
Document title: [**Business Continuity and Disaster Recovery Policy - April 2018**]

Approval date: [**April 2018**]

Purpose of document: [AUC should implement a business continuity and disaster recovery plan that cater for the business goals and expectations during disasters. Proper arrangements and actions need to be planned ahead]

Office/department responsible: [**Official AUC Office/Department/Center/School Name – not units**]

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]

Business Continuity and Disaster Recovery Policy

Policy Statement

AUC should implement a business continuity and disaster recovery plan that cater for the business goals and expectations during disasters. Proper arrangements and actions need to be planned ahead.

Reason for Policy/Purpose

To protect AUC services and ensure its continuation during and after disasters.

Who Approved This Policy

Wessam Maher, Principal Campus Information Security Officer

Who Needs to Know This Policy

AUC Faculty
AUC 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, Office of Information Technology

If you have any questions on the policy, you may send an e-mail to infosec@aucegypt.edu

Policy/Procedures

1. Business continuity and disaster recovery activities are focused on AUC business priorities that need to be kept and secured from any damage or disaster while keeping the proper organization resiliency to keep operating during disasters.
2. Business continuity and disaster recovery activities are led by information security office.
3. A proper risk assessment and business impact analysis should be performed periodically as a basis for this activity.
4. A plan copy should be stored in remote location.
5. The plans should be tested regularly; all test should be documented. Different types of tests are recommended.
6. All new information systems should be included in the plans before going live.
7. Redundancy, backup, failover activities should be designed as needed to server AUC business objectives.
8. The plans should be updated and reviewed regularly
9. A proper asset inventory and data inventory should be in place as well as documented business processes.
10. Crisis communication plan should be in place and aligned with the university.
11. Disaster declaration decision should be clearly assigned to responsible persons.
12. Proper communication plan and call tree should be in place.
13. Risk tolerance, Recovery point objective and recovery time objective should be approved from senior management and data owners.

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: April 2018
Last Amended Date: April 2018
Next Review Date: April 2020