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: INFO-TECH SYSTEMS INTEGRATORS PTE LTD
Primary address: 30 Kallang Place, #07-14,
                Singapore 339159
Web address:   www.info-tech.com.sg
Contact name:  Torrance Yeoh / Lim Yik Hai
Contact number: +65 81261021 / +65 91882636

Company Chop: Company Representative Signature:

Certification Body Contact Information:

Company name: SOCOTEC Certification Singapore Pte Ltd
Web address:   www.socotec-certification-international.sg
Contact name:  John Choo
Contact email:  cheong.juan-chun@socotec.com

Company Chop: Lead Auditor Signature:
Cloud Service Provider Background

Overview of service offering:

Info-tech offers Complete Cloud HR Software including industry first innovative Face Recognition with GPS Mobile / Tablet App for staff Attendance. Info-tech cloud HR Software has simple & user friendly yet comprehensive Attendance, Payroll, Leave, Claim, Appraisal & Job costing software modules.

Info-tech mobile app supports iOS & Android with “Your HR matters on the go” slogan. Employees can do attendance, apply leave, view their payslip, tax forms & any messages from HR. Managers will be updated with live push notification of staff lateness, absent & Leave.

Products and services provided by Info-Tech are as follows

- Mobile Attendance App
  Industry first Mobile attendance App with Face Recognition & GPS integrated with complete HR Software
- Time Attendance Software
  Real time sync employee’s attendance from Biometric machines / Mobile Attendance App
- Payroll Software
  Infopay is a simple & user-friendly payroll software to manage Singapore payroll calculation for employees.
- E-Leave Software
  Electronic leave application system - Stay updated with Mobile Push Notification
- E-Claim Software
  Electronic claim application system
- E-Appraisal Software
  Electronic Appraisal Application System
- E-Staff Portal
  Your HR Matters on the Go
- Project Costing Software
  Project Cost Software / Project Cost system is a cloud-based software which captures the employee’s time spent on each project using mobile apps / biometric machines and compute the project costing based on their salaries & payroll benefits

Service model:

☐ Virtual machine instances owned by the user
☐ Network facilities
☐ Compliance with applicable standards

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
- Others: Upon INFO-TECH management Approval (Info-Tech Provides customers with detailed information about security, compliance, Policies upon request)
- 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) (Audit reports can be shared upon Info-Tech Management approval)

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 _________________________________

Data Control

3. Data ownership

All data on the cloud service is owned by the cloud user except for: Application / System specific configuration data

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: 1 Day
- Maximum data retention period is: 7 Days (customer has option for taking 5 backups which they can keep as per their requirements)
- Deleted immediately

Log data is retained for a period of:

- Minimum data retention period as follows: 1 Day
- Maximum data retention period is: 60 Days
Not retained

User data is retained for a period of:

- Minimum data retention period is: 1 Day
- Maximum data retention period is: 60 Days
- 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: ___________ 1 ________________

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

Provider Performance

7. Availability

The committed network uptime is:

- ____________%
- As per SLA

The committed system uptime is:

- ____________%
- As per SLA

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 ______ 24Hrs ____________
- RTO ______ 24 Hrs ____________
- 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: As per agreement
- Infrastructure failure
- Liability: As per agreement
- Virtual machine instance failure
- Liability: As per agreement
- Migrations
- Liability: As per agreement
- Unscheduled downtime
- Liability: As per agreement
- Database failure
- Liability: As per agreement
- Monitoring failure
- Liability: As per agreement

Service Support

10. Change management

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

- Communication plan and procedures for proactive notification
- 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
- 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: Service extension

12. 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: 9AM to 6PM Weekdays Singapore Time
- 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: As per agreement
Mean time to repair on detection of faults: As per agreement

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)
14. Data portability
Importable VM formats: _VHD_
Downloadable formats: _VHD_
Supported operating systems: _2012, 2016, 2019_
Language versions of supported operating systems:
  English
Supported database formats: _MSSQL_
API:
  Common: Will be provided based on the requirements
  Customised

Upon service termination, data is available through:
  Physical media
  Standard methods as described above
  Other methods: Downloadable as reports from portal

15. 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:

16. User management
  Identity management
  Role based access control
17. Lifecycle: The cloud user may select the following for service upgrades and changes:
- Automatic provisioning
- User customisable provisioning

Security Configurations

18. Security configuration enforcement checks

Security configuration enforcement checks are performed:
- Manually
- Using automated tools

How often are enforcement checks being performed to ensure all security configurations are applied?
VA and Pen tests are done quarterly. External Audits are done annually as per MTCS Standards.

19. Multi-tenancy

- Distinct physical hosts
- Distinct physical network infrastructure
- 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 _____________
- Load balancing ports___________
- Load balancing protocols_________
- Anti-DDOS protection systems or services
- Defence-in-depth mechanisms, please specify: _________________
- Network traffic isolation, please specify: Isolated between staging and production environments
- 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: 

Shared or dedicated storage network bandwidth, please specify: 10GBPS Shared

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 