>
<td>Twenty Four (24) Hours</td>
<td>As Deemed Practical</td>
<td>N/A</td>
<td>N/A</td>
<td>As Deemed Practical</td>
</tr>
</tbody>
</table>

Escalation & Prevention

In the event of an escalation, iCIMS’s internal escalation contacts are as follows:

<table>
<thead>
<tr>
<th>Level</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>1(^{st}) Level</td>
<td>Manager, Customer Success</td>
</tr>
<tr>
<td>2(^{nd}) Level</td>
<td>Manager, Product Development and/or Manager, Hosting/IT (as applicable)</td>
</tr>
<tr>
<td>3(^{rd}) Level</td>
<td>Chief Technology Officer and/or Chief Operating Office (as applicable)</td>
</tr>
</tbody>
</table>

Reporting

For all Severity 1 and 2 Issues, iCIMS shall make available to the POC an Issue report within five (5) working days after Issue Resolution, including the actions taken by iCIMS to achieve Issue Resolution, the response time, and the resolution time. iCIMS shall retain issue reports for at least one month for later reference by the POC.

---

\(^2\) Email and voicemails are deemed to be “received” by iCIMS at the beginning of the next business hour.
**Maintenance**

iCIMS furnishes Updates that include Issue Resolutions promptly after availability of the Issue Resolution, and Updates that include enhancements or other improvements typically within thirty (30) days following general availability of such Update.

**Data Security**

The servers and network supporting the Application are located in the Data Center which is secured by 24x7x365 security, controlled access, and egress to registered parties only, and multiple layers of logical security via firewalls, router management, and user passwords. Specific details regarding the Data Center are available at www.icims.com/gc/ITdocumentation. Further, iCIMS makes use of clustering, load-balancing, and fail-over technologies on the servers supporting the Application. All servers are configured with redundant storage solutions. Many storage devices are hot-swappable, with hot and cold spares kept in stock.

The Application uses authentication and authorization mechanisms, including the use of access control lists, to ensure that Subscriber and User Data can only be accessed by Users who have been so authorized by Subscriber. The recommended Application configuration utilizes HTTPS with server certification, Subscriber authentication and authorization, and encryption. iCIMS uses commercially available software to reasonably maintain security of the Application.

iCIMS monitors its systems 24x7x365 through a combination of third-party and proprietary tools to provide early detection and notification of potential issues, with on-call technical personnel available to prevent issues or correct an Issue quickly if it arises. iCIMS conducts a Backup at least daily and prior to any Update to the Application. iCIMS maintains seven (7) days of daily Backups onsite and moves one of the daily Backups to an off-site storage facility on a weekly and quarterly basis. iCIMS maintains the offsite weekly Backups for approximately ten (10) weeks and the quarterly Backups for approximately one (1) year.

**Disaster Recovery**

In the event of a Disaster, iCIMS shall use commercially reasonable efforts to re-establish access to the Application within seventy-two (72) hours utilizing the most recent Backups. Actual recovery times will vary based on the nature and extent of the Disaster.

In the event of minor to moderate Disaster (e.g., hardware failure), iCIMS will promptly replace the hardware, configuring it for its intended purpose. In most cases, the Application will remain fully functional while the faulty hardware is replaced.

In the event of a major or complete Disaster (e.g., earthquakes, explosions, fires, other natural disasters that result in physical destruction of all or a portion of the Data Center), iCIMS shall promptly initiate a full hardware replacement at a new Data Center unaffected by the Disaster. iCIMS’s technical personnel shall promptly configure the hardware for its intended purpose. The licenses of most software used by iCIMS can simply be transferred without requiring the software vendor to issue a replacement license. iCIMS shall contact software vendors that tie their licenses to hardware serial numbers and shall issue replacement licenses. iCIMS shall then restore Subscriber and User Data from the most recent Backup and shall conduct testing to ensure the Application and Data is properly recovered.

**Remedy**

It is iCIMS’s practice to review the root cause, response times, and Issue Resolutions for all Severity Level 1 and 2 Issues and develop preventative measures, as appropriate. Accordingly, in the event iCIMS fails to meet any obligation in this Policy (a “Service Level Obligation Failure” or “SLO Failure”), iCIMS shall use commercially reasonable efforts to promptly correct and further prevent such SLO Failure. In the event of an SLO Failure extending for two (2) consecutive months or any four (4) months within a twelve (12) month period, Subscriber will have the right, as its sole an exclusive remedy for such breach, to terminate the Agreement for convenience and receive a refund of any pre-paid amounts for the Subscription.