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:	Microsoft Corporation
Primary address:	One Microsoft Way
	Redmond, WA 98052-6399
Web address:	http://www.microsoft.com
Contact name:	Greg Roberts
Contact number:	+1-425-246-6509

Certification Body Contact Information	
Company name:	Certification International Singapore Pte Ltd
Web address:	http://www.socotec-certification-international.sg
Contact name:	John Cheong
Contact email:	Cheong.Yuen-Chun @socotec.com

Cloud Service Provider Background

Overview of service offering:

Office 365 (O365) is a multi-tenant cloud computing-based subscription service offering from Microsoft. Cloud computing has been defined by NIST as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or cloud provider interaction. Further, as defined within NIST SP 800-145 (The NIST Definition of Cloud Computing), the service model for O365 is Software-as-a-Service (SaaS). SaaS is a model of software deployment whereby one or more applications and the computational resources to run them are provided for use on demand as a turnkey service. Its main purpose is to reduce the total cost of hardware and software development, maintenance, and operations. Security provisions are carried out mainly by the cloud provider. The cloud subscriber does not manage or control the underlying cloud infrastructure or individual applications, except for preference selections and limited administrative application settings.

O365 provides customers with cloud versions of Exchange Online (EXO), Information Protection, SharePoint Online (SPO) (including Project Online), Skype for Business (SfB) and other features. Exchange Online is an email service. SharePoint Online is a solution for creating sites to share documents and information. Skype for Business is a communication service that offers instant messaging, audio and video calling, online meetings, and web conferencing capabilities.

Office 365 services in scope are: Exchange Online, SharePoint Online, Information Protection, Skype for Business, Office Online, Office Services Infrastructure (OSI), Suite User Experience, and Domain Name Service (DNS). Please see https://products.office.com/en-us/business/explore-office-365-for-business for Office 365's full service offerings.

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

No.	Criteria	Description	Remarks
		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 _____ ☐ 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	By providing customers with compliant, independently verified cloud services, Use the shared responsibility model, Microsoft makes it easier under the shared responsibility model for customers to achieve compliance for software services they run in the cloud. Microsoft provides Office 365 customers with detailed information about our security and compliance programs, including audit reports and compliance packages, to help customers assess our services against their own legal and regulatory requirements. In addition, Microsoft has developed an extensible compliance framework that enables it to design and build

		☐ 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 <u>(e.g. Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organisation)</u>	services using a single set of controls to speed up and simplify compliance across a diverse set of regulations and rapidly adapt to changes in the regulatory landscape. Microsoft provides a compliance program for financial service customers. Please check with your account manager. As part of Office 365 Independent Verification of security posture, the environment undergoes 3rd party penetration testing against the environment. Customers can conduct independent penetration test after notifying Microsoft. In addition, the 3rd Party assessors conduct detailed review of Risk Assessment and Vulnerability Scans. The findings of these assessments are documented within their assessment(s). Additional information on Independent Verification can be found here: http://office.microsoft.com/en-us/business/office-365-trust-center-cloud-computing-security-FX103030390.aspx#compliance as part of the 3rd Party assessment.
2.	Compliance	The following guidelines / standards / regulations are adhered to:	Independently verified

		☒ Singapore Personal Data Protection Act ☒ ISO / IEC 27001 ☐ ISO 9000 ☐ ISO / IEC 20000 ☒ CSA Open Certification Framework ☐ PCI-DSS ☒ Others <u>SOC 1 and SOC 2 SSAE 16/ISAE 3402; CSA Cloud Controls Matrix; FedRAMP (U.S. only); HIPAA BAA and other listed in the Remarks</u>	By providing customers with compliant, independently verified cloud services, Microsoft makes it easier under the shared responsibility model for customers to achieve compliance for software services they run in the cloud. Microsoft provides Office 365 customers with detailed information about our security and compliance programs, including audit reports and compliance packages, to help customers assess our services against their own legal and regulatory requirements. Office 365 are compliant to the following certifications: • ISO/IEC 27001:2013 • SOC 1 and SOC 2 SSAE 16/ISAE 3402 Type 1 and Type 2 • CSA Cloud Controls Matrix 1.2 (Azure) • FedRAMP/FISMA • UK G-Cloud • Japan Cloud Security Gold Mark Certification • Australia IRAP • HIPAA BAA • Life Sciences GxP • FERPA • FIPS 140-2 • Data Processing Agreements (DPAs)

			• European Union (EU) Model Clauses • US-EU Safe Harbor framework • PIPEDA • GLBA For Office 365: http://office.microsoft.com/en-us/business/office-365-trust-center-cloud-computing-security-FX103030390.aspx#compliance Microsoft's privacy representative for Singapore can be reached at the following address: Microsoft Operations Pte Ltd Attn: Frederic Blanchi, Privacy Officer 1 Marina Boulevard, #22-01 One Marina Boulevard Singapore 018989
Data Control			
3.	Data ownership	All data on the cloud service is owned by the cloud user except for: content the customer did not upload into or create within the service. 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_____	The following lists several frequently asked questions with regards to data ownership: http://office.microsoft.com/en-us/business/office-365-online-data-portability-FX103045783.aspx
4.	Data retention	Data deleted by the user is retained as follows: ☒ Minimum data retention period is: 0 Days ☒ Maximum data retention period is: 30 Days_	Customers may extract and/or delete Customer Data at any time **(Active Delete).** Data will be deleted right away for services with

		☐ Deleted immediately Log data is retained for a period of: ☒ Minimum data retention period as follows: _90 Days_ ☒ Maximum data retention period is: 180 days ☐ Not retained User data is retained for a period of: ☒ Minimum data retention period is: 90 days after account closure_____ ☒ Maximum data retention period is: _180 days after account closure_ ☐ Not retained The following types of data are available for download by the cloud user: ☐ Log data ☐ Other Log Data_from VMs as well as diagnostic data from Azure Diagnostic API	no recycle bin function. Data will be retained to maximum 30 days for services support recycle bin function. . Customers remain responsible for all storage and other applicable charges during this retention period. When a Subscription expires or terminates **(Passive Delete), we** will retain user data from minimum 90 days to maximum 180 days. On log data retention, this varies by type of log. Logs controlled by the user are retained maximum to 180 days.
5.	Data sovereignty	The primary data locations are: ☒ Singapore ☒ Asia Pacific ☐ Europe ☐ United States The backup data locations are: ☒ Singapore ☒ Asia Pacific ☐ Europe ☐ United States No. of countries in which data centres are operated: 8 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	Customers data will be stored in Singapore and other countries in Asia region (Hong Kong, Korea, Malaysia and Japan), this includes service logs that contain customer-authored data. Please find the details of Office 365 data centre locations here: http://www.microsoft.com/online/legal/v2/?docid=25 Office 365 Trust Centre link: https://products.office.com/en-us/business/office-365-

		☒ Yes, except as noted: See Trust Center link for details	trust-center-cloud-computing-security
		☐ 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 Consent is obtained via service agreement and in privacy statement.	
		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)	Non-disclosure is addressed in the service agreement, which includes the following commitment: Microsoft will not disclose Customer Data to a third party (including law enforcement, other government entity, or civil litigant; excluding our subcontractors) except as Customer directs or unless required by law. Should a third party contact Microsoft with a demand for Customer Data, Microsoft will attempt to redirect the third party to request that data directly from Customer. As part of that, Microsoft may provide Customer's basic contact information to the third party. If compelled to disclose Customer Data to a third party, Microsoft will promptly notify

				Customer and provide a copy of the demand, unless legally prohibited from doing so.

Provider Performance

7.	Availability	The committed network uptime is: ☒ <u>99.9 to 99.95</u>% ☐ Varies according to price plan The committed system uptime is: ☒ <u>99.9 to 99.95</u>% ☐ Varies according to price plan The cloud environment has the following single points of failure: ☒ None	Minimum SLA for all Office 365 services in scope is 99.9%. Please find the details and conditions of SLAs for Office 365 services: http://office.microsoft.com/en-us/business/office-365-trust-center-cloud-computing-security-FX103030390.aspx#operations No single point of failure since the underlying infrastructure is distributed.
8.	BCP / DR	☒ Disaster recovery protection ☒ Backup and restore service ☒ User selectable backup plans ☐ Escrow arrangements ☐ No BCP / DR is available ☐ RPO <u>Managed by cloud user</u> ☐ RTO <u>Managed by cloud user</u> ☐ Others, please specify: _____	Microsoft does not provide escrow arrangements, but will provide process for SLA service credit claims. Exchange (EXO)'s RTO is 60 minutes and RPO is 0. Skype for Business (SFB)' RTO is 180 minutes and RPO is 5 minutes. Sharepoint Online (SPO)'s RTO is 120 minutes and RPO is 60 minutes.
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 for outages is addressed in the Service Level Agreements, available here: http://technet.microsoft.com/en-us/library/office-365-service-level-agreement.aspx

		Liability: <u>Same as network failure</u>	
		☒ Virtual machine instance failure	
		Liability: <u>Same as network failure</u>	
		☐ Migrations	
		Liability:_____	
		☒ Unscheduled downtime	
		Liability: <u>Same as network failure</u>	
		☒ Database failure	
		Liability: <u>Same as network failure</u>	
		☒ Monitoring failure	
		Liability: <u>Same as network failure</u>	

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	Assistance in migration to new services when legacy solutions are discontinued - SaaS: Will provide guidance for migration scenarios.
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: _____	RBAC is implemented on Office 365.

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: <u>Dependent on local business hours</u> ☒ After office hours support, please specify the hours of operations: <u>24x7 support in English</u> Service response time: <u>Dependent on severity of incident and type of support plan; between 15 minutes – 8 hours</u> The following are available to users upon request: ☐ Permanent access to audit records of customer instances ☒ Incident management assistance Incident response time: <u>Dependent on severity of incident and type of support plan; between 15 minutes – 8 hours</u> Mean time to repair on detection of faults: _____	Please find the different support plans as follows: http://technet.microsoft.com/en-us/library/office-365-support.aspx Customers have continuous access to their own virtual machines and other services. Auditing of workloads, vulnerability assessment and penetration testing within the Virtual Machines or for their own virtual machines is the customer's responsibility.
13.	Billing	The following billing modes are available (please elaborate granularity of charges and measurement): ☒ Pay per usage per hour (up to per user per hour/day/month/year for SaaS) ☐ Fixed pricing_____(up to yearly/monthly/daily) ☒ Other pricing model <u>Enterprise Agreement for Azure</u> ☐ Not disclosed ☐ Available billing history: _____Months	Other pricing model: Office 365 has a monthly committed spend model which offers discounts to corporations based on the number of users. Additional information can be found: http://products.office.com/en-us/business/compare-office-365-for-business-plans Customers are able to see the entire billing history since the subscription starts.

14.	Data portability	Importable VM formats: <u>Not Applicable</u> Downloadable formats: <u>Separate data format</u> Supported operating systems: <u>See side remarks</u> Language versions of supported operating systems: <u>See side remarks</u> Supported database formats: <u>See side remarks</u> API: ☒ Common <u>See side remarks</u> ☒ Customised <u>See side remarks</u> Upon service termination, data is available through: ☒ Physical media ☒ Standard methods as described above ☐ Other methods	Customers can extract their data from Office 365 anytime, there is no VM associated. Supported OS: • Windows, iOS and Android http://blogs.office.com/2014/10/28/new-office-365-extensibility-windows-ios-android-web-developers/ • Language Support: http://blogs.office.com/2013/01/07/support-for-international-users-and-multiple-languages-in-the-new-office/
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: _____	Microsoft Office 365 currently runs certain IPv6 services on Azure today. These services are constantly updated. Please contact Microsoft for the latest updates and roadmap, which is available under the terms of Microsoft's non-disclosure agreement.
16.	User management	☒ Identity management ☒ Role based access control ☒ Federated access model	For Office 365, Role Based Access Control (RBAC) is used to identify and control the access privileges of each

		☒ Integration with Identity management solutions ☐ Others_____	service team's personnel. Customer can implement RBAC through the utilization of Active Directory (AD). AD is a Commercial Off The Shelf (COTS) directory service implemented by Microsoft for Windows domain networks. Office 365 MT uses Azure AD to implement Role Based Access Control (RBAC) via the use of AD groups. For the purposes of this control, the term "security group" references an Azure AD group which is used to enforce RBAC permissions.
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 being performed to ensure all security configurations are checks applied? External audits are done annually. Self-assessment is performed daily.	Refer to the following link for more information: http://office.microsoft.com/en-us/business/office-365-trust-center-cloud-computing-security-FX103030390.aspx#welcome
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)	Minimum performance during peak periods – No.
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 <u>You can use any IP address range defined in RFC1918. That means the entire 10.0.0.0/8 (16,777,216 addresses)</u> ☐ Load balancing ports _____ ☐ Load balancing protocols _____ ☒ Anti-DDOS protection systems or services ☒ Defence-in-depth mechanisms, please specify: <u>See side remarks</u> ☒ Network traffic isolation, please specify: <u>See side remarks</u> ☒ Shared or dedicated bandwidth, please specify: <u>Shared. Dedicated based on geographical availability. See side remarks.</u> ☐ QoS traffic control services ☒ Alerts to be sent for unusual high usage ☐ Minimum performance during peak periods_____ ☐ Minimum period to scale up network throughput _____	Defence-in-depth mechanisms, please specify: http://www.windowsazure.com/en-us/support/legal/security-overview/ Microsoft Azure network security whitepaper: http://download.microsoft.com/download/4/3/9/43902EC9-410E-4875-8800-0788BE146A3D/Windows%20Azure%20Network%20Security%20Whitepaper%20-%20FINAL.docx

| 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:
_____

☐ Quality of service storage traffic control services

☐ Maximum storage capacity for entire cloud, please specify:
_____

☒ Maximum storage capacity for single user, please specify:
<u>100 TB per account for storage account created before 7 June 2012</u>
<u>200 TB per account for storage account created on 7 June 2012 or later</u>
<u>1 TB per user for Office 365</u>
☒ Maximum expandable storage, please specify:
<u>Refer to above for maximum storage account</u>

☒ 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 | Office 365 Storage includes a "service" called Geo-Replication. It provides durability by constantly maintaining multiple healthy replicas of data both within and between data centres.

With geo-replication, Azure Storage keeps data durable in two locations. It replicates customer data hundreds of miles between two locations (i.e. between North and South US, between North and West Europe, and between East and Southeast Asia) to provide disaster recovery in case of regional disasters.

Also the geo-replication information from one data centre to another as following:

http://blogs.msdn.com/b/windowsazurestorage/archive/2011/09/15/introducing-geo-replication-for-windows-azure-storage.aspx

Billing alert enables customer to get proactive email notifications when the bill goes above a certain monetary threshold that customer configures. |