October 2022

Document title: **[Cloud Hosting Policy – October 2022]**

Approval date: **[July 2018]**

Purpose of document: **[This policy establishes the technical terms and conditions for cloud or offsite Service Providers and services. All IT-related RFPs, Contracts, etc. must abide by this policy. These technical terms and conditions will help to protect AUC departments by mitigating the risks associated with entrusting AUC data to a third party.]**

Office/department responsible: **[**Office of Information Security**]**
Approved by: **[Nagwa Nicola, Chief Technology Officer]**

Document classification level: **[PUBLIC]**

Document accessible: **[https://www.aucegypt.edu/about/university-policies]**

Document includes: **[Policy]**

Related documents/see also: **[AUC Data Governance Policy, Information Security Policy, Electronic Mail Email Policy, Acceptable Use Policy, Peer to Peer Sharing Policy]**

Cloud Hosting Policy

Policy Statement

Cloud and offsite hosting offer a credible alternative to traditional IT delivery models. Cloud and offsite hosting can provide benefits such as rapid delivery, enhanced scalability, agility, and new funding models. This policy provides a way for AUC to utilize offsite-hosting facilities to include software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) – is referred to as "Cloud and Offsite Hosting Services" in the remainder of this policy. AUC is governing these services' usage through this document.

Reason for Policy/Purpose

This policy establishes the technical terms and conditions for cloud or offsite Service Providers and services. All IT-related RFPs, Contracts, etc., must abide by this policy. These technical terms and conditions will help to protect AUC departments by mitigating the risks associated with entrusting AUC data to a third party.

Who Approved This Policy

Nagwa Nicola, Chief Technology Officer

Who Needs to Know This Policy

AUC Faculty and Staff

Web Address for this Policy

https://www.aucegypt.edu/about/university-policies

Contacts

Responsible University Official: Wessam Maher, Chief Information Security and Risk Officer
Responsible University Office: Office of Information Security
If you have any questions on the policy, you may send an e-mail to infosec@aucegypt.edu

Policy/Procedures

General Terms and Conditions (mandatory)

All cloud and offsite hosting services should pass through approvals from the Officer of Information Technology and Information Security unit before purchase approval and renewal. A non-Disclosure Agreement should be signed between both parties. All legal documents should be revised by AUC legal office. A proper ROI/Cost-Benefit analysis should be performed and approved by management before deciding to move or initiate AUC services on any cloud.

Agreements should contain or cover the following statements and Clauses

Clause 1 (mandatory)
The Service Provider shall have a fully implemented information security program to protect AUC information assets and provide a high-level overview of that program to AUC Information Security Office side.

Clause 2 (mandatory)
AUC shall own all rights, title, and interest in its data related to the services provided by this contract. The Service Provider shall not access AUC User accounts or AUC Data, except (i) in the course of data center operations, (ii) response to service or technical issues, (iii) as required by the express terms of the contract, or (iv) at AUC written request.

Clause 3 (mandatory)
Protection of personal privacy and sensitive data shall be an integral part of the business activities of the Service Provider to ensure that there is no inappropriate or unauthorized use of AUC information at any time. To this end, the Service Provider shall safeguard the confidentiality, integrity, and availability of AUC information and comply with the following conditions:

a) Personal information obtained by the Service Provider shall become and remain the property of AUC.
b) At no time shall any data or processes, which either belong to or are intended for the use of the AUC or its officers, agents, or employees, be copied, disclosed, or retained by the Service Provider or any party related to the Service Provider for subsequent use in any transaction that does not include AUC.

c) The Service Provider shall not use any information collected in connection with the service issued from this proposal for any purpose other than fulfilling the service.
d) The Service Provider shall encrypt all non-public data in transit to the cloud during the life of the contract.
e) For engagements where the Service Provider stores sensitive, personally identifiable, or otherwise confidential information, this data shall be encrypted at rest. Examples are Social Security Number, Date of Birth, Driver's License number, passwords, financial data, and federal/state tax information.

Clause 4 (mandatory)
The Service Provider shall not store or transfer non-public AUC data outside of the agreed country of service residence without the written consent of AUC. This includes backup data and Disaster Recovery locations.

Clause 5 (mandatory)
The Service Provider shall provide written notice to AUC of any actual security breach that jeopardizes AUC data or processes. This notice shall be given to AUC within 24 hours of its discovery. Full disclosure of the jeopardized data shall be made. In addition, the Service Provider shall inform AUC of the actions it is taking or will take to reduce the risk of further loss to AUC.

Clause 6 (mandatory)
All communication shall be coordinated with AUC when the Service Provider is liable for the loss; Service Provider shall recover all costs of response and recovery from the breach.

Clause 7 (mandatory)
The Service Provider shall contact AUC upon receipt of any electronic discovery; litigation holds, discovery searches, and expert testimonies related to, or which in any way might reasonably require access to the data of AUC. The Service Provider shall not respond to subpoenas, service of process, and other legal requests related to AUC without first notifying AUC unless prohibited by law from providing such notice.

Clause 8 (mandatory)
In the event of termination of the contract, the Service Provider shall implement an orderly return of AUC data in an AUC-defined format and the subsequent secure disposal of AUC data.

Suspension of services:
During any period of suspension, the Service Provider shall not take any action to erase any AUC data.

Termination of any services or agreement entirety:
In the event of termination of any services or agreement in entirety, the Service Provider shall not take any action to erase AUC data for a period of 90 days after the effective date of the termination. After such 90 day period, the Service Provider shall have no obligation to maintain or provide any AUC data and shall thereafter, unless legally prohibited and subject to applicable law, destroy all AUC data in its systems or otherwise in its possession or under its control.

Post-Termination Assistance:
AUC shall be entitled to any post-termination assistance generally made available with respect to the Services unless a unique data retrieval arrangement has been established as part of a Service Level Agreement.

Secure Data Disposal
When requested by AUC, the provider shall destroy all requested data in all of its forms, for example, disk, CD/DVD, backup tape, and paper. Data shall be permanently deleted and shall not be recoverable, according to the National Institute of Standards and Technology (NIST) approved methods, and certificates of destruction shall be provided to AUC.

Clause 9 (mandatory)
The Service Provider shall conduct criminal background checks on all staff, including subcontractors, utilized to fulfill the obligations of the contract. If any staff being utilized to fulfill the obligations of the contract have criminal convictions or pending litigation, including but not limited to dishonesty or criminal fraud, the service provider shall notify AUC. The Service Provider shall promote and maintain an awareness of the importance of securing AUC's information among the Service Provider's employees and agents.

Clause 10 (mandatory)
The Service Provider must manage AUC's records in accordance with all applicable records management laws and regulations, including those set forth by US Federal laws and Egyptian laws.

Clause 11
The Service Provider shall allow AUC access to system security logs, latency statistics, etc., that affect this engagement, its data, and or processes. This includes the ability of AUC to request a report of the records that a specific user accessed over a specified period.

Clause 12
The Service Provider shall allow AUC to audit conformance to the contract terms. AUC may perform this audit or contract with a third party at its discretion and AUC's expense.

Clause 13
The Service Provider shall perform an independent audit of their data centers at least annually at their expense and provide a redacted version of the audit report upon request. The Service Provider may remove their proprietary information from the redacted version. For example, a Service Organization Control (SOC) 2 audit report can be sufficient.

Clause 14
Advance notice (to be determined at contract time) shall be given to AUC of any major upgrades or system changes that the Service Provider will be performing. A major upgrade is a replacement of hardware, software, or firmware with a newer or better version, in order to bring the system up to date or to improve its characteristics and usually includes a new version number. AUC reserves the right to defer these changes if desired.

Clause 15
The Service Provider shall disclose its non-proprietary security processes and technical limitations to AUC such that adequate protection and flexibility can be attained between AUC and the Service Provider. For example, in virus checking and port sniffing – AUC and the Service Provider shall understand each other's roles and responsibilities.

Clause 16
The Service Provider shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff access to customer data to that which is absolutely needed to perform job duties.

Clause 17
AUC shall have the ability to import or export data piecemeal or in entirety at its discretion without interference from the Service Provider. This includes the ability for AUC to import or export data to/from other Service Providers.

Clause 18
The Service Provider shall be responsible for the acquisition and operation of all hardware, software, and network support related to the services being provided. The technical and professional activities required for establishing, managing, and maintaining the environment are the responsibilities of the Service Provider. The system shall be available 24 hours per day, 365 days per year basis (with agreed-upon maintenance downtime), and provide service to customers as defined in the Service Level Agreement.

Clause 19
The Service Provider shall identify all of its strategic business partners related to services provided under this contract, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Service Provider, who will be involved in any application development and/or operations.

AUC shall be notified, in advance, if any AUC services or data are to be subcontracted to a third party. The Service Provider shall not subcontract any of its rights and obligations under its contract with AUC without the written consent of AUC.

Clause 20
AUC shall have the right at any time to require that the Service Provider removes from interaction with AUC's data any Service Provider representative who AUC believes is detrimental to its working relationship with the Service Provider. AUC will provide the Service Provider with notice of its determination and the reasons it requests the removal. If AUC signifies that a potential security violation exists with respect to the request; the Service Provider shall immediately remove such individual. The Service Provider shall not assign the person to any aspect of the contract or future work orders without AUC's consent.

Clause 21
The Service Provider shall provide business continuity and disaster recovery plan upon request and ensure that AUC's Recovery Time Objective (RTO) and Recovery Point Objective (RPO) are met, as defined in the contract.

Clause 22
The Service Provider shall use web services exclusively to interface with AUC's data in near real-time when possible.

Clause 23
The Service provider shall encrypt all AUC non-public data that resides on any Service Provider's mobile devices during the life of the contract.

Related Information

https://www.aucegypt.edu/about/university-policies

History/Revision Dates

Origination Date: January 2016
Last Amended Date: July 2018
Last Review Date: October 2022
Next Review Date: October 2025