

---

Document title: **Identity and Access Management Policy – February 2018**

Approval date: **February 2018**

Purpose of document: **This document addresses the management of permissions for accessing AUC data and resources.**

Office/department responsible: **Office of IT**

Approved by: **Nagwa Nicola, Chief Technology Officer**

Document classification level: **PUBLIC**

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

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

---

## **Identity and Access Management Policy**

---

### **Policy Statement**

---

AUC data and resources must be secured by strong identity management processes and procedures. All users who uses or access AUC data or resources must have unique identifier across all systems and their access permissions, granting and revoking are adequately managed.

---

### **Reason for Policy/Purpose**

---

Ensure community are fully aware of the requisite security needed to protect a digital asset and access to AUC assets and information resources.

---

### **Who Approved This Policy**

---

Nagwa Nicola, Chief Technology Officer  
Wessam Maher, Principal Campus Information Security Officer

---

### **Who Needs to Know This Policy**

---

Entire AUC community

---

## Web Address for this Policy

---

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

---

## Contacts

---

Responsible University Official: Wessam Maher

Responsible University Office: Information Security Office, Office of Information Technology

If you have any questions on the policy, you may send an e-mail to [infosec@aucegypt.edu](mailto:infosec@aucegypt.edu)

---

## Policy/Procedures

---

1. Every user or person who deals with AUC systems, data, assets and digital resources must have a single, digital and unified identity.
2. Identities should be unique for every person, using shared identity should be approved and documented by management and information security
3. Redundant identities should be regularly identified and rectified
4. Any identity owner leaves AUC or ends his/her relation with AUC should have his/her access terminated and identity disabled or deleted.
5. All systems and digital assets access should be identified or traced automatically by the unified identity.
6. Identity provisioning and de-provisioning actions should be managed by strict processes and workflows.
7. Identity access privilege should be tied with the user relationship with AUC and in specific with regards to the role and accountabilities assigned.
8. Identity access privilege review and adjustment should be triggered whenever the person status is affected like moving internally inside AUC, getting promoted, resigning, getting fired, involved in an investigation or accused of a violation, going on a paid/unpaid leave...etc.
9. Any change in identity record details or metadata should be managed by strict processes and shouldn't affect the integrity of the record. These changes must be aligned with relevant processes like password change and approval workflows processes...etc.
10. Access control limits and boundaries authorizations are established, documented and reviewed properly.
11. Access limits should be approved by relevant stakeholders, data owners as well as information security, depending on the criticality of the case.
12. Access authorization requests and granting actions should be formalized and documented
13. Access limits should be based on need to know, need to use and least privilege principles and designed to accommodate AUC applications/systems. The general access rule is "Everything is generally forbidden unless expressly permitted"
14. Purchasing decisions of new systems and applications must take into consideration the integration needs both technically and from business perspective. Implementation of new systems and applications must include an integration with the unified identity management solutions and related processes
15. Segregation of duties should be established between access request, access authorization and access administration processes
16. Semi-annual periodic access review should be maintained and approved by the access granting stakeholders.

17. The ability to disable access to certain identity need to managed adequately and swiftly considering it as a time sensitive action.
18. IT and Information Security are data custodians; accordingly, they can't grant access to any identity. Proper data trustee, data domain trustee and other delegated roles are the authorized parties to grant and revoke access to data and systems.
19. Revoking the access can be done by IT and Information Security in special cases to protect AUC information and digital assets whenever appropriate.
20. Application and system function and design capabilities as well as the processed information criticality level should be considered while designing its identity and access management processes and workflows
21. All relevant actions for provisioning, de provisioning, access change...etc. should be documents and its relevant logs should be maintained adequately
22. Access level review and certification should be done at least twice per year.
23. Records and logs of all granting and revoking actions should be maintained at all times in centralized repositories.
24. All old and new AUC solutions and systems whether hosted in AUC or on a cloud should be managed by AUC authorized identity management
25. Access rights should not be granted until the authorization process is complete.

### **Privileged Identity and Access Management**

AUC has privileged administrators who has access to the backbone of AUC systems and digital services/accounts, these digital access keys should be managed and monitored adequately to protect AUC ultimately.

1. Privileged access should be managed properly considering its criticality
2. Privileged access should include all privileged access types on all services, systems and applications. This includes cloud, social media and outsourced systems.
3. Access rights should not be granted until the authorization process is complete
4. Privileged access rights should be assigned to a user ID different from those used for regular business activities. Regular business activities should not be performed from privileged ID
5. Specific procedures should be established and maintained in order to avoid the unauthorized use of generic administration user IDs according to systems' configuration capabilities
6. For generic administration user IDs, the confidentiality of secret authentication information should be maintained when shared (e.g. changing passwords frequently and as soon as possible when a privileged user leaves or changes job, communicating them among privileged users with appropriate mechanisms).
7. The competences of users with privileged access rights should be reviewed regularly in order to verify if they are in line with their duties.
8. Requirements for expiry of privileged access rights should be defined
9. An authorization process and a record of all privileges allocated should be maintained.
10. Access history and commands action logs should be maintained for reference, investigations and auditing needs.
11. Bypassing privileged access management solutions is forbidden at all times, exceptions should be approved by Information Security.
12. All old and new AUC solutions and systems whether hosted in AUC or on a cloud should be managed by AUC authorized privilege identity management

13. All AUC systems and digital services should be managed by AUC defined privilege management control, new systems should be designed to comply from day one before going live.
14. All social media, cloud and outsourced administrative systems should be accessed and managed through AUC defined privilege management controls.

---

## **Related Information**

---

AUC Data Governance Policy  
Information Security Policy  
Electronic Mail Email Policy  
Acceptable Use Policy  
Peer to Peer Sharing Policy

---

## **History/Revision Dates**

---

Origination Date: February, 2018  
Last Amended Date: February, 2018  
Next Review Date: April 2019