Service Level, Support, & Security Exhibit

I. Service Level

1. **Availability:** The Service will be generally available 99.9% of the time (meaning maximum 43.2 minutes a month of downtime), except as provided below. General availability will be calculated per calendar month, as follows:

$$\left[\frac{\left(\text{Total} - \text{nonexcluded} - \right)}{\text{Total} - \text{excluded}} \right] \geq 99.9\%$$

   Where:
   - "*total*" means the total number of minutes for the month
   - "*nonexcluded*" means downtime that is not *excluded*
   - "*excluded*" means the following:
     - Any planned downtime of which CloudShare gives 24 hours or more notice. CloudShare will use best efforts to schedule all planned downtime during the weekend hours from 6:00 p.m. Friday, Pacific Time, through 3:00 a.m. Monday, Pacific Time. CloudShare shall provide notice for all planned downtime.
     - Any unavailability caused by circumstances beyond CloudShare's reasonable control, including without limitation, acts of God, acts of government, flood, fire, earthquakes, civil unrest, acts of terror, strikes or other labor problems (other than those involving CloudShare employees).

2. **Responsiveness:** The use of the word "degraded" in the Severity Levels in Section II includes problems with the responsiveness of the Service. Reported cases of degradation will be investigated by CloudShare and corrected in accordance with the priorities and protocols in Section II if they are attributable to CloudShare or its ISP. CloudShare is not responsible for correction of responsiveness issues that are related to the Software's own internal responsiveness or use of the Software in excess of the contracted level of use, such as in excess of a maximum number of students identified in the Agreement; if such maximum is identified and Customer intends to make a higher level of use, notification of such expected higher level of use will not make CloudShare responsible for responsiveness associated with the higher level of use. In addition, CloudShare is not responsible for general internet connectivity problems that exist beyond CloudShare's connectivity to the internet, such as might be caused by a slow wi-fi connection at a hotel where a demonstration is given.
3. **Claims:** CloudShare will continuously monitor the performance of the Service and track its compliance with this SLA. In the event that Customer believes CloudShare is not meeting this SLA, in each instance, Customer will open a trouble ticket using CloudShare's automated facility for this purpose within three (3) days of the downtime providing CloudShare with information about when the event occurred ("Claim"), when Customer notifies CloudShare of any Claim. CloudShare will verify such Claim against CloudShare's system records. Should any periods of downtime submitted by Customer be disputed, CloudShare will provide to Customer a record of Service availability and/or responsiveness, as appropriate for the period in question. CloudShare will only provide records of system availability in response to good faith Customer Claims.
4. **Service Level Credits** will be as described in the SaaS Terms.

II. Support

CloudShare Support provides technical support for CloudShare infrastructure and application issues and inquiries, but does not include assistance for customer applications installed and configured on the CloudShare service.

The team ensures a positive experience and is available to address questions and requests.

Support is provided 365 days a year, 24 hours a day, 7 days a week, and includes provision of implementation services and hotline support. In addition, CloudShare proactively monitors and maintains the system.

Based on the worldwide services provided under the Agreement, multiple regional administrators will be assigned to manage its system (unless the implementation is large and warrants multiple managers). These people have administrator permissions and are able to configure the system. Whenever a question arises or assistance is required, the administrator can call the CloudShare support line or email the support mailbox: support@CloudShare.com.

Non-administrator users may contact CloudShare Support; however, since they are not authorized to make configuration changes, the administrator should be copied on all requests. CloudShare will use its best efforts to help any user that requires assistance.

If deemed appropriate, a vendor's end users or students using the CloudShare platform may also contact the CloudShare Support Team.

Support Process

1. Support inquiries can be initiated from any channel below.
2. A new support ticket is opened in the CloudShare support system.
3. The ticket requester receives an automatic reply acknowledging the opening of the ticket.
4. CloudShare Support provides an initial response based on the ticket severity. (Ticket severity is detailed below.)
5. CloudShare Support fixes the problem or provides an acceptable workaround to mitigate the issue.
6. CloudShare Support marks the ticket as resolved, and the ticket requester receives an email confirmation. If the requester needs to reactivate the ticket, they can reply to the email or update the ticket in the support portal.

CloudShare Support is committed to rapid response and resolution of customer support requests.

Response is defined as the amount of time required for the CloudShare CSR to process the request, investigate, duplicate or determine the nature of the problem, and respond to the customer with an action plan.

Resolution is defined as an answer, fix or satisfactory workaround to the customer ticket request.

Solution is defined as a permanent or long-term resolution to the customer ticket request, problem or question.

If, in a given case, CloudShare demonstrates to the customer that the problem is attributable to the customer's application or to the customer's actions or inactions, CloudShare will be entitled to invoice the customer on a time and materials basis at CloudShare's prevailing rates for any work performed in connection with its efforts to resolve the problem.

Severity Levels

Ticket requests are assigned priority as follows (in business days/hours, Eastern Time):

Severity	Description	Response Time	Update Time	Resolution Time
Urgent	Service is down or unavailable A critical CloudShare component is unavailable or inaccessible, resulting in total disruption of work or critical business impact.	1h	2h	4h
High	Service is operational but highly degraded Service is functional, but degraded to the point of major impact on usage to some or all users.	2h	4h	8h
Medium	Service is operational but partially degraded Service is functional, but slightly degraded for some or all users, for which an acceptable workaround or solution exists.	8h	2d	4d
Low	Minor problem or change request Inquiry regarding a routine technical issue; information requested on application capabilities, enhancement request, minor defect or missing or erroneous documentation.	1d		

We strongly urge customers to use telephone support for issues with Urgent severity.

Tickets are assigned the following statuses:

Status	Description
Open	The TR has been created and assigned.
Pending	The TR has been investigated. Initial investigation requires additional details from customer.
Solved	The TR has been closed for any of the following reasons: The customer and the CSR agree that a satisfactory resolution has been provided. CloudShare's support team has made multiple attempts to contact the customer to investigate or resolve the problem, and the customer has not responded, or the customer has not provided the information or assistance reasonably requested and required by CloudShare. For TRs submitted via email, the status may be changed to Solved when the CSR has provided a reply and is confident that the reply will resolve the issue or question without further activity required. If further investigation is needed, the customer may re-open the ticket and CloudShare Support will continue the investigation in order to arrive at a mutually acceptable resolution.
Re-opened	The TR has been re-opened because the original response or resolution provided did not resolve the issue. The CSR assigned to the service request will again pursue resolution of the problem.

Support Channels

- Support Portal: https://support.CloudShare.com
  - Knowledge Base
  - Community support
  - Create tickets
  - Review tickets and their statuses
- Phone Support
  - International: +1.650.331.3428
  - Dedicated Enterprise Support Line: +1.650.331.3417
- Email Support: support@CloudShare.com

III. Security

A. Physical Security

Facilities:
CloudShare servers are hosted at Tier III, SSAE-16, PCI DSS, or ISO 27001 compliant facilities identified in the Data Processing Exhibit. Our cage space is physically and logically separated from other data center customers. The co-location facilities are powered by redundant power, each with UPS and backup generators. CloudShare reserves the right to change or add hosting sites that meet the same level of security and reliability, including the possibility of using virtual sites such as those provided by Google, MicroSoft Azure, or Amazon Web Services.

On-Site Security:
Our data center facilities feature a secured perimeter with multi-level security zones, 24/7 manned security, CCTV video surveillance, multifactor identification with biometric access control, physical locks, and security breach alarms.

Monitoring:
All systems, networked devices, and circuits are constantly monitored by both CloudShare and the co-location providers.

Location:
CloudShare has data centers in the EU (Amsterdam), the United States (Miami) and Singapore. Customers can choose to locate their data in any of them.

B. Network Security:

Dedicated Security Team:
Our Security Team is on call 24/7 to respond to security alerts and events.

Protection:
Our network is protected by redundant layer 7 firewalls (Check Point Security blades and Fortinet's Fortigate NGFW), best-in-class router technology, secure HTTPS transport over public networks, regular audits, and network intrusion detection/prevention technologies (IDS/IPS) that monitor and block malicious traffic and network attacks.

Architecture:
Our network security architecture consists of multiple security zones of trust. More sensitive systems, like our database and backend servers, are protected in our most trusted zones.
Each environment has its own dedicated L2 segment completely separated from other environments and consequently any other Customer.
Other systems are housed in zones commensurate with their sensitivity, depending on function, information classification, and risk. Depending on the zone, additional security monitoring and access controls will apply. DMZs are utilized between the Internet, and internally, between the different zones of trust.

Network Vulnerability Scanning:
We constantly scan all traffic flowing through our networks that allows us to quickly identify potentially vulnerable systems or malicious activity coming to or from our network.

Third Party Penetration Tests:
Each year CloudShare hires a third party security expert firm to perform a wide range of penetration tests across our systems. Each finding is fixed while more severe ones are being handled within days.

Security Incident Event Management:
SIEM system (Splunk) gathers extensive logs and metrics from all network devices and services. This system creates triggers which notify our security team based on pre-determined rules, heuristics and correlated events. A response by the team soon follows.

Intrusion Detection and Prevention:
IPS is deployed in major ingress and egress junctions monitoring for potential risks. This system is configured to generate paged alerts upon incidents which are configured with dynamic thresholds when new threats are published.

DDoS Mitigation:
Apart from internal techniques and procedures, a third party contractor is being contracted on-demand to mitigate larger scale and more complex distributed attacks.

Logical Access:
Access to the CloudShare Production Network is restricted by an explicit need-to-know basis, utilizes least privilege, is frequently audited and monitored, and is controlled by our Operations Team. Employees accessing the CloudShare Production Network are required to use multiple factors of authentication.

Security Incident Response:
Employees get security incident mitigation, preventions and response process training. Escalation paths and channels of communication are updated and refreshed. When a system alert is triggered it is escalated to a 24/7 team which covers Ops, network and security.

C. Encryption:

Communications between the customer and CloudShare servers are being encrypted via HTTPS and TLS. CloudShare web application is HTTPS only while transferring files into and out of CloudShare Cloud Folders can be done via FTPS.

D. Availability and Continuity:

Uptime:
CloudShare maintains a publicly available system-status webpage that includes system availability details, scheduled maintenance, service incident history, and relevant security events.

Redundancy:
CloudShare's service is highly available and clustered in every tier to eliminate single points of failure. This includes the hardware level (Switches & Routers, Storage clusters with RAIDed arrays, Firewalls and Hypervisors) and software levels (Load balanced services and virtualized servers) and databases.

Disaster Recovery:
Our DRP plan ensures our services' availability in case of a disaster. This plan is being constantly updated, tested and practiced to achieve needed continuity.
Customers' Blueprints are backed up regularly on and off site. The Recovery Time Objective is 24 hours and the Recovery Point Objective is 24 hours.

Application Security – Secure Development:

Security training:
Annual code training for our software engineers is held and is mandatory. New engineers are trained on that before they write any code that goes into production. The training covers OWASP top security flaws, common attack vectors and our own security controls.

Database access Security controls:
Our ORM (NHibernate) layer has integrated data-scoping and data-visibility controls, preventing any possibility of cross-customer data flow regardless of attack vector. This scoping mechanism has precedence over any query or code directive.

QA:
Our code base is being tested and reviewed by our QA teams. They are also proficient with application security standards and identify, test and triage security vulnerabilities in code.

Separation of Environments:
Testing, Staging and Production environments are completely separated physically and logically from each other. No actual customer data is shared between the environments and is kept on data center premises only.

E. Application Vulnerabilities:

Dynamic Vulnerability Scanning:
We employ a number of third-party, qualified security tools to continuously scan our application. CloudShare is scanned weekly against the OWASP Top 10 security flaws. We maintain a part time dedicated in-house product security team to test and work with engineering teams to remediate any discovered issues.

Static Code Analysis:
Our source code repositories for our platform are continuously scanned for security issues via our integrated static analysis tooling

Security Penetration Testing:
In addition to our extensive internal scanning and testing program, each year CloudShare employs third-party security experts to perform detailed penetration tests on different parts of the application.

F. Product Security Features:

Authentication Options:
Users of the platform can choose to authenticate via user-password with configurable password policy (see below), or via oAuth SSO with LinkedIn or Facebook, or via any SAML based SSO service (with support for SAML 1.x and 2.x), or Microsoft ADFS integration for SSO.

Configurable Password Policy:
CloudShare enforces strong password polices to reduce the risk of brute force or dictionary attacks.

Secure Credential Storage:
CloudShare follows secure credential storage best practices by never storing passwords in human readable format, and only as the result of a secure, salted, one-way hash.

API Security & Authentication:
CloudShare API is SSL-only and you must be a verified user to make API requests. API authentication and

authorization is done via HMAC based Authorization Request Header involving the user API Key, API ID, salted session ID and timestamp – to prevent any playback or MitM attacks.

Access Privileges & Roles:
Access to data within your CloudShare account is governed by access rights, and the customer can define granular access privileges. CloudShare has various permission levels for users accessing your CloudShare Environment, and this can be broken down into an overall Account Manager, Project Manager, Team Manager, Team Member, and End User.

IP Restrictions:
CloudShare can be configured to only allow access from specific IP address ranges the customer defines. This can be applied at the application level by our support personnel upon request. However, IP spoofing and VPNs remain a concern with regard to the effectiveness of such restrictions.

G. Security Awareness:

Policies:
CloudShare has developed a comprehensive set of security policies covering a range of topics. These policies are shared with, and made available to, all employees and contractors with access to CloudShare information assets.

Training:
All new employees attend Security Awareness Training, and the Security Team provides security awareness updates via email, Slack channel, and in presentations during internal meetings.

Background Checks:
CloudShare performs background checks on all new employees in accordance with local laws. The background check includes Criminal, Education, and Employment verification.

Confidentiality Agreements:
All new hires are screened through the hiring process and required to sign Non-Disclosure and Confidentiality agreements.