Cloud Service Provider Contact Information

Company Name: Fujitsu Asia Pte Ltd
Primary Address: Nexus @ one north | 1 Fusionopolis Link, #04-01 Singapore 138542 | North Lobby
Web Address: 
Contact Name: How Kar Fai
Contact Number: +65 97673023

Cloud Service Provider Background

Service Model: VM own by user
Deployment model: Private Cloud

Tier Level
Remark

Certificate Number

Company Stamp & Signature
Certification Body Contact Information
Company name: TÜV SÜD PSB Pte Ltd
Web address: www.tuv-sud-psb.sg
Contact name: +65 6779 7777, MS Department
Contact number: +65 6778 7777

Company Stamp & Signature:

TÜV SÜD PSB Pte Ltd
1 Science Park Drive
Singapore 118221
Tel: +65 6779 7777, FAX: +65 6779 7088
Co. Reg. No.: 199002667R
## Legal & Compliance

### 1 Right to audit

The user has the right to audit:

- [x] Virtual machine instances owned by the user
- [ ] Network facilities
- [ ] Compliance with applicable standards
- [ ] Technical controls
- [ ] Policies and governance
- [ ] Data centre facilities
- [x] Others: ISAE report will be send to customers
- [ ] None

Regulators recognised by Singapore law have the right to audit:

- [ ] Virtual machine instances owned by the user
- [ ] Network facilities
- [ ] Compliance with applicable standards
- [ ] Technical controls
- [ ] Policies and governance
- [ ] Data centre facilities
- [ ] Other's
- [ ] None

Audit / assessment reports that can be made available on request:

- [x] Penetration test
- [ ] Threat and vulnerability risk assessment
- [x] Vulnerability scan
- [ ] Audit reports (e.g. Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organisation)

### 2 Compliance

The following guidelines / standards / regulations are adhered to:

- [ ] Singapore Personal Data Protection Act
- [ ] ISO / IEC 27001
| **ISO 9000** |  |
| **ISO / IEC 20000** |  |
| **CSA Open Certification Framework** |  |
| **PCI-DSS** |  |
| **Others** | **ISAE3402** |

### Data Control

3. **Data ownership**

All data on the cloud service is owned by the cloud user except for:

- The cloud User retains the ownership on the derived data or attributes of cloud usage except for the following:
  - Advertising or marketing
  - Statistics analysis on usage
  - Others

4. **Data retention**

Data deleted by the user is retained as follows:

- Minimum data retention period is: 30 days snapshot retention. If needed will need to restore VM for data retrieval
- Maximum data retention period is:
- Deleted immediately
- Log data is retained for a period of:
  - Minimum data retention period as follows: 30 days snapshot retention. If needed will need to restore VM for data retrieval
  - Maximum data retention period is:
  - Not retained
- User data is retained for a period of:
  - Minimum data retention period is: 30 days snapshot retention. If needed will need to restore VM for data retrieval
  - Maximum data retention period is:
  - Not retained
- The following types of data are available for download by the cloud user:
  - Log data
  - Other

5. **Data sovereignty**

The primary data locations are:

- Singapore
- Asia Pacific
- Europe
<table>
<thead>
<tr>
<th>United States</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>The backup data locations are:</td>
<td></td>
</tr>
<tr>
<td>☑ Singapore</td>
<td></td>
</tr>
<tr>
<td>☐ Asia Pacific</td>
<td></td>
</tr>
<tr>
<td>☐ Europe</td>
<td></td>
</tr>
<tr>
<td>☐ United States</td>
<td></td>
</tr>
<tr>
<td>☐ Other</td>
<td></td>
</tr>
</tbody>
</table>

No. of countries in which data centres are operated: [ ]

The user's data stored in the cloud environment will never leave the locations specified in item 5:

☑ Yes

☐ Yes, except as required by law

☐ Yes, except as noted:

☐ No

User's consent is required prior to transferring data to a location not specified in item 5 or a third party:

☑ Yes

☐ Yes, except as required by law

☐ Yes, except as noted:

☐ No

Note: Cloud users are responsible for determining the impact of data protection and data sovereignty....

6 Non-disclosure

☑ Non-disclosure agreement template can be provided by Cloud Service Provider

☑ Cloud Service Provider may use customer's NDA (pending legal review)

Provider Performance

7 Availability

For each cloud service offered, CSP should disclose relevant numbers)

The committed network uptime is:

☐ 6

☐ Varies according to price plan

The committed system uptime is:
<table>
<thead>
<tr>
<th>9</th>
<th>99.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td>Varies according to price plan</td>
</tr>
</tbody>
</table>

The cloud environment has the following single points of failure:

- None

8 **BCP / DR**

- ✔ Disaster recovery protection
- ✔ Backup and restore service
- ○ User selectable backup plans
- ○ Escrow arrangements
- ○ No BCP / DR is available
- ○ RPO
- ○ RTO
- ○ Others, please specify

9 **Liability**

The following terms are available for the users on failure of the provider to meet the service commitment:

- Network failure
- Infrastructure failure
- Virtual machine instance failure
- Migrations
- Unscheduled downtime
- Database failure
- Monitoring failure

**Service Support**

The Cloud Service Provider has established the following for changes, migrations, downtime, and other potential interruptions to cloud services:
<table>
<thead>
<tr>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication plan and procedures for proactive notification</td>
</tr>
<tr>
<td>Assistance in migration to new services when legacy solutions are discontinued</td>
</tr>
<tr>
<td>Ability to remain on old versions for a defined time period</td>
</tr>
<tr>
<td>Ability to choose timing of impact</td>
</tr>
</tbody>
</table>

**Self-service provisioning and management portal**

Provide self-service provisioning and management portal for users to manage cloud services:

- [ ] No
- [ ] If yes, describe the functions of the self-service provisioning and management portal provided:
  - [ ] Allow role-based access control (RBAC)
  - [ ] Manage resource pools (e.g., VMs, storage, and network) and service templates
  - [ ] Track and manage the lifecycle of each service
  - [ ] Track consumption of services
  - [ ] Other

**Incident and problem management**

Delivery mode of support:

- [ ] Access via email
- [ ] Access via portal
- [ ] Access via phone support
- [ ] Direct access to support engineers

Availability of support:

- [ ] 24 x 7
- [ ] During office hours support, please specify the hours of operations: 
- [ ] After office hours support, please specify the hours of operations: 

Service response time:

The following are available to users upon request:

- [ ] Permanent access to audit records of customer instances
- [ ] Incident management assistance

Incident response time:

Mean time to repair on detection of faults:
### Billing

The following billing modes are available (please elaborate granularity of charges and measurements):

- [ ] Pay per usage, up to per minute/hour/day/month for compute/storage for IaaS/PaaS, and per user per hour/day/month/year for SaaS
- [ ] Fixed pricing monthly (up to yearly/monthly/day weekly)
- [ ] Other pricing model
- [ ] Not disclosed
- [ ] Available billing history: [ ] months

### Data Portability

**Importable VM formats:** VMDK separate charging

**Downloadable formats:** VMDK separate charging

**Supported operating systems:** Windows 2008/2012, RHEL 5/6/7

**Language versions of supported operating systems:** English

**Supported database formats:**

**API:**

- [ ] Common
- [ ] Customised

**Upon service termination, data is available through:**

- [ ] Physical media
- [ ] Standard methods as described above
- [ ] Other methods

### Access

**Type of access to the service is through:**

- [ ] Public access
- [ ] Private access (e.g. VPN, dedicated link)
- [ ] IPv6 access is supported
- [ ] Other access methods

**Public access speed (shared bandwidth) in Mbps:**

### User Management

- [ ] Identity management
- [ ] Role-based access control
- [ ] Federated access model
- [ ] Integration with identity management solutions
- [ ] Others
17 Lifecycle

The cloud user may select the following for service upgrades and changes:

- [ ] Automatic provisioning
- [x] User customisable provisioning

**Security configuration**

18 **enforcement checks**

Security configuration enforcement checks are performed:

- [x] Manually
- [ ] Using automated tools

How often are enforcement check being performed to ensure all security configurations are applied?

19 **Multi-tenancy**

- [ ] Distinct physical hosts
- [ ] Distinct physical network infrastructure
- [x] Virtual instance grouping
- [ ] User definable security domains
- [x] User customisable firewall
- [x] User definable access policies

**Service Elasticity**

20 **Capacity elasticity**

The following capacity elasticity options are available:

- [ ] Programmatic interface to scale up or down
- [ ] Mean time to start and end new virtual instances
- [x] Alerts to be sent for unusual high usage
- [ ] Minimum performance during peak periods
- [ ] Minimum duration to scale up computing resources
- [ ] Minimum additional capacity guaranteed per account

**Network resiliency and elasticity**

The following network resiliency and elasticity options are available:

- [x] Redundant Internet connectivity links
- [ ] Redundant Internal connectivity
- [ ] Selectable bandwidth up to \( \text{Mbps} \)
- [ ] Maximum usable IPs
- [ ] Load Balancing Ports
- [x] Load balancing protocols
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-DDoS protection systems or services</td>
<td></td>
</tr>
<tr>
<td>Defence-in-depth mechanisms, please specify:</td>
<td></td>
</tr>
<tr>
<td>Network traffic isolation, please specify:</td>
<td></td>
</tr>
<tr>
<td>Shared or dedicated bandwidth, please specify:</td>
<td></td>
</tr>
<tr>
<td>QoS traffic control services</td>
<td></td>
</tr>
<tr>
<td>Alerts to be sent for unusual high usage</td>
<td></td>
</tr>
<tr>
<td>Minimum performance during peak periods</td>
<td></td>
</tr>
<tr>
<td>Minimum period to scale up network throughput</td>
<td></td>
</tr>
</tbody>
</table>

**Storage redundancy and elasticity**

The following storage redundancy and elasticity options are available:

- Redundant storage connectivity links within each data centre
- Redundant storage connectivity links between data centres belonging to the same cloud
- Storage traffic isolation, please specify:
- Shared or dedicated storage network bandwidth, please specify:
- Quality of service storage traffic control services
- Maximum storage capacity for entire cloud, please specify:
- Maximum storage capacity for single user, please specify:
- Maximum expandable storage, please specify:
- Alerts to be sent for unusual high usage
- Minimum storage I/O performance during peak periods
- Minimum period to scale up storage I/O throughput