

## Qube Learning Service Level Agreement Performance, Security & Support

---

### Overview

Qube understands that the confidentiality, integrity, and availability of our customers' information are vital to their business operations and our own success. We use a multi-layered approach to protect that key information, constantly monitoring and improving our application, systems, and processes to meet the growing demands and challenges of security.

Our service is collocated in dedicated spaces at top-tier data centers. These facilities provide carrier-level support, including:

#### Access control and physical security

- 24-hour manned security
- Dedicated concrete-walled Data Center rooms
- Computing equipment in access-controlled steel cages
- Building engineered for local seismic, storm, and flood risks
- Tracking of asset removal

#### Environmental controls

- Humidity and temperature control
- Redundant (N+1) cooling system

#### Power

- Underground utility power feed
- Redundant (N+1) CPS/UPS systems
- Redundant power distribution units (PDUs)
- Redundant (N+1) diesel generators with on-site diesel fuel storage

#### Network

- Concrete vaults for fiber entry
- Redundant internal networks
- Network neutral; connects to all major carriers and located near major Internet hubs
- High bandwidth capacity

#### Fire detection and suppression

- VESDA (very early smoke detection apparatus)
- Dual-alarmed, dual-interlock, multi-zone, pre-action dry pipe water-based fire suppression

## Secure transmission and sessions

Connection to the Qube environment is via SSL 3.0/TLS 1.0, using global step-up certificates from VeriSign, ensuring that our users have a secure connection from their browsers to our service.

Qube Learning uses advanced technology for Internet security. When you access Qube's SaaS platform using Secure Socket Layer (SSL) technology, username and password encryption is provided in transit and at rest, as well as server authentication to ensure that your data is safe, secure, and available only to registered users. Qube equipment, applications and data are located in physically secure facilities that require badge access at all times.

Qube services require that each valid user in your organization possess a unique user name and password that must be entered each time a user logs into our servers. We utilize a state-of-the-art secure server environment that uses firewalls and other advanced technologies to prevent interference or access from outside intruders.

### Network protection

- Perimeter firewalls and edge routers block unused protocols
- Internal firewalls segregate traffic between the application and database tiers
- Intrusion detection sensors throughout the internal network report events to a security event management system for logging, alerts, and reports
- A third-party service provider continuously scans the network externally and alerts changes in baseline configuration

### Internal and Third-party testing and assessments

Qube tests all code for security vulnerabilities before release, and regularly scans our network and systems for vulnerabilities. Third-party assessments are also conducted regularly:

- Application vulnerability threat assessments
- Network vulnerability threat assessments
- Selected penetration testing and code review
- Security control framework review and testing

### Security Monitoring

Our Information Security department monitors notification from various sources and alerts from internal systems to identify and manage threats.

## Qube System Performance

Qube Learning is committed to the highest level of system performance and uptime for our customers. We achieve 99.9% website uptime and system availability, excluding downtime for scheduled maintenance. We utilize redundant, geographically distributed data centers and servers that deliver fault tolerant services for all Qube Learning SaaS customers. Qube is committed to the highest level of system service we can provide. We back our commitment with our promise to utilize best efforts to provide 24-by-7 availability of all Qube Products, Services and client Deliverables.

### Backups

- All data are backed up to disks at each data center, on a combination schedule of incremental and full backups
- The backups are transferred electronically offsite and are preserved for six months

### Disaster Recovery

- The Qube service performs real-time replication to disk at each data center, and near real-time data replication between the production data center and the disaster recovery center
- Data are transmitted across encrypted links
- Disaster recovery tests verify our projected recovery times and the integrity of the customer data

## End User Support

Our customers may select from 3 levels of support to best meet service and support requirements: Silver, Gold and Platinum Support. Our support levels are designed to meet the business requirements of enterprise end-user customers as well our value-added resellers, distributors and their respective end-users.

Summary features and provisions included with Silver, Gold and Platinum Support are presented in below, and are provided on an annual basis to clients with current Qube Licenses and/or End-user License Subscriptions.

### Silver Support: Level 1

- Access to the Qube User FAQs

### Gold Support: Level 2

- Silver Support plus...
- 24-hour turnaround on support email from the end user
- Telephone support between hours of 8am-5pm PST with a single point of Client contact
- Priority resolution over Silver Support customers
- Access to the Qube Support Site

### Platinum Support: Level 3

- Gold Support plus...
- Telephone support between hours of 8am-5pm PST with all users
- Telephone support between hours of 8am-5pm PST with a multiple of learner administration contacts at Client
- IM access by multiple learner administrators
- Priority resolution over Silver & Gold Support customers

If you have additional questions, please contact us at [Sales@Qube.com](mailto:Sales@Qube.com) or 415-464-8880.