Contents

1. Service Level Objective (SLO) ........................................................................................................ 1

2. Availability and Reliability ........................................................................................................... 1
   2.1 Operating Hours ......................................................................................................................... 1
   2.2 Redundancy ............................................................................................................................... 2
   2.3 Fault Management .................................................................................................................... 2
   2.4 Updates ................................................................................................................................... 2
   2.5 Support .................................................................................................................................... 2
   2.6 Data Deletion ............................................................................................................................ 2
   2.7 DLP (Data Loss Prevention) & Disaster Recovery Plan ............................................................... 3

3. CSIRT ........................................................................................................................................... 4
   3.1 Internal security management policies ....................................................................................... 5
   3.2 Human Error Prevention Management Systems ........................................................................... 6

4. Data Encryption ............................................................................................................................. 7
   4.1 Data in Transit Encryption .......................................................................................................... 7
   4.2 Data at Rest Encryption ............................................................................................................. 8

5. Server Security .............................................................................................................................. 8

6. Vulnerability & Penetration Testing ............................................................................................ 9
   6.1 Collecting Information of Third Party OS and Software Vulnerability ......................................... 9
   6.2 Detection and Prevention of Any Possible Fault or Failure ......................................................... 9

7. Product-Based Secure Access Features ....................................................................................... 11
   7.1 Sub-domain and login page ....................................................................................................... 11
   7.2 Multi-Factor Authentication (MFA) .......................................................................................... 12
   7.3 Login and Password Policies .................................................................................................... 15
   7.4 Audit Log .................................................................................................................................. 16

8. Compliance ................................................................................................................................... 16
1. Service Level Objective (SLO)

We provide 24/7 monitoring and have set our Service Level Objectives for our infrastructure to provide the most reliable service to our Kintone.com clients.

- Uptime rate: 99.99%
- Response time: within 4 seconds
- Recovery time: within 10 mins
- Access log storage time: 1 year online

Historical Uptime Results

<table>
<thead>
<tr>
<th>Month</th>
<th>Uptime</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sept 2018</td>
<td>99.852%</td>
</tr>
<tr>
<td>Aug 2018</td>
<td>99.956%</td>
</tr>
<tr>
<td>July 2018</td>
<td>99.994%</td>
</tr>
<tr>
<td>June 2018</td>
<td>99.993%</td>
</tr>
<tr>
<td>May 2018</td>
<td>99.962%</td>
</tr>
<tr>
<td>Apr 2018</td>
<td>99.979%</td>
</tr>
</tbody>
</table>

Click here to download the full uptime report.

2. Availability and Reliability

2.1 Operating Hours

Our platform operates 24 hours a day, 365 days a year (excluding regular maintenance), with regular backup and redundancy built-in.

2.1.1 Regular maintenance

When and if necessary, regular maintenance occurs the second Friday of the month, unless the 1st of the month lands on a Saturday or Sunday – in which case it will be conducted on the first Friday.

2.1.2 Occasional maintenance
If there’s a need for occasional maintenance, at least 1 week advanced notification will be given.

2.2 Redundancy

Kintone operates a fully redundant system which includes servers, networks, storage, and data (Hyperlink to 4 DLP (Data Loss Prevention)).

2.3 Fault Management

Kintone has developed and maintains an extensive Fault Management system, which is comprised of a set of functions that prevent, detect, and correct malfunctions, and initiate recovery automatically within the Kintone cloud platform.

2.4 Updates

As a policy, Kintone platform and product updates are propagated across the platform at the same time for all clients.

2.5 Support

2.5.1 Support Hours

Standard support hours are Monday through Friday 9 am – 5:00 pm PST. More detailed Support SLA can be found here.

2.5.2 Support Contact

Support phone number: 415-692-6546  Support e-mail: support@kintone.com

2.6 Data Deletion

All data stored within a customer account sub-domain shall be deleted 30 days after the termination of an account. All backup data shall be completely deleted approximately 2 weeks after the initial data deletion.
2.7  DLP (Data Loss Prevention) & Disaster Recovery Plan

“Square” is our backup system designed to protect clients' data, and includes the following locations and storage server sets:

- 2 Regions (East and West Japan)
- 4 storage servers (3 storage servers in East Japan and 1 storage server in West Japan)

2.7.1  Hard Disk Redundancy (RAID 6)

The Storage Server set has 12 hard disks per server. 10 of the 12 hard disks were implemented with RAID6. RAID6 allows for two disk failures within the RAID set before any data is lost. The 2 additional hard disks are prepared as “hot spares”.

2.7.2  Mirroring (RAID 1)

Customer data is updated to the storage server and the replication storage server simultaneously. This RAID1 ‘mirroring’ system protects against the loss of data due to storage server failures because of hard disk failure or power supply failure.
2.7.3 14-day Backup Data with Backup Server

The East Japan Data Center (EJDC) maintains storage servers, replication storage servers and backup storage servers. The most recent 14-days of data is stored there. Backup data beginning from one day prior to the current day can be restored. Restoration capabilities are tested daily.

2.7.4 2 Regions for Remote Backup “BCP”

The West Japan Data Center (WJDC) has remote backup storage servers in case of any catastrophic event affecting the EJDC. All backup data stored in the backup storage servers in EJDC are automatically backed up to the WJDC.

2.7.5 Data Centers Meet FISC Standards for Most Reliable

Data Centers Meet Tier 4 FISC Facility Safety Standards

The data centers that house and manage Cybozu.com servers, including Kintone.com, comply with the requirements of the The Center for Financial Industry Information Systems (FISC) Facility Safety Standards, considered one of the strictest compliance agencies in Japan. (Cybozu Inc is Kintone’s parent company).

The data centers meet Tier 4 specifications, the highest level, for most of the categories in the Data Center Facility Standard regulated by the Japan Data Center Association.

2.7.6 A+ Rating for Secure Network Encryption (SSL/TLS)

As detailed below in Section 5, Server Security, Kintone maintains an A+ rating for server security by Qualysys, the leading provider of infrastructure security compliance solutions.

2.7.7 Power Supply and Network Redundancy

We provide Power Supply and Network redundancy to help reduce the chance for disaster-related damage.

2.7.8 Hard Disk Physical Destruction

After service, retired hard disks shall be physically destroyed to prevent any possible information leakage from such disks.

3. CSIRT
Cy-SIRT (Cybozu Computer Security Incident Response Team) is an in-house expert security group created to prepare against and handle any Security incidents. Cy-SIRT helps create policies to protect against threats and responds rapidly and in real-time to identify, contain, and eradicate threats as they arise.

3.1 Internal security management policies

3.1.1 Only highly access-restricted devices can be connected to the data center
3.1.2 Product environment and testing environment shall be separated

3.1.3 Infrastructure operations system shall be operated only by authorized members within a dedicated access control room

3.2 Human Error Prevention Management Systems

3.2.1 Service Updates

To prevent Human Error, systems shall be tested and verified several times before updates occur.

Product development → Quality control check → In-company loading check → Update rehearsal → Final update
3.2.2 Separation of product environment and remote backup environment

The Product Environment and Remote Backup Environment shall be separated and prohibited to operate simultaneously.

When data is deleted in Product Environment, that data can not be deleted at the same time in the Backup Environment.

3.2.3 Automation

Automation is implemented to minimize failure probabilities caused by human error.

Kintone.com promotes automation wherever possible instead of manual system operations. For example, the creation of a client sub-domain environments and adding and cancelling services are all automated.

3.2.4 Automatic Logging of Manual Operations

Manual operations performed by humans shall be done while following prescriptive manuals.

All such manual operation activities however, shall be logged automatically.

3.2.5 Working alone is prohibited

In an emergency case, humans operating the system without a manual is permitted.

However, even in an emergency case, working alone is prohibited as 2 or more authorized technicians must work together.

4. Data Encryption

Kintone encrypts all data both in transit and at rest. Learn more.

4.1 Data in Transit Encryption

All data is encrypted as it moves between our servers and your web browser.

The Kintone service is offered only with SSL connections, and provides optional IP address connectivity restrictions, 2-Factor Authentication and basic authentication.
4.2 Data at Rest Encryption

We also encrypt all data stored on our servers.

Our Data at Rest Encryption encrypts all inactive data stored within our servers. Kintone uses a 512 bit key length encryption scheme, the same used in Windows BitLocker and OS X FileVault.

5. Server Security

Our Server Security level is confirmed as A+ by Qualys’ SSL Labs per below.

Source: Qualys SSL labs

A+ rating by Qualys SSL Labs for cloud server security

We deploy the latest SSL/TLS (1.2 or higher) technology

- HTTP Strict Transport Security (HSTS)
- Perfect Forward Secrecy (PFS)
- SHA-2 certificate
6. Vulnerability & Penetration Testing

Kintone has third-party vulnerability testing auditors such as Vulnerability Defense Laboratory perform vulnerability/penetration audits on our platform on a semi-annual or as needed (when any major updates occur) basis.

6.1 Collecting Information of Third Party OS and Software Vulnerability

A vulnerability assessment is the process of identifying and quantifying security vulnerabilities in a software environment.

A penetration test simulates the actions of an external and/or internal cyber attacker that aims to breach the information security of the organization.


6.2 Detection and Prevention of Any Possible Fault or Failure

6.2.1 An autonomous fault management system

Kintone.com has an “autonomous decentralized agent system’ called “Tsukuyomi”, a prophet in Japanese mythology who can predict future events. Appropriately, this system is designed to prevent, detect, and correct faults or failures and initiate recovery in the Kintone servers.

In the “Tsukuyomi” system, Servers monitor each other to detect faults or failures. After detection, the automatic recovery process instantly replaces the fault server to the spare server. If multiple servers go down, then special recovery plan will be initiated.
6.2.2 DoS, DDoS attack protection and mitigation

Denial of Service (DoS) attacks are common attacks wherein a huge volume of traffic (TCP, UDP and ICPM packets) is sent to a specific sub-domain (URL) within a very short time. In such instances, the tenant’s sub-domain will be automatically shut down to protect the rest of the tenants in Kintone’s multi-tenant system.

Network monitoring systems and intrusion detection/prevention systems continuously monitor the Kintone system.
7. Product-Based Secure Access Features

7.1 Sub-domain and login page

7.1.1 Customers have unique sub-domains for their log-ins option

- IP address restriction / 2-Factor Authentication option
- Unique login names per account

7.1.2 Login page

- Images and company name can be changed for destination confirmation used to counter phishing attempts
7.2 Multi-Factor Authentication (MFA)

7.2.1 Basic authentication – Free

– Sets up an extra login page before accessing the sub-domain (users enter a shared login name and password)

– Note: The password should be changed if a user leaves the company

7.2.2 IP address restrictions – Free

– Restricts access from IP addresses that are not listed
– Can be used together with Basic Authentication and Client Certificate Authentication to provide individual device-based access

**Secure access setting screen**

Secure access settings can be reviewed and set in the Security & Authentication admin control panel displayed below. Setting Changes are reflected immediately.

![Secure access setting screen](image)

### 7.2.3 Secure access through client certificates

– Client certificates can be issued for individual users to install onto their devices in order to gain a unique access gateway through the IP fencing restriction setting.

– Certificates can be set to expire at set time intervals and re-issued easily.

4 Examples of Security Settings Options with the Kintone.com /Cybozu.com cloud platform
I want to easily strengthen security

- IP address restrictions: Reject all
- Basic authentication: On

I want to restrict accessibility only to the company

- IP address restrictions: Partial permission
- Basic authentication: Off

I want to access from outside while retaining the smoothness of internal access

- IP address restrictions: Partial permission
- Basic authentication: On
7.3 Login and Password Policies

7.3.1 Password settings

The following is a list of password settings that can be configured when setting up a Kintone account.

- Password Character length
- Password Character complexity
- Password reuse policy
- Password expiration policy

7.3.2 Logins

7.3.2.1 Account lockout policy

- Account lockout threshold – number of incorrect attempts
- Account lockout duration – length of time the lockout will occur.

7.3.2.2 Automatic login policy

- Enable/disable auto login
- Enable auto login duration
7.4 Audit Log

You can browse and download the audit log of operations such as logins, modifications, file downloads, etc. Custom audit log settings can also be set to initiate notification emails.

<table>
<thead>
<tr>
<th>Date</th>
<th>Connection source</th>
<th>User</th>
<th>Service</th>
<th>Module</th>
<th>Action</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015-03-05 14:49:05</td>
<td>XX.XXX.XXX.XXX</td>
<td>sato</td>
<td>Garoon</td>
<td>Basic system</td>
<td>login</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>2015-03-05 14:37:45</td>
<td>XX.XXX.XXX.XXX</td>
<td>sato</td>
<td>Garoon</td>
<td>Basic system</td>
<td>login</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>2015-03-05 14:37:41</td>
<td>XX.XXX.XXX.XXX</td>
<td>sato</td>
<td>Garoon</td>
<td>Messages</td>
<td>login</td>
<td>FAILED</td>
</tr>
<tr>
<td>2015-03-05 14:37:41</td>
<td>XX.XXX.XXX.XXX</td>
<td>sato</td>
<td>Garoon</td>
<td>Basic system</td>
<td>login</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>2015-03-05 14:32:09</td>
<td>XX.XXX.XXX.XXX</td>
<td>sato</td>
<td>Garoon</td>
<td>To-Do List</td>
<td>modify</td>
<td>SUCCESS</td>
</tr>
<tr>
<td>2015-03-05 14:41:22</td>
<td>XX.XXX.XXX.XXX</td>
<td>sato</td>
<td>Garoon</td>
<td>Bulletin Board</td>
<td>create</td>
<td>SUCCESS</td>
</tr>
</tbody>
</table>

8. Compliance

Information Security Management System (ISMS)

Cybozu Inc’s Cybozu.com and Kintone.com cloud infrastructure has achieved ISO 27001 certification of our Information Security Management System (ISMS) covering our infrastructure, data centers, and services.

【Certification registration】

Design, construction and maintenance of operational infrastructure of a cloud service developed in-house.

Initial ISO 27001 certification registration date was November 10th, 2011 with subsequent audit updates occurring since.
ISO 27001 certified registration number IS 577142

**Information Security Management System (FISC)**

As mentioned above, the data centers the Kintone.com cloud is currently operating from comply with The Center for Financial Industry Information Systems (FISC) Facility Safety Standards, considered one of the strictest compliance agencies in Japan.

In fact, the data centers meet Tier 4 specifications, the highest level, for most of the categories in the Data Center Facility Standards as regulated by the Japan Data Center Association.