aws

Amazon Web Services Response to:
Infocomm Media Development Authority of Singapore (IMDA)

---

25 November 2021

Submitted By:

Amazon Web Services, Inc.
410 Terry Avenue North Seattle, WA 98109-5210
Clara Lim
claralim@amazon.com

Submitted To:

Infocomm Media Development Authority Of Singapore (IMDA)

aws

Cloud service provider self-disclosure
(MTCS SS584:2020)

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

Date of Disclosure: 25 November 2021

Applicable cloud service (s): IaaS, PaaS, SaaS

Cloud Service Provider Contact Information
Company name: Amazon Web Services, Inc.   Primary address: 410 Terry Avenue North Seattle, WA 98109, United States   Web address: h t t p s : / / aws.amazon.com   Contact name: Clara Lim   Contact email: claralim@amazon.com   MTCS Certificate Number: 2021-041   Company Chop _____ Company Representative Signature: _____*Clara*_____
Certification Body Contact Information
Company name: EY CertifyPoint   Web address: https://www.ey.com/en_nl/consulting/certify-point   Contact name: Jatin Sehgal   Contact email: certifypoint@nl.ey.com   DocuSigned by: *Wilco Pieterse*   3F3C49E77D1349D...   Company Chop _____ Lead Auditor Signature: _____
Cloud Service Provider Background
Overview of service offering: AWS is an on-demand delivery of compute power, database storage, applications, and other IT resources through a cloud services platform via the internet with pay-as-you-go pricing.

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this response.

Service model:

☒ Virtual machine instances owned by the cloud service customer

☐ 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 cloud service customer has the right to audit: ☒ Virtual machine instances owned by the cloud service customer ☐ 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:	AWS adheres to a Shared Responsibility Matrix, in which AWS maintains responsibility for the physical controls at its data centres. Auditing for most layers and controls remains the responsibility of the customer. The definition of AWS-defined logical and physical controls is documented in the SOC1 Type II report (SSAE 16). The SOC II report and other certifications are available for download and review via https://aws.amazon.com/artifact/. All documents are available under the terms of Amazon's non-disclosure agreement. Please visit https://aws.amazon.com/compliance for more information.

		☐ Virtual machine instances owned by the cloud service customer ☒ 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)	Customers can carry out security assessments or penetration tests against their AWS infrastructure, subject to the AWS Customer Support Policy for Penetration Testing and AWS Security Testing Terms and Conditions. For more information, see https://aws.amazon.com/security/penetration-testing/. AWS Security regularly engages independent security firms to perform external vulnerability threat assessments. AWS follows a modified approach for vulnerability management and has procedures in place to address vulnerabilities timely aligned with the needs of the organization The AWS SOC1 Type II report provided additional details on the specific control activities executed by AWS are available for download and review via https://aws.amazon.com/artifact/.
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 _____	The AWS cloud infrastructure has been designed and managed in alignment with regulations, standards, and best-practices including: • HIPAA SOC 1/SSAE 16/ISAE3402 (formerly SAS7 0) • SOC 2 • SOC 3 • PCI DSS Level 1 • ISO 27001 • ISO 9001 • ISO 27017 • ISO 27018 • FedRAMP(SM) • DIACAP and FISMA • ITAR • FIPS 140-2 • CSA • MPAA Please visit https://aws.amazon.com/compliance/ for more information.

	Data Control		
3.	Data ownership	All data on the cloud service is owned by the cloud service customer except for: _____ The cloud service customer retains the ownership on the derived data or attributes of cloud usage except for the following: ☐ Advertising or marketing ☒ Statistics analysis on usage ☐ Others _____	AWS customers own all right, title and interest in their content. Please review the following link for further information: https://aws.amazon.com/agreement
4.	Data retention	Data deleted by the cloud service customer 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 is: _____ ☐ Maximum data retention period is: _____ ☐ Not retained (Customer data) Cloud service customer 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 service customer: ☐ Log data ☒ Others _____	AWS provides customers with the ability to delete the customer's content. However, AWS customers retain control and ownership of their content so it is the customer's responsibility to manage content retention to their own requirements. Customers may store and retain log data associated with their use of AWS services by using a service called AWS CloudTrail. AWS CloudTrail is a web service that records API calls made on customer account and delivers log files to their Amazon S3 bucket. Customer control the retention policies for their AWS CloudTrail log files. By default, log files are stored indefinitely. Customer can use Amazon S3 object lifecycle management rules to define their own retention policy. 90 days after a customer closes its account, any content remaining in customer account will be permanently deleted, and AWS services that aren't already terminated will be terminated. However, service attributes might be retained as long as necessary for billing and administration purposes. AWS retains account information, as described in the Privacy Notice. Customer cannot reopen that account after 90 days post account closure and cannot create new AWS accounts using the email address that was associated with the customer's account at the time of its closure.

			Please to these links below: https://aws.amazon.com/premiumsupport/knowledge-center/close-aws-account/
5.	Data sovereignty	The primary data locations are: ☒ Singapore ☒ Asia Pacific Seoul ☐ Europe _____ ☒ United States ☐ Others _____ The backup data locations are: ☒ Singapore ☒ Asia Pacific Seoul ☐ Europe _____ ☒ United States ☐ Others _____ No. of countries in which data centres are operated: 25__ The cloud service customer'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 Cloud service customer'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	AWS provides customers the flexibility to place instance and store data within multiple Geographic Regions. AWS customers designate in which physical region their data and their servers will be located. AWS does not move customer data without customer agreement, except as necessary to comply with the law or a binding order of a governmental body. Please to these links below: https://aws.amazon.com/compliance/data-privacy-faq/ AWS has a Region in Singapore, Asia Pacific, Europe and the United States. For more information, please visit http://aws.amazon.com/about-aws/global-infrastructure/. Customer may specify the AWS regions in which Customer Content will be stored. Customer consents to the storage of

		☒ Yes, except as noted: <u>AWS Service Terms,</u> <u>AWS Customer Agreement</u> ☐ No *Note: Cloud service customers are responsible for determining the impact of data protection and data sovereignty laws on the locations where data is stored. In addition, cloud service customers 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.*	Content in, and transfer of Content into, the AWS regions Customer selects, except as specified in the Customer Agreement or Service Terms. AWS will not access or use Customer Content except as necessary to maintain or provide the Service Offerings, as necessary to comply with the law or a binding order of a governmental body, or as specified in the Customer Agreement or Service Terms. https://aws.amazon.com/agreement/ Please refer to the link: https://aws.amazon.com/service-terms/ https://aws.amazon.com/agreement/
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: ☐ <u>100 %</u> ☐ Varies according to price plan The committed system uptime is: ☐ <u>100 %</u> ☐ Varies according to price plan The cloud environment has the following single points of failure: ☐ _____ ☒ none	Please refer to the link: https://aws.amazon.com/legal/service-level-agreements/
8.	3rd Party dependency	Highlight areas of critical dependency for service delivery: _____	

aws

9.	BCP / DR	☒ Disaster recovery protection ☒ Backup and restore service ☒ Cloud service customer selectable backup plans ☐ Escrow arrangements ☐ No BCP / DR is available ☐ RPO_____ ☐ RTO_____ ☐ Others, please specify:_____	The customer retains control of data and applications. The customer is responsible for architecting their own DR plans. AWS gives customer fine- grained control and many building blocks to build the appropriate DR solution given their DR objectives (RTO and RPO) and budget. Please visit https://aws.amazon.com/cloudendure-disaster-recovery/ for more architecture guidelines
10.	Liability	The following terms are available for the cloud service customers 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: _____	Please refer to these links: https://aws.amazon.com/legal/service-level-agreements/

11.	Shared responsibility	☒ Communication of shared roles & responsibilities for which CSC needs to implement and manage for use if this cloud service. URL (or attach file): https://aws.amazon.com/compliance/shared-responsibility-model/	
	Service Support		
12.	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	AWS SOC 1 Type II report provides an overview of the controls in place to manage change management in the AWS environment. In addition, refer to the ISO27001 standard, Annex A, Domain 12.5 for further details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. Changes are authorized, logged, tested, approved and documented. Most updates are done in a manner that will not impact the customer. AWS will communicate with customers, either via email, or through AWS Service Health Dashboard when there is a chance they may be affected.
13.	Self-Service Provisioning and Management portal	Provide self-service provisioning and management portal for cloud service customers 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 ☒ Health monitoring ☐ Others: _____	

| 14. | Incident and Problem Management | Delivery mode of support:

☒ Access via email

☒ Access via portal

☒ Access via phone support

☒ Direct access to support engineers (via livechat)

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: _____

Notification time of cloud service outage incident:

   On-going _____

Communication channel used for notification of cloud service outage incident:

   https://status.aws.amazon.com/ _____

The following are available to cloud service customers upon request:

☒ Permanent access to audit records of customer instances

☒ Incident management assistance

Incident response time: _____

Meantime to repair on detection of faults: _____ | All paid AWS Support tiers offer customers of AWS Infrastructure Services an unlimited number of support cases with pay-by-the-month pricing and no long-term contracts. The four tiers provide developers and businesses the flexibility to choose the support tiers that meet their specific needs.

Please visit https://aws.amazon.com/premiumsupport/ for further details.

Log data associated with AWS Infrastructure Services are stored and retained using a service called AWS CloudTrail. AWS CloudTrail is a web service that records API calls made on customer account and delivers log files to their Amazon S3 bucket.

Customer control the retention policies for their AWS CloudTrail log files. By default, log files are stored indefinitely. Customer can use Amazon S3 object lifecycle management rules to define their own retention policy. |

15.	Billing	The following billing modes are available (please elaborate granularity of charges and measurement): ☒ Pay per usage: <u>Minutes/Hourly/monthly</u> (up to per min/hour/day/month for compute/storage for IaaS/PaaS, and per cloud service customer per hour/day/month/year for SaaS) ☐ Fixed pricing _ (up to yearly/monthly/daily) ☐ Other pricing model _____ ☐ Not disclosed ☐ Available billing history: _____ Months	Please refer to the following links for pricing information: https://aws.amazon.com/pricing https://aws.amazon.com/pricing/services/ AWS provides customer billing history as month-to-date. http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/view-billing-dashboard.html
16.	Data portability	Importable VM formats: _____ Downloadable formats: JSON/XML/other open formats (to specify)_____ Supported operating systems: _____ Language versions of supported operating systems: _____ Supported database formats: _____ Policy/guide available https://docs.aws.amazon.com/ API: ☐ Common _____ ☐ Customised _____ Upon service termination or prolonged outage, data is available through: ☐ Physical media ☒ Standard methods as described above ☐ Other methods _____	https://aws.amazon.com/ec2/vmimport/ Amazon Machine Images (AMIs) are preconfigured with an ever- growing list of operating systems. AWS work with its partners and community to provide customer with the most choices possible. Customer are also empowered to use AWS bundling tools to upload their own operating systems. The operating systems currently available to use with customer Amazon EC2 instances include: • CentOS • Debian • SUSE Linux Enterprise • Amazon Linux • Ubuntu • Red Hat Enterprise Linux • Windows Server • Windows Server Any database can be run on AWS as long as it runs on Linux or Windows. For managed database services, Amazon RDS gives customer access to the capabilities of a familiar MySQL, Oracle, Microsoft SQL Server, or PostgreSQL database engines.

17.	Interoperability	Use of industry standards and availability of APIs to support interoperability: ☒ Transport supported (e.g. REST based HTTPS/MQTT) _____ ☒ Format supported (e.g. JSON/XML) _____ ☒ APIs supported _____ ☐ Other methods _____ Guide available https://docs.aws.amazon.com/ _____	
18.	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: Contingent on customer network speeds. _____	AWS offers support for IPv6 across numerous regions, including Asia Pacific (Singapore). https://aws.amazon.com/blogs/aws/aws-ipv6-update-global-support-spanning-15-regions-multiple-aws-services/
19.	User Management	☒ Identity management ☒ Role based access control ☒ Federated access model ☒ Integration with Identity management solutions ☐ Others _____	
20.	Lifecycle	The cloud service customer may select the following for service upgrades and changes: ☒ Automatic provisioning ☒ Cloud service customer customisable provisioning	

	Security Configurations		
21.	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? <u>Continually</u>	Security configuration at the OS level and up is the responsibility of the customer. AWS is responsible for patching systems supporting the delivery of service to customers, such as the hypervisor and networking services. This is done as required per AWS policy and in accordance with ISO 27001, NIST, and PCI requirements. Customers control their own guest operating systems, software and applications and are therefore responsible for patching their own systems. AWS SOC 1 Type II report provides an overview of the controls in place to manage change management in the AWS environment. In addition, refer to ISO 27001 standard, Annex A, domain 12.5 for further details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.
22.	Multi-tenancy	☒ Distinct physical hosts Only for dedicated instances ☒ Distinct physical network infrastructure ☒ Virtual instance grouping ☒ Cloud service customer definable security domains ☒ Cloud service customer customisable firewall (Utilizing VPC customers can create their own security boundary) ☒ Cloud service customer definable access policies	On AWS, everything is virtual and the networking is software based. Please visit http://aws.amazon.com/vpc to learn about the networking feature. For dedicated hardware, please visit http://aws.amazon.com/dedicated-instances/.

23.	Hybrid Cloud provision	Ability to monitor, track, apply and enforce CSC's security & privacy policies on its cloud workloads: ☒ Data protection and encryption key mgmt. enforcement geolocation-based/resource pools and secure migration of cloud workloads ☒ Key mgmt. and key/store controlled by CSC ☒ Persistent data flow segmentation before and after geolocation-based/resource pools secure migration ☐ Compliance enforcement for regulated workloads between on-premises private and hybrid/public cloud ☐ Others _____	The AWS shared responsibility model applies to data protection in AWS Outposts. Encryption is enabled by default via AWS Key Management Service (AWS KMS) keys. Alternatively, customers could specify a symmetric customer managed key as the default KMS key for EBS encryption. AWS Outposts is designed to operate with a constant and consistent connection between customer's Outpost and an AWS Region. AWS Outposts is HIPAA eligible, PCI, SOC, ISMAP, IRAP and FINMA compliant, ISO, CSA STAR, and HITRUST certified. Under the shared responsibility model, AWS is responsible for the hardware and software that run AWS services. This applies to AWS Outposts, just as it does to an AWS Region. This includes patching the infrastructure software and configuring infrastructure devices. Customers are responsible for implementing best practices for data encryption, patching guest operating system and applications, identity and access management, and operating system, network, and firewall configurations.
	Service Elasticity		
24.	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)	Auto Scaling allows customer to scale their Amazon EC2 capacity up or down automatically according to conditions they define. With Auto Scaling, customer can ensure that the number of Amazon EC2 instances they're using increases seamlessly during demand spikes to maintain performance, and decreases automatically during demand lulls to minimize costs. http://aws.amazon.com/autoscaling/ Minimum additional capacity guaranteed per account will depend on the instance type selected. https://aws.amazon.com/ec2/instance-types/

| 25. | 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 ____5+_____

☒ Load balancing ports _____

☒ Load balancing protocols _____

☒ Anti-DDOS protection systems or services

☒ Defence-in-depth mechanisms, please specify: __
_____

☒ Network traffic isolation, please specify: _____
_____

☒ 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
_____ | The AWS network provides significant protection against traditional network security issues and the customer can implement further protection. See the AWS Security Whitepaper for more information on this topic, including a discussion of DDoS attacks:

https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

Please visit https://aws.amazon.com/vpc to understand how customer have complete control over their virtual networking environment, including selection of their own IP address range, creation of subnets, and configuration of route tables and network gateways.

AWS Direct Connect provides 1 Gbps and 10Gbps connections, and customer can easily provision multiple connections if they need more capacity.

Using Amazon VPC, customers are by default offered a minimum of 5 usable IPs, but may request more through the console if required.

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Appendix_Limits.htm |

aws

| 26. | 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 cloud service customer, 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 _____ | Please visit the following links to understand the various storage options available on the AWS platform.

Usage, SLA, performance, and scalability vary based on the storage options that customer choose.

https://aws.amazon.com/ebs

https://aws.amazon.com/s3

https://aws.amazon.com/glacier

https://aws.amazon.com/importexport/

https://aws.amazon.com/storagegateway/

To read more about how AWS isolates customer storage traffic, please visit the following link:

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html |