Jan 2020

Master Service Level Agreement

Master SLA Statement of Intent

Acceptance of your applicable terms of service (the "Underlying Agreement")), incorporates the terms of this Master Service Level Agreement ("SLA") into the Underlying Agreement by reference. If there is any conflict between a provision in this SLA and a provision in the Underlying Agreement, this SLA will control.

Specific service level commitments for each of the Services are identified in the applicable Service SLA. "Company" means the entity that owns or provides the applicable Services, such as ZixCorp Systems, Inc., AppRiver LLC, and any of their affiliates.

This Master SLA is applicable to all Services offered by the Company.

Definitions
Terms defined in the Underlying Agreement are applicable.

End-User – shall mean a natural person that owns an email account or accounts defined in the email directory of the Customer's electronic email system.
Fix – shall mean the restart, repair or replacement of binary executable code versions of the Software, Hardware, Data Center or trusted third data center functions.
Force Majeure – means the following events: (a) acts of God, such as fire, flood, earthquake or other natural causes; (b) terrorist events, riots, insurrections, war or national emergency; (c) judicial, legal or other action of a governmental authority, which action makes performance impossible, (d) strikes, lockouts, or other labor difficulties or (e) any other event outside of the reasonable control of a party. .
Hardware – shall mean the physical server unit provided by the Company, on which Software resides.
Hosted Services– shall mean Company applications delivered to customers over the Internet as a service. The Company shall be responsible for managing access to the application, including security, availability, and performance.
Agent- shall mean any third-party organization that resells the Services to Customers.
Planned Maintenance – shall mean the periodic pre-announced occurrences when the Hosted Services shall be taken out of service for maintenance.
Problem – shall mean a reported instance, regardless of the source, where a Services feature, or any feature or function thereof, does not perform according to applicable published specifications or published documentation.
Recipient - shall mean any natural human person that receives an email, encrypted email or secure portal notification generated by an End-User using Company Services.
Release – shall mean the general public availability of a Service that is offered to Customer for which there is a change in the version release number to the right of the decimal point in the tenths or a change to the left of the decimal point (e.g. 3.0 to 3.1 or 3.0 to 4.0).
Services – shall mean any subscribed service delivered by Company for a fee. The Services may include the provision and installation of Company owned Hardware and/or Software on the Customer/Agent premises.
Service Upgrade – shall mean a revision to Services or features, improvements or modifications which are proactive and/or corrective versions or builds of the Services and are not marketed as a new Release.
Software – shall mean the Company executable code used to deliver the Services.
Support Requests – shall mean a Customer-generated call or email to Company Technical Support, seeking resolution of the failure of Services to function in accordance with the applicable published specifications and/or published documentation.
Spam – shall mean an email that is both unsolicited by the intended recipient and sent in bulk. In this context, "bulk" means the intended recipient's personal identity and context are irrelevant because the message was sent to many other potential recipients with substantially the same content; and "unsolicited" means the intended recipient had not verifiably granted deliberate, explicit, and still-revocable permission for the email to be sent. "Spam" may also be a delivery mechanism for a "Virus" and other malicious Unsolicited Bulk Email (UBE) such as "phishing".
Technical Support – shall mean all applicable Company procedures, documentation, web resources and employees who assist Customers with the provision, configuration, troubleshooting and maintenance of the Services.
Unavailability – shall mean when, because of failure, Customer is unable to use the Services for their intended purpose. Unavailability shall not include Planned Maintenance or Customer caused outages or interruptions. Unavailability is measured from the time the Customer reports a failure by telephone to Company Technical Support until the operational capability is restored.
Virus/Malware - shall mean a binary or executable code whose purpose is to gather information from the infected host (such as trojans), change or destroy data on the infected host (such as Ransomware), use inordinate system resources in the form of memory, disk space, network bandwidth or CPU cycles on the infected host, use the infected host to replicate itself to other hosts, or provide control or access to any of the infected host's system resources.
Workaround – shall mean an intervention or method in which a feature or benefit can be derived without engaging the original design or procedures.

Technical Support

Customers are required to provide front-line support to their End-Users and Recipients. Company Technical Support provides second - and third - line Technical Support for any Problem escalated by Customer. Company offers Customers training and Technical Support documentation for supporting their End-Users and Recipients. Technical Support documentation includes End-User and Recipient instructional materials and front-line support documentation that covers error messages, corrective actions, troubleshooting steps and escalation procedures.

Agents are required to provide second-line support to their Customers. Company Technical Support provides third - line Technical Support for any Problem escalated by the Agent. Company offers Agent training and Technical Support documentation for supporting their Customers. Technical Support documentation includes End-User and Recipient instructional materials and front-line support documentation that covers error messages, corrective actions, troubleshooting steps and escalation procedures.

Customers/Agents should contact Company Technical Support when a Problem cannot be resolved by the Customer/Agent. Support Requests must come from a person or entity who is a designated representative of Customer/Agent that has been previously registered with Company Technical Support. Customer/Agent is responsible for providing updates to the list of designated representatives and associated contact information. A Problem ticket is created for every reported Problem. Company Technical Support will resolve the Problem or escalate the Problem to be diagnosed, replicated, researched, and corrected, as appropriate, in the shortest time reasonably possible. The Problem is assigned a severity, which determines the urgency and effort applied to the Problem. Only designated representatives will receive Service notifications.

Problem Correction and Classification

Company is responsible for using commercially reasonable efforts to correct Problems as quickly as possible. Escalation procedures ensure Problems are corrected or a satisfactory Workaround is provided to Customer/Agent. The assigned severity code determines the escalation path and time commitments for Problem correction. Company maintains a multi-tiered escalation procedure. At each level of the escalation, additional resources and higher technical knowledge are applied to correct the Problem.

Company will open a Problem ticket and assign a severity code based on the description provided by the Customer/Agent.

Severity Code 1 - Critical Problem that renders the Services inoperable and/or cause it to substantially fail to perform the basic functions as designed. A major outage or down condition where no Workaround exists. Severity Code 1 conditions are only applicable to production environments and affect all Customer/Agent on that environment.

> *Company will use commercially reasonable efforts to (a) isolate and classify the Problem, (b) immediately assign Company technical resources to research and correct the Problem, (c) provide Customer/Agent with periodic reports on the status of corrections (time period agreed-to by the Customer/Agent), and (d) provide Customer/Agent with a resolution for the Problem which may be implemented through a Workaround, Fix, Services Upgrade and/or provision of new Hardware. Company shall make commercially reasonable efforts to resolve and correct a Severity 1 Problem within four (4) hours from notification.*

Severity Code 2 - Either a Critical Problem where a Workaround exists, or a non-critical Problem that significantly impacts the functionality of the Services.

> *Company will use commercially reasonable efforts to (a) isolate and classify the Problem, (b) assign Company technical resources to research and correct the Problem within 72 hours of determination, if practical, (c) provide Customer/Agent with periodic reports on the status of corrections, and (d) provide Customer/Agent with a resolution for the Problem which may be implemented through a Workaround, Fix, Services Upgrade and/or provision of new Hardware. If changes are required to the Company Software, Company shall make commercially reasonable efforts to resolve and correct a Severity 2 Problem within ten (10) business days from notification.*

Severity Code 3 – Isolated Problem that does not significantly affect the functionality provided by the Services or requests for information, reports or system changes.

> *Company will use commercially reasonable efforts to correct a Severity 3 Problem in a future Services Upgrade or Release.*

Severity Code 4 –Service enhancement requests or non-reproducible Customer/Agent Problems.

All suggestions and requests for enhancements are submitted to Company Product Management for consideration for inclusion in a future Services Upgrade or Release.

Company Data Center and Trusted Third Party Data Center Reliability

The Company Data Center is the central operations hub for Company's backbone Services, providing seamless delivery of encryption keys, secure message storage and delivery, message status notifications, threat filtering, archiving and other Services. The Company Data Center has the capacity, scalability, and infrastructure to provide a stable, secure, and highly responsive environment for Company's backbone Services. For some Hosted Services, Company may choose to employ trusted third party data centers to provide additional scalability and national data residency. To reduce the risk of Unavailability, the Company Network Operations Center ("NOC") provides 24x7 monitoring of the network platform, Company's servers, and the Internet. All critical systems have network redundancy. These measures provide identification of potential issues and substantially reduce the risk of outages. The Company Data Center and trusted third party data center services are designed and operated to be available 99.99% of the time as measured on an annual basis.

Responsibilities of the Customer/Agent

a) Customer/Agent is responsible for providing resources and documentation sufficient for Company to reproduce any reported Problem, including a detailed description of the Problem, any log files, steps to replicate, environmental network interdependencies and descriptions, or any other information required by Company to replicate and resolve the Problem.
b) Customers are responsible for providing first-line technical support to their End-User and their Recipients.
c) Agents are responsible for providing second-line technical support to their Customers.
d) Customer agrees to report any damage or loss to Hardware or Software installed on the Customer/Agent premises to Company Technical Support and will expeditiously report any issues pertaining to the performance of any of the Company Services.
e) Customer/Agent should report any suspected breach of the terms of this SLA, within five (5) days of the event, by email to sla@zixcorp.com.
f) Customer/Agent should report suspected breaches to Company as specified in the Company privacy policy.
g) Customer/Agent shall allow reasonable remote or local access to premises for Company employees or designees to allow an installation, inspection, or maintenance of the Company Hardware or Software located on the Customer/Agent premise.

Responsibilities of Company

a) Company (with Customer/Agent cooperation) agrees to use commercially reasonable efforts to establish the cause of any alleged Unavailability.
b) Company will provide Technical Support for the preceding Release of a Service for a period not to exceed 12 months. This is applicable where Software is installed on Customer devices or located on the Customer/Agent premise.
c) Company will use commercially reasonable efforts to restore critical systems of the Hosted Services within twelve (12) hours in the event of Force Majeure. A system Unavailability due to Force Majeure will not be considered Unavailability time.

Exclusions and Limitation of Liability

a) Company reserves the right for Technical Support to be outsourced to a third-party vendor, subject to the terms and conditions with respect to subcontracting, with the understanding that Company shall be responsible for the quality and performance of the Technical Support by the third-party vendor.
b) Company shall not be responsible for the configuration, maintenance or correction of third-party software, hardware or communications facilities.
c) Company shall have no obligation to provide Technical Support for its Services under the following circumstances:
   a. For altered, damaged, or modified Software or Hardware or any portion of the Services incorporated with, on, or into other software;
   b. For Software that is not a supported Release; or
   c. For Problems caused by negligence, misuse, application of the Services other than as specified in applicable published specifications or published documentation, or other factors beyond the control of Company.
d) Company may amend or revise this SLA at any time. Such amendments or revisions will be considered effective when an updated SLA is posted either to Company's website(s), sent to Customer/Agent organizational contacts, or other multimedia forums of distribution. Customer/Agent may, upon written request, receive direct notification of changes to the SLA.