Advanced Info Service
Public Company Limited

1291/1 AIS Tower,
Phaholyothin Rd., Samsen Nai,
Phayathai, Bangkok 10400
Tel : (662) 299 6000

CSA: Statement of Applicability

สายธุรกิจ AIS

Document Version: 1.1

Document Owner: INFOSEC

Last Updated: 15/Aug/2017

Advanced Info Service
Public Company Limited

1291/1 AIS Tower,
Phaholyothin Rd., Samsen Nai,
Phayathai, Bangkok 10400
Tel : (662) 299 6000

Document Control

Document Approvals

This document has been reviewed and approved by:

Document Owner	
Name:	**INFOSEC**
Date:	15/Aug/2017

Version History

The following table records all the revisions made to this document:

Revision	Date	Created By	Detail	Reviewed by	Authorized by
1.0	25/OCT/2016	INFOSEC	Initial Release	Senee Khetsakul	ISMR
1.1	15/Aug/2017		Review after external audit	Senee Khetsakul	ISMR

LR: Legal Requirement, **CO**: Contractual Obligation, **BR/BP**: Business Requirement/Best Practice, **RA**: Risk Assessment Result

CLOUD CONTROLS MATRIX V 3.0.1		Applicable (Y/N)	Reason for selection				Implementation Description/Reference
Control	Description		LR	CO	BR/BP	RA	
Application & Interface Security							
AIS-01	Application Security	Y			O		- (ISMS-PLC-06) System Acquisition Development and Maintenance Policy
AIS-02	Customer Access Requirements	Y			O		- System admin and tenant access level are defined in the terms and conditions of delivering the service.
AIS-03	Data Integrity	N					AIS provides only IaaS solution. Thus, customers are responsible for data handling in their VM host.
AIS-04	Data Security / Integrity	Y			O		- (ISMS-PLC-06) System Acquisition Development and Maintenance Policy
Audit Assurance & Compliance							
AAC-01	Audit Planning	Y			O		- Refer to Internal audit manual
AAC-02	Independent Audits	Y			O		- Internal ISMS and CSA CCM Audit Process - Certification audit by CB
AAC-03	Information System Regulatory Mapping	Y			O		- The legal department regularly monitors changes to the regulatory requirements in relevant jurisdictions and notifies the infosec team via e-mail. - Each tenant instance runs on its own dedicated VM and is isolated from network layer 3 (VLAN) and up.
Business Continuity Management & Operational Resilience							
BCR-01	Business Continuity Planning	Y			O		- แผนความต่อเนื่องทางธุรกิจ Business Continuity Plan (BCP) อาคาร TLS1
BCR-02	Business Continuity Testing	Y			O		- แผนความต่อเนื่องทางธุรกิจ Business Continuity Plan (BCP) อาคาร TLS1
BCR-03	Datacenter Utilities / Environmental Conditions	Y			O		- UPS and Generator are installed to support during emergency situation - Important communication links have a backup link. - Waterleak, UPS, Smoke Dectector, Generator, Humidity & Temperature
BCR-04	Documentation	Y			O		- Information system documentation is available to authorized employees.
BCR-05	Environmental Risks	Y			O		- The following environmental control devices are installed: FM200, N2, Waterleak Detector, Smoke Detector, Precision Air, Chiller, Dehumidity
BCR-06	Equipment Location	Y			O		- Environment of Data Center has been properly controlled to protect equipment from damage. The following systems were installed; • Temperature and humidity conditioning system • Fire extinguishing system designed for electronic equipment • Fire and smoke detection system - Fire alarm was installed to notify authorized person immediately when detecting incident. - Important equipment which requires to be placed outside the Data center must be securely kept in lockable rack, cabinet or room to prevent unauthorized access. - Personal Computer/Workstation must be securely used and protected according to (ISMS-PLC-02) Acceptable Use Policy.
BCR-07	Equipment Maintenance	Y			O		- Infrastructure equipments and System equipments will receive preventive maintenance as defined in the Equipment Maintenance Plan (whether in-house or outsource maintenance). - Equipment maintenance will be carried out by authorized and qualified staffs/vendors - Record of maintenance and repair must be kept for important equipment.
BCR-08	Equipment Power Failures	Y			O		- UPS and Generator are installed to support during emergency situation
BCR-09	Impact Analysis	Y			O		- แผนความต่อเนื่องทางธุรกิจ Business Continuity Plan (BCP) อาคาร TLS1
BCR-10	Policy	Y			O		- Employees can access policies and procedures via intranet.
BCR-11	Retention Policy	Y			O		- Customer data is only retained for the duration of the contract or as agreed with the customer.
Change Control & Configuration Management							
CCC-01	New Development / Acquisition	Y			O		- (ISMS-PLC-06) System Acquisition Development and Maintenance Policy - Change Management Process
CCC-02	Outsourced Development	N					There is no software being developed by outsourced. All software is either developed in-house, software package or opensource
CCC-03	Quality Testing	Y			O		- (ISMS-PLC-06) System Acquisition Development and Maintenance Policy
CCC-04	Unauthorized Software Installations				O		- Change Management Process
CCC-05	Production Changes	Y			O		- Change Management Process
Data Security & Information Lifecycle Management							
DSI-01	Classification	Y			O		- (ISMS-PLC-03) Information Classification and Handling Policy
DSI-02	Data Inventory / Flows	Y			O		- (ISMS-PLC-04) Network Management Policy
DSI-03	Ecommerce Transactions	N					Ecommerce transactions are not in the scope of AIS IaaS soulution.
DSI-04	Handling / Labeling / Security Policy	Y			O		- (ISMS-PLC-03) Information Classification and Handling Policy
DSI-05	Non-Production Data	N					There is no non-production data in AIS IaaS environment.
DSI-06	Ownership / Stewardship	Y			O		- (ISMS-PCD-003) Asset Inventory Procedure - (ISMS-FM-010) Inventory of Assets
DSI-07	Secure Disposal	Y			O		- (ISMS-PLC-03) Information Classification and Handling Policy - (ISMS-PCD-007) Information Disposal Procedure
Datacenter Security							
DCS-01	Asset Management	Y			O		- (ISMS-PCD-003) Asset Inventory Procedure - (ISMS-FM-010) Inventory of Assets
DCS-02	Controlled Access Points	Y			O		- Data Center has installed access control, CCTV, Smoke Detector, WaterLeak Dectection. - Office area has installed access control, CCTV, Smoke Detector
DCS-03	Equipment Identification	Y			O		- Assets are manually tracked.
DCS-04	Off-Site Authorization	Y			O		- (ISMS-PLC-07) Physical Security Policy
DCS-05	Off-Site Equipment	Y			O		- (ISMS-PCD-003) Asset Inventory Procedure - (ISMS-PCD-007) Information Disposal Procedure
DCS-06	Policy	Y			O		- (ISMS-PLC-07) Physical Security Policy
DCS-07	Secure Area Authorization	Y			O		- (ISMS-PLC-07) Physical Security Policy
DCS-08	Unauthorized Persons Entry	Y			O		- (ISMS-PLC-07) Physical Security Policy
DCS-09	User Access	Y			O		- (ISMS-PLC-07) Physical Security Policy
Encryption & Key Managementy							
EKM-01	Entitlement	N					Key management is outside of AIS IaaS solution
EKM-02	Key Generation	N					Key management is outside of AIS IaaS solution
EKM-03	Sensitive Data Protection	Y			O		- (ISMS-PLC-08) Cryptographic and Key Management Policy
EKM-04	Storage and Access	N					Key management is outside of AIS IaaS solution
Governance and Risk Management							
GRM-01	Baseline Requirements	Y			O		- Information security baselines are documented for all component of the cloud infrastructure.
GRM-02	Data Focus Risk Assessments	Y			O		- (ISMS-PLC-01) Information Security Policy - (ISMS-PLC-10) ISMS Manual
GRM-03	Management Oversight	Y			O		- Routine monitoring and random checked by Manager/Line of command

AIS

Statement of Applicability (SoA)

Version: 1.1
Date: 15 Aug 2017

LR: Legal Requirement, **CO**: Contractual Obligation, **BR/BP**: Business Requirement/Best Practice, **RA**: Risk Assessment Result

CLOUD CONTROLS MATRIX V 3.0.1		Applicable	Reason for selection				Implementation Description/Reference
Control	Description	(Y/N)	LR	CO	BR/BP	RA	
GRM-04	Management Program	Y			O		- (ISMS-PLC-01) Information Security Policy - (ISMS-PLC-10) ISMS Manual
GRM-05	Management Support/Involvement	Y			O		- (ISMS-PLC-01) Information Security Policy - (ISMS-WI-01) Third-Party Code of Conduct
GRM-06	Policy	Y			O		- (ISMS-PLC-01) Information Security Policy - (ISMS-WI-01) Third-Party Code of Conduct - Privacy Data Law (Draft)
GRM-07	Policy Enforcement	Y	O		O		- Defined in employee contracts. อ้างอิงข้อ 3.3.42 ข้อบังคับการทำงานของบริษัท บทที่ 9 เรื่องวินัย การพักงานและการลงโทษ
GRM-08	Policy Impact on Risk Assessments	Y			O		- (ISMS-PLC-01) Information Security Policy - (ISMS-PLC-10) ISMS Manual
GRM-09	Policy Reviews	Y			O		- (ISMS-PLC-01) Information Security Policy - (ISMS-PLC-10) ISMS Manual
GRM-10	Risk Assessments	Y			O		- (ISMS-PLC-01) Information Security Policy - (ISMS-PLC-10) ISMS Manual
GRM-11	Risk Management Framework	Y			O		- (ISMS-PLC-01) Information Security Policy - (ISMS-PLC-10) ISMS Manual
Human Resources							
HRS-01	Asset Returns	Y			O		- Refer to HR process - The privacy policy follows an act order from Office of The National Broadcasting and Telecommunications Commission. (นโยบายหลักเกณฑ์คุ้มครองสิทธิของผู้ใช้บริการโทรคมนาคมเกี่ยวกับข้อมูลส่วนบุคคล สิทธิในความเป็นส่วนตัว และเสรีภาพในการสื่อสารถึงกันโดยทางโทรคมนาคม)
HRS-02	Background Screening	Y			O		- For new employees, Background checks are conducted by HR (e.g. checking original qualification document) - For third party company, refer to Contract and NDA (planned)
HRS-03	Employment Agreements	Y	O		O		- All permanent and outsourced employees must sign contract with the organization
HRS-04	Employment Termination	Y			O		- HR and Manager will be responsible for all resign/end of contract personnel
HRS-05	Mobile Device Management	Y			O		- (ISMS-PLC-02) Acceptable Use Policy - (ISMS-PLC-09) Mobile Device, Teleworking and BYOD Policy
HRS-06	Non-Disclosure Agreements	Y	O		O		- NDA exists between the organization and its employees including vendors/third parties.
HRS-07	Roles / Responsibilities	Y			O		- (ISMS-PLC-10) ISMS Manual - (ISMS-PLC-01) Information Security Policy
HRS-08	Technology Acceptable Use	Y			O		- (ISMS-PLC-02) Acceptable Use Policy
HRS-09	Training / Awareness	Y			O		- Create yearly security training plan for security awareness and regularly technical operation training (Yearly Training Plan) and Training record are kept at HR department - New employee will attend orientation training.
HRS-10	User Responsibility	Y			O		- Employees are provided security awareness training resources and sign an agreement acknowledging their responsibilities upon joining the company.
HRS-11	Workspace	Y			O		- (ISMS-PLC-02) Acceptable Use Policy
Identity & Access Management							
IAM-01	Audit Tools Access	Y			O		- Administrative access to the production servers and application are logged.
IAM-02	Credential Lifecycle / Provision Management	Y			O		- (ISMS-PLC-05) System Access Control Policy - The employee exit process involves closing all employee accounts.
IAM-03	Diagnostic / Configuration Ports Access	Y			O		- All access management consoles in AIS's cloud infrastructure require access through CAS terminal.
IAM-04	Policies and Procedures	Y			O		- (ISMS-PLC-05) System Access Control Policy
IAM-05	Segregation of Duties	Y			O		- (ISMS-PLC-10) ISMS Manual - (ISMS-PLC-05) System Access Control Policy
IAM-06	Source Code Access Restriction	N					There is no software being developed.
IAM-07	Third Party Access	Y			O		- (ISMS-WI-01) Third-Party Code of Conduct - (ISMS-PLC-05) System Access Control Policy
IAM-08	Trusted Sources	Y			O		- No access to tenant data
IAM-09	User Access Authorization	Y			O		- (ISMS-PLC-05) System Access Control Policy
IAM-10	User Access Reviews	Y			O		- (ISMS-PLC-05) System Access Control Policy
IAM-11	User Access Revocation	Y			O		- (ISMS-PLC-05) System Access Control Policy
IAM-12	User ID Credentials	Y			O		- (ISMS-PLC-05) System Access Control Policy - Password Standard
IAM-13	Utility Programs Access	Y			O		- (ISMS-PLC-05) System Access Control Policy - Administrative utilities and applications are restricted to a limited number of personnel who require access to perform their job.
Infrastructure & Virtualization Security							
IVS-01	Audit Logging / Intrusion Detection	Y			O		- Computer-Related Crime Act B.E. 2550 - Log System will be monitored by VCSO team. - Other logs are kept at each machine.
IVS-02	Change Detection	Y			O		- AIS's virtual infrastructure management platform collects all change logs to the VM images.
IVS-03	Clock Synchronization	Y			O		- Computer-Related Crime Act B.E. 2550 - Devices are configured to synchronize time with NTP Server; except standalone system.
IVS-04	Information System Documentation	Y			O		- Refer to capacity management report.
IVS-05	Vulnerability Management	Y			O		- (CSA-PCL-01) Cloud security policy
IVS-06	Network Security	Y			O		- (ISMS-PLC-04) Network Management Policy
IVS-07	OS Hardening and Base Controls	Y			O		- Virtualization Security Guidelines
IVS-08	Production / Non-Production Environments	Y			O		- (ISMS-PLC-04) Network Management Policy
IVS-09	Segmentation	Y			O		- (ISMS-PLC-04) Network Management Policy
IVS-10	VM Security - Data Protection	Y			O		- Virtualization Security Guidelines
IVS-11	Hypervisor Hardening	Y			O		- Virtualization Security Guidelines
IVS-12	Wireless Security	Y			O		- (ISMS-PLC-04) Network Management Policy
IVS-13	Network Architecture	Y			O		- (ISMS-PLC-04) Network Management Policy
Interoperability & Portability							
IPY-01	APIs	N					The APIs are not provided for customers by default.
IPY-02	Data Request	Y			O		All structured and unstructured data are available to the customer upon request in an industry-standard format (e.g., .doc, .xls, .pdf, logs, and flat files).
IPY-03	Policy & Legal	Y			O		The using of APIs is available based on request.
IPY-04	Standardized Network Protocols	Y			O		VMWare provides standardized network protocols for the import and export of data and to manage the service.
IPY-05	Virtualization	Y			O		VMWare provides provides an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF).
Mobile Security							

LR: Legal Requirement, **CO**: Contractual Obligation, **BR/BP**: Business Requirement/Best Practice, **RA**: Risk Assessment Result

CLOUD CONTROLS MATRIX V 3.0.1		Applicable (Y/N)	Reason for selection				Implementation Description/Reference
Control	Description		LR	CO	BR/BP	RA	
MOS-01	Anti-Malware	Y			O		- Use anti-virus software for server, client and email. - Anti-virus signature will be updated automatically and checked by Client team
MOS-02	Application Stores	Y			O		Application usage restrictions for BYOD are defined. Employees can only use approved applications for accessing email.
MOS-03	Approved Applications	Y			O		Application usage restrictions for BYOD are defined. Employees can only use approved applications for accessing email.
MOS-04	Approved Software for BYOD	Y			O		Application usage restrictions for BYOD are defined. Employees can only use approved applications for accessing email.
MOS-05	Awareness and Training	Y			O		- Create yearly security training plan for security awareness and regularly technical operation training (Yearly Training Plan) and Training record are kept at HR department - New employee will attend orientation training.
MOS-06	Cloud Based Services	Y			O		Users can use only pre-approved applications.
MOS-07	Compatibility	Y			O		BYOD users are advised to only download applications from official stores, they can only use approved applications for accessing email.
MOS-08	Device Eligibility	Y			O		BYOD users are advised to only download applications from official stores, they can only use approved applications for accessing email.
MOS-09	Device Inventory	Y			O		All company issued mobile devices are recorded on the company asset register. Employees using BYOD devices to access company email have to accept company security policies
MOS-10	Device Management	Y			O		All BYOD are managed centrally by MDM.
MOS-11	Encryption	N					Mobile encryption is not in the scope of AIS IaaS soulution.
MOS-12	Jailbreaking and Rooting	Y			O		- (ISMS-PLC-09) Mobile Device, Teleworking and BYOD Policy
MOS-13	Legal	Y			O		- (ISMS-PLC-09) Mobile Device, Teleworking and BYOD Policy
MOS-14	Lockout Screen	Y			O		- (ISMS-PLC-02) Acceptable Use Policy
MOS-15	Operating Systems	Y			O		- (ISMS-PLC-09) Mobile Device, Teleworking and BYOD Policy
MOS-16	Passwords	Y			O		- (ISMS-PLC-02) Acceptable Use Policy - Password Standard
MOS-17	Policy	Y			O		- (ISMS-PLC-09) Mobile Device, Teleworking and BYOD Policy
MOS-18	Remote Wipe	Y			O		The company has privileges to perform remote wipe of BYOD devices used to synchronise AIS email. employees are made aware of this.
MOS-19	Security Patches	Y			O		- Patch management is handled by CMIT (WSUS)
MOS-20	Users	Y			O		- (ISMS-PLC-09) Mobile Device, Teleworking and BYOD Policy
Security Incident Management, E-Discovery & Cloud Forensics							
SEF-01	Contact / Authority Maintenance	Y			O		- Security Incident Management Procedure
SEF-02	Incident Management	Y			O		- Security Incident Management Procedure
SEF-03	Incident Reporting	Y			O		- Security Incident Management Procedure
SEF-04	Incident Response Legal Preparation	Y	O		O		- Forensic Handling Procedure
SEF-05	Incident Response Metrics	Y			O		- Security Incident Management Procedure
Supply Chain Management, Transparency and Accountability							
STA-01	Data Quality and Integrity	Y			O		- (ISMS-WI-01) Third-Party Code of Conduct
STA-02	Incident Reporting	Y			O		- Security Incident Management Procedure
STA-03	Network / Infrastructure Services	Y			O		- Refer to capacity management report.
STA-04	Provider Internal Assessments	Y			O		- (ISMS-WI-01) Third-Party Code of Conduct
STA-05	Supply Chain Agreements	Y			O		- (ISMS-WI-01) Third-Party Code of Conduct
STA-06	Supply Chain Governance Reviews	Y			O		- Third Party services have been monitored to ensure that they meet requirements specified in Third Party Agreement. All service reports from Third Party was kept to ensure service of Third Party.
STA-07	Supply Chain Metrics	Y			O		- Supplier agreements require SLA and measurements to be provided to ensure Service levels are in line with expectations
STA-08	Third Party Assessment	Y			O		- Third Party services have been monitored to ensure that they meet requirements specified in Third Party Agreement. All service reports from Third Party was kept to ensure service of Third Party.
STA-09	Third Party Audits	Y			O		- Third Party services have been monitored to ensure that they meet requirements specified in Third Party Agreement. All service reports from Third Party was kept to ensure service of Third Party.
Threat and Vulnerability Management							
TVM-01	Anti-Virus / Malicious Software	Y			O		- Use anti-virus software for server, client and email. - Anti-virus signature will be updated automatically and checked by Client team
TVM-02	Vulnerability / Patch Management	Y			O		- Hypervisor patch management is handled by VCSO
TVM-03	Mobile Code	Y			O		- (ISMS-PLC-09) Mobile Device, Teleworking and BYOD Policy - Use anti-virus software for server and client.

Cloud Security Manger/ISMR