Annex A (normative)

Cloud Service Provider Disclosure

The form is to be completed for each cloud service provided. For questions not applicable or not disclosed, indicate accordingly in the remarks.

Cloud Service Provider Contact Information:

Company name: RMA Infoworks Pte. Ltd.

Primary address: 200 Jalan Sultan

#03-38

Singapore 199018

Web address: www.rmainfoworks.com.sg

Contact name: Mick Tan

Contact number: 64941522

Company Chop: Company Representative Signature:

Certification Body Contact Information:

Company name: SOCOTEC Certification International

Web address: www.socotec-certification-international.com

Contact name: John Cheong

Contact email:cheong.Yuen-Chun@socotec.com

Company Chop: Lead Auditor Signature:

Cloud Service Provider Background

Overview of service offering:

We provide cloud storage and data management services to customers globally.

Service model:

- ☐ Virtual machine instances owned by the user
- ☐ Network facilities
- ☒ Compliance with applicable standards Deployment model:

Deployment model:

- ☐ Private cloud
- ☐ Community cloud
- ☐ Hybrid Cloud
- ☒ Public cloud

Tier:

- ☒ Level 1
- ☐ Level 2
- ☐ Level 3

Legal and Compliance

1. Right to audit

The user has 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 (Upon request)
- ☐ Others _____
- ☐ 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

☐ Others _____

☐ None

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

☒ Penetration test

☒ Threat and vulnerability risk assessment

☒ 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 _ISO37001_____

Data Control

3. Data ownership

All data on the cloud service is owned by the cloud user except for: Intellectual Property Of Cloud Platform

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: _____

☐ Maximum data retention period is: _____

☒ Deleted immediately

Log data is retained for a period of:

☐ Minimum data retention period as follows: _____

☐ Maximum data retention period is: _____

☐ Not retained

☐ User data is retained for a period of:

☐ Minimum data retention period is: _____

☐ 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_____

☐ United States

☐ Other _____

The backup data locations are:

☒ Singapore

☐ Asia Pacific_____

☐ Europe_____

☐ United States

☐ Other _____

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 laws on the locations where data is stored. In addition, users should understand the risks associated with relevant laws that may allow for law enforcement or other government access to data in-transit or storage with Cloud Service Providers.

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

The committed network uptime is:

☐ _____%

☒ Varies according to price plan

The committed system uptime is:

☐ _____%

☒ Varies according to price plan

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_Up to 24 hours__

☒ RTO_Within 8 hours_____

☐ 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

☐ Liability: _____

☐ Infrastructure failure

☐ Liability: _____

☐ Virtual machine instance failure

☐ Liability:_____

☐ Migrations

☐ Liability:_____

☐ Unscheduled downtime

☐ Liability:_____

☐ Database failure

☐ Liability:_____

☐ Monitoring failure

☐ Liability:_____

Service Support

10. Change management

The Cloud Service Provider has established the following for changes, migrations, downtime, and other potential interruptions to cloud services:

- [x] Communication plan and procedures for proactive notification
- [x] Assistance in migration to new services when legacy solutions are discontinued
- [ ] Ability to remain on old versions for a defined time period
- [ ] Ability to choose timing of impact

11. Self-service provisioning and management portal

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

- [ ] Yes
- [x] 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
- [ ] Others:_____

12. Incident and problem management

Delivery mode of support:

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

Availability of support:

- [ ] 24 x 7
- [x] During office hours support, please specify the hours of operations: _09:00 to 18:00 hours_
- [ ] 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: _____4 hours_____

Mean time to repair on detection of faults: _____

13. Billing

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

☐ Pay per usage _____ (up to per min/hour/day/month for compute/storage for IaaS/PaaS, and per user per hour/day/month/year for SaaS)

☒ Fixed pricing_____(up to yearly/monthly/daily)

☐ Other pricing model_____

☐ Not disclosed

☐ Available billing history: _____Months

14. Data portability

Importable VM formats: _____

Downloadable formats: _____

Supported operating systems: _____

Language versions of supported operating systems:

_____

Supported database formats: _____

API:

☐ Common _____

☐ Customised _____

Upon service termination, data is available through:

☒ Physical media

☐ Standard methods as described above

☐ Other methods _____

15. Access Type of access to the service is through:

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

Public access speed (shared bandwidth) in Mbps: _____

16. User management

- [ ] Identity management
- [x] 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 Configurations

18. Security configuration enforcement checks

Security configuration enforcement checks are performed:

- [x] Manually
- [ ] Using automated tools

How often are enforcement checks 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

☐ User customisable firewall

☐ 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 _____

☒ 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 _____ (number of cores and GB memory)

21. Network resiliency and elasticity

The following network resiliency and elasticity options are available:

☐ Redundant Internet connectivity links

☐ Redundant Internal connectivity

☐ Selectable bandwidth up to _____Mbps

☒ Maximum usable IPs _____2_____

☐ Load balancing ports_____

☐ Load balancing protocols_____

☐ Anti-DDOS protection systems or services

☐ Defence-in-depth mechanisms, please specify: _____

☐ Network traffic isolation, please specify: ISOLATED AND DEDICATED SWITCHES

☐ Shared or dedicated bandwidth, please specify: _____

☐ QoS traffic control services

☐ Alerts to be sent for unusual high usage

☐ Minimum performance during peak periods_____

☐ Minimum period to scale up network throughput _____

22. 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: ISOLATED AND DEDICATED SWITCHES
- ☐ Shared or dedicated storage network bandwidth, please specify:_____
- ☐ Quality of service storage traffic control services
- ☒ Maximum storage capacity for entire cloud, please specify: 60 TB_____
- ☒ Maximum storage capacity for single user, please specify: SUPPORT UP TO 2TB
- ☐ 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 _____