SUPPORT & MAINTENANCE POLICY

This Support & Maintenance Policy ("SMP") is part of the Subscription Agreement by and between Subscriber and iCIMS ("Agreement"). In the event of a conflict between the SMP 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 then-current Subscription Agreement found at www.icims.com/gc. This SMP applies to the support and maintenance practices for the Subscription once implementation for such Subscription is completed.

Support and maintenance practices specific to Power-Ups are set forth in our then current Power-Up Support & Maintenance Policy, incorporated into this SMP by reference and available at www.icims.com/gc.

Definitions

- **"Backup"** means an encrypted backup of the servers, including Subscriber Data, log files, configurations, and any control files required to restore Subscriber's configuration of the Subscription in the event of a Disaster.
- **"Demarcation Point"** means iCIMS' border router which is used to establish connectivity from the Hosted Environment to the public Internet.
- **"Disaster"** means any act of nature (e.g., fire, earthquake, natural disaster), act of government (e.g., war, terrorism, embargo), or any other act or circumstance that is beyond the reasonable control of iCIMS that results in partial or total failure or destruction of computer hardware, communications capabilities, or facilities of the Hosted Environment.
- **"Hosted Environment"** means the hosted locations of the iCIMS applications, networks, and servers supporting the Subscription. Specific details regarding the Hosted Environment are available at www.icims.com/gc-it.
- **"Issue"** means a condition that inhibits the use and/or performance of the Subscription, including, but not limited to, an event that results in performance degradation, function unavailability, errors, security exposure, or other defects, such that the Subscription, taken as a whole, does not operate substantially as described in the Documentation.
- **"Maintenance Period"** means the time period during which the Subscription may not be available because of required system maintenance, upgrades, and other Hosted Environment requirements.
- **"Normal Business Hours"** means 24x5 (9:00 PM ET Sunday – 9:00 PM ET Friday; 2:00 AM GMT Monday – 2:00 AM GMT Saturday), excluding iCIMS recognized holidays.[1]
- **"Other Support Request"** means (i) a request to change to an existing configuration, (ii) a question regarding usability, Documentation, training, or another knowledge enhancement question; (iii) an enhancement request; or (iv) any other incidental matter that delays Subscriber from completing business functions that are not critical to Subscriber's business and for which there is a work-around or alternative solution.
- **"Resolution"** means one of the following:
  - A correct answer to the question regarding the configuration, use, and/or operation of the Subscription;
  - A configuration change consistent with the Subscription Documentation that substantially meets the request;
  - A patch, correction, or bug fix such that the Subscription substantially conforms to its Documentation; or
  - Notice that an Issue is caused by a non-iCIMS provided product or service.

[1] ET – Eastern Time; GMT – Greenwich Mean Time. Please note that all business hours are iCIMS' local business hours for the regional help desk, subject to local holidays. A listing of iCIMS' recognized local holidays for an applicable year is available on the iCIMS Community at iCIMS Holiday Schedule.

- **"Subscription Availability"** means the availability of the Subscription at the Demarcation Point for use by Subscriber without a Severity 1 Issue, 24 hours per day, 7 days per week, 365 days per year (24x7x365) less the Maintenance Period and Recovery Time Objective, and represents the combined availability of networks and servers supporting the Subscription.
- **"System Administrator(s)"** are Users the Subscriber designates as primary liaisons between Subscriber and iCIMS for technical support who act as primary system administrator(s) and shall have the ability to make system wide changes to workflow, reporting, login groups and user privileges.
- **"Updates"** means updates, enhancements, revisions, fixes, patches, or other changes to the Subscription 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 a part of the Subscription once placed in a production environment. For clarity, an Update does not include a release of an upgraded version of a module, component, and/or application that may be available at an additional fee sold under an Order Form.
- "**Uptime Percentage"** means 99.9%.

Support

Subscriber shall designate and maintain at least one (1) System Administrator for all support Issues under this Agreement. A secondary System Administrator may also be designated by Subscriber. Additional System Administrators per Subscription may be considered upon request, which iCIMS may grant in its sole and reasonable discretion. All support Issues must be submitted by a System Administrator via the iCIMS Community at: https://community.icims.com/. System Administrators can also utilize the iCIMS product suite links provided in the platform which will direct the System Administrator to the iCIMS Community and allow the System Administrator to submit support cases, view past support cases, and access the iCIMS Knowledge Base for training, tips & tricks, and FAQs. Subscriber shall notify iCIMS to request the transfer of System Administrator designation to another User by contacting their Account Team or submitting a case through the iCIMS Community.

Hosting

Subscription Availability, measured on a calendar month basis, will be greater than or equal to the Uptime Percentage. Notwithstanding Subscriber/User-side network issues, the Subscription 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

When a designated System Administrator is submitting a case, the following information must be provided:

- Subscriber name, System Administrator name, email address, and telephone number (including area code);
- Information about the nature of the Issue;
- Information about the location of the Issue;
- Any Subscription error messages associated with the Issue and the steps leading up to the Issue occurrence;
- Detailed description of the Issue; and
- Business impact of the Issue.

In the event iCIMS becomes aware and/or Subscriber notifies iCIMS of an Issue, iCIMS shall address the Issue based on its severity level, which is determined by iCIMS in its sole and 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 iCIMS' technical support team receiving notice of the Issue or Other Support Request through Subscriber's submission of a case via the iCIMS Community to the initial response and Resolution, respectively, by iCIMS.

Severity	Definition	Initial Response	Status Update	Escalation (as set forth in the table below)	Work Around (if available)	Resolution
Severity 1	Any Issue that (i) compromises the integrity or security of the Subscription or Subscriber Data, or (ii) completely prevents the operation of the Subscription or precludes work by Users from reasonably continuing, and for which there is no reasonable work-around.	Thirty (30) Minutes	Every Hour	To the Highest Escalation Contact Within Eight (8) Hours	Four (4) Hours	One (1) Day
Severity 2	Any Issue that (i) substantially restricts the operations of the Subscription, but for which an alternative solution or work-around exists, or (ii) does not substantially restrict the operations of the Subscription, but for which an alternative solution or work-around does not exist.	Two (2) Hours	Every Day	To the Next Escalation Contact on a Daily Basis	One (1) Day	One (1) Week
Severity 3	Any Issue that does not substantially restrict the operations of the Subscription and for which there is an alternative solution or work-around.	Eight (8) Hours	Every Week	To the Next Escalation Contact on a Quarterly Basis	N/A	Next Update[3]
Severity 4	Any Other Support Request	Twenty-Four (24) Hours	As Deemed Practical	N/A	N/A	As Deemed Practical

Escalation & Prevention

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

Level	Role
1st Level	Manager within Customer Service
2nd Level	Manager within Labs – Engineering, Director within Customer Service, and/or Manager within Cloud Hosting (as applicable)
3rd Level	Director/VP within Labs – Engineering, and/or Director/VP, Cloud Hosting (as applicable)
4th Level	VP, Services and/or Chief Technology Officer (as applicable)

[2] Notification of an Issue to iCIMS' through Subscriber's submission of a case via the iCIMS Community are deemed to be "received" by iCIMS at the beginning of the next business hour.

[3] "Next Update" may include, but does not require, minor updates, enhancements, revisions, fixes, patches or other changes to the Subscription that iCIMS makes generally available to all Subscribers with an active Subscription. For clarity, minor updates will be designated through changes in the decimal of the previous version.

Reporting

For all Severity 1 Issues, iCIMS shall, upon request, make available to the System Administrator an Issue report within five (5) business days after an investigation into the Issue has been concluded, which may include 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 (1) month for later reference by the System Administrator.

Maintenance

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

Data Security

The servers and network supporting the Subscription are located in the Hosted Environment which is secured by 24x7x365 security, controlled ingress and egress to registered parties only, and multiple layers of logical security via firewalls, router management, and User passwords. Specific details regarding the Hosted Environment are available at https://www.icims.com/gc-it. Further, iCIMS makes use of clustering, load-balancing, and fail-over technologies on the servers supporting the Subscription. All servers are configured with redundant storage solutions.

The Subscription uses authentication and authorization mechanisms, including the use of access control lists, to ensure that Subscriber Data can only be accessed by Users who have been so authorized by Subscriber. The recommended Subscription configuration utilizes encryption in transit, Subscriber authentication and authorization, and encryption at rest. iCIMS uses commercially available software, and other tools to reasonably maintain security of the Subscription.

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 Subscription. iCIMS maintains seven (7) days of encrypted daily Backups with high availability and transfers encrypted Backups to a secured storage location daily. iCIMS also sends encrypted transaction logs to its disaster recovery facilities throughout the day. iCIMS maintains encrypted Backups for approximately one (1) year.

Backup & Disaster Recovery

iCIMS maintains a comprehensive disaster recovery plan to help ensure availability of Subscriber Data in the event of a Disaster. iCIMS tests this recovery plan annually. The majority of iCIMS technical infrastructure has been architected for the cloud and leverages best practices such as high availability and replication of services across multiple locations.

iCIMS' Hosted Environment provides first-level protection for disaster recovery through redundancy at all levels of the operation. Specific details regarding the Hosted Environment are available at https://www.icims.com/gc-it.

iCIMS makes use of clustering, load-balancing, and failover technologies within its architecture. This serves to help minimize any noticeable impact as a result of the failure of a specific server. The majority of iCIMS' technical infrastructure has been architected for the cloud and leverages best practices such as high availability and replication of services across multiple locations.

In the event of a Disaster, iCIMS shall use commercially reasonable efforts to re-establish access to the Subscription within twenty-four (24) hours (**"Recovery Time Objective"**) utilizing the most recent Backups. Actual recovery times will vary based on the nature and extent of the Disaster. iCIMS shall use commercially reasonable efforts to recover Subscriber Data from a Backup made less than or equal to twenty-four (24) hours prior to the Disaster (the **"Recovery Point Objective"**).

In the event of a partial Disaster, iCIMS and/or iCIMS' managed service provider will be notified of the Disaster and will take steps to address any affected infrastructure/service or hardware, if applicable. Should a partial Disaster affect any component of iCIMS' cloud infrastructure, iCIMS technical personnel will be notified by internal and external monitoring software. iCIMS technical personnel will review the affected infrastructure/service and will take necessary action. Should a partial Disaster affect one of iCIMS' Hosted Environments, iCIMS will be notified by Hosted Environment personnel as to the arrangements being made to replace or fix the affected system. The clustering, load-balancing, and fail-over technologies used by iCIMS help to mitigate certain noticeable effects that certain partial Disasters might have otherwise had on the Subscription. In certain situations, the Subscription will remain fully functional while the partial Disaster is addressed.

In the event of a complete Disaster (e.g., earthquakes, explosions, fires, other natural disasters that result in physical destruction of the Hosted Environment), iCIMS will be notified by the managed service provider as to the extent of the Disaster. Based on this information, iCIMS will initiate rebuilding the infrastructure in the appropriate disaster recovery environment. Subscriber Data will then be restored from Backups, as necessary. Once the systems are back online, iCIMS will conduct testing to ensure everything was properly recovered to the expected state.

Remedy

It is iCIMS' 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, and for which the underlying Issue has not been resolved, within sixty (60) consecutive days or for any one-hundred and twenty (120) days in any three hundred and sixty (360) day period, Subscriber will have the right upon prior written notice to iCIMS, as its sole and exclusive remedy for such breach, to terminate the specific Subscriptions (i.e., the particular product(s), offering(s), portal(s), module(s), line item(s) to which such SLO Failure pertains) ("**Affected Subscription**") for convenience and receive a refund of any pre-paid, but unused amounts specific to the Affected Subscription.