

---

Document title: [ **Change Management Policy- August 2018**]

Approval date: [ **August 2018**]

Purpose of document: [ **The purpose of the Change Management Policy is to manage changes to AUC information systems, assets and resources in a rational and predictable manner so that all related stakeholders can plan accordingly. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce negative impact to the user community and to increase the value of Information Resources.**]

Office/department responsible: [ **Information Technology Office, Information Security Office**]

Approved by: [ **Wessam Maher, Principal Campus Information Security 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** ]

---

## **Change Management Policy**

---

### **Policy Statement**

All changes to any Information system, resource or asset must be approved first by Change Management Committee, all changes must be documented and well communicated to all relevant stakeholders.

---

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

The purpose of the Change Management Policy is to manage changes to AUC information systems, assets and resources in a rational and predictable manner so that all related stakeholders can plan accordingly. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce negative impact to the user community and to increase the value of Information Resources.

---

### **Who Approved This Policy**

Wessam Maher, Principal Campus Information Security 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

Responsible University Office: Information Security Office

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

---

## Definitions

---

Term (alphabetical order)	Definition as it relates to this policy
<b>Digital assets/Information Resource</b>	any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.
<b>Data Owner</b>	The manager or agent responsible for the function which is supported by the resource, the individual upon whom responsibility rests for carrying out the program that uses the resources. The owner is responsible for establishing the controls that provide the security. The owner of a collection of information is the person responsible for the business results of that system or the business use of the information. Where appropriate, ownership may be shared by managers of different departments.
<b>Data Custodian</b>	Guardian or caretaker; the holder of data, the agent charged with implementing the controls specified by the owner. The custodian is responsible for the processing and storage of information. For mainframe applications Information Services is the custodian; for micro and mini applications the owner or user may retain custodial responsibilities. The custodian is normally a provider of services.
<b>Change Management</b>	The process of controlling modifications to hardware, software, firmware, application, network, digital infrastructure and documentation to ensure that Information Resources are

	protected against improper modification before, during, and after system implementation. <b>Change:</b> <ul style="list-style-type: none"> <li>• Any implementation of new functionality</li> <li>• Any interruption of service</li> <li>• Any repair of existing functionality</li> <li>• Any change in networking functionality</li> <li>• Any removal of existing functionality</li> </ul>
<b>Scheduled Change</b>	Formal notification received, reviewed, and approved by the review process in advance of the change being made.
<b>Unscheduled Change</b>	Failure to present notification to the formal process in advance of the change being made. Unscheduled changes will only be acceptable in the event of a system failure or the discovery of a security vulnerability.
<b>Emergency Change</b>	When an unauthorized immediate response to imminent critical system failure is needed to prevent widespread service disruption.

---

## **Policy/Procedures**

---

1. Every change to any AUC Information Resources/Digital assets resource such as: operating systems, computing hardware, networks, and applications is subject to the Change Management Policy and must follow the Change Management Procedures.
2. Significance of the change to be defined as a “change” is set by the Change Management Committee CMC procedures and guidelines.
3. All changes affecting computing environmental facilities (e.g., air-conditioning, water, heat, plumbing, electricity, and alarms) need to be reported to or coordinated with the leader of the change management process.
4. A Change Management Committee CMC, appointed by both VP and CTO, will meet regularly to review change requests and to ensure that change reviews and communications are being satisfactorily performed.
5. Information Security Office must be included in Change Management Committee to ensure that AUC information and digital assets are secured at all times adequately. Accordingly, Information Security impact should be delivered to CMC and senior management for any change.
6. A formal written change request must be submitted for all changes, whether scheduled, unscheduled or emergency ones.
7. All scheduled change requests must be submitted in accordance with change management procedures so that the Change Management Committee has time to review the request, determine and review potential failures, and make the decision to

- allow or delay the request.
8. Change requests must fulfill Information Security requirements.
  9. All change requests must receive formal Change Management Committee approval before proceeding with the change.
  10. All change requests must be submitted early enough to provide the Change Management Committee the adequate time to process the request according to its severity, complexity and urgency.
  11. The appointed leader of the Change Management Committee may deny a scheduled or unscheduled change for reasons including, but not limited to, inadequate planning, inadequate backout plans, the timing of the change will negatively impact a key business process such as year ends accounting, or if adequate resources cannot be readily available. Adequate resources may be a problem on weekends, holidays, or during special events.
  12. Customer notification must be completed for each scheduled or unscheduled change following the steps contained in the Change Management Procedures.
  13. A Change Review must be completed for each change, whether scheduled or unscheduled, and whether successful or not.
  14. A Change Management Log must be maintained for all changes. The log must contain, but is not limited to:
    - a. Date of submission and date of change
    - b. Owner and custodian contact information
    - c. Nature of the change
    - d. Indication of success or failure
  15. All AUC information systems and digital assets must comply with an Information Resources change management process that meets the standards outlined above.
  16. Change Management Committee can approve specific changes to bypass the committee approval cycle under certain conditions.
  17. Emergency Changes are allowed as an exception and should be reported officially to the Change Management Committee within 24 hours maximum and labeled as “emergency change”. The action owner need to add VP for Digital Innovation in this report. Change Management Committee has the right to accept or refuse this change. Abuse to this rule is not allowed.
  18. Verbal approvals and communications should be the minimum and if it occurs then it must be documented afterwards officially the soonest.
  19. Proper testing should be performed for any change.
  20. An adequate backup/fall back plan for aborting and recovering from unsuccessful changes and unforeseen events must be in place with clear stakeholders responsibilities and accountabilities.
  21. Proper communication to relevant stakeholders and data owners should be performed at all times when needed.
  22. IT is considered as a data custodian, accordingly any change consequences like possible problems that may happen because of the change or any worst case scenarios must be communicated and approved by the relevant data owners. This communication should be on an appropriate high level business language.

23. A proper inventory to all change management processes, logs and approvals should be in place
24. Change management policy domain is for information systems and digital assets that are already in production and passed the release management processes, however if a new production systems will integrate with other running components then it must be governed by this policy

Any user found to have violated this policy (or part thereof) may be subject to disciplinary action, up to and including termination of employment or dismissal from the University.

---

### **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: June 2018  
Last Amended Date: August 2018  
Next Review Date: October 2019