
Document title: **Cyber Security Incident Response Policy – January 2018**

Approval date: **January 2018**

Purpose of document: This document addresses the management of cyber security incidents affecting AUC assets and services

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>]

Document includes: [**Policy, charts, appendix and approvers**]

Related documents/see also: [**Information Security Policy, Acceptable Usage Policy**]

Cyber Security Incident Response Policy

Policy Statement

Cyber Security incidents that may occur to AUC assets and services must be reported to the appropriate teams only. Relevant communication to parties other than AUC responsible teams must be restricted. AUC encourages the community to report any suspected incident and will protect the whistleblower identity.

Reason for Policy/Purpose

This policy defines the ways that AUC faculty, staff, students and other third parties doing work for AUC, must respond to a cyber security incident.

The policy defines relevant responsibilities. The policy acknowledges that a quick, effective, practiced, and orderly response is a critical determinant of an incident's outcome. The underlying motivation for this policy is to help assure that AUC information systems continue to be trustworthy, available, and reliable.

Who Approved This Policy

Nagwa Nicola, Chief Technology Officer

Who Needs to Know This Policy

Entire AUC community including whoever has an access to AUC digital resources like visitors, contractors, consultants...etc.

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

Definitions

Term (alphabetical order)	Definition as it relates to this policy
cyber security incident	Any information systems related event involving a violation of the law, or a violation of AUC security policy. Such an incident may alternatively involve any significant disruption of AUC production information systems, or any information systems related event that seriously jeopardizes the security or privacy of AUC property or interests. An incident may alternatively involve the information-systems-related compromise of the welfare of AUC community, customers, business partners, or stakeholders. Examples of cyber security incidents include hacker intrusions, virus infestations, web site defacements, and denial of service attacks.
AUC Community	Includes faculty, staff, students, alumni, donors and whoever has an access to AUC digital resources
Cyber Security Incident Response Team (CSIRT),	Group of skilled information technology specialists who have been designated as the ones to take action in response to reports of cyber security incidents

Policy/Procedures

Scope of Duties

AUC staff and faculty are expected to be present, and to assist to the best of their abilities, with the restoration of normal business activity after an emergency or a disaster disrupts AUC business activity. Such an emergency or disaster could stem from a cyber security incident, violation or problem. After faculty's and staff's family and personal assets are determined to be safe, employees are expected to put in overtime, work under stressful conditions, and otherwise within reason to do whatever it takes to maintain AUC as a going concern.

Users must not attempt to deal with cyber security incidents, violations or problems without expert technical assistance. Technical responses to cyber security incidents, violations and problems must be handled exclusively by AUC Information Security Office staff, AUC Cyber Security Incident Response Team (CSIRT), and/or others who have been authorized by AUC Principal Campus Information Security Officer.

Cyber Security Incident Response Team (CSIRT) is a group of skilled information technology specialists who have been designated as the ones to take action in response to reports of cyber security incidents. CSIRT is responsible for preparing, maintaining, and periodically testing response procedures to a variety of cyber security incidents that can occur to AUC.

Reporting Incidents to Appropriate Internal Parties

All AUC community have a duty to report cyber security incidents, violations and problems to the IT Help Desk on a timely basis so that prompt remedial action may be taken. It is not the job of non-technical workers to assess the severity or the urgency of these incidents, violations and problems. The Designated Incident Coordinator who is then on-duty, the person identified by the Principal Campus Information Security Officer to immediately respond to all such reports, will make this assessment.

In the course of doing their work, many community users come across information security alerts, warnings, descriptions of suspected vulnerabilities, and the like. All of these should be forwarded to the IT Help Desk, and they will in turn be sent to the Designated Incident Coordinator. Users are prohibited from utilizing AUC information systems to forward such information to other users, whether the other users are internal or external to AUC.

In general, all unusual and/or suspicious information-security-related events must be promptly reported. These events include unusual and troublesome requests for AUC internal information coming from an external party, previously unseen dysfunctional information system behavior, suspected cyber virus infestations, erroneous information systems results, and information system down conditions. Unauthorized disclosure of sensitive AUC information, or sensitive information belonging to a third party that has been entrusted to AUC, must also be reported via the IT Help Desk.

Reporting Incidents to Third Parties

Unless previously approved by the Information Security Office, AUC community members must not report cyber security incidents, problems, and/or violations to any outside parties. These parties include news reporters, researchers compiling statistics on cybercrime, independent organizations compiling technical reports about incidents, and/or professional society members.

Likewise, AUC community members who discover a weakness or vulnerability in the information security measures used by AUC must not discuss these matters with anyone other than the Designated Incident Coordinator, the Information Security Officer, the Internal Audit Manager, or trained investigators designated by one of these two managers. Open discussion of these weaknesses or vulnerabilities may lead to their exploitation by unauthorized parties. An exception of course is provided those who are authorized to work directly on information

security matters. In the case of incidents involving CJIS-related sensitive information, such incidents shall be escalated to Principal Campus Information Security Officer.

Privacy and Protection of Workers Reporting Incidents

Any attempt to interfere with, prevent, obstruct, or dissuade AUC community in their efforts to report a suspected cyber security incident, problem or violation is strictly prohibited and cause for disciplinary action. Any form of retaliation against an individual reporting cyber security incidents, problems or violations is also prohibited and cause for disciplinary action.

AUC will protect its community members who in good faith report, through the communications channels mentioned in this policy, what they believe to be incidents, violations or problems. This means that these workers will not be terminated, threatened, or discriminated against because they report what they perceive to be a vulnerability, wrongdoing or dangerous situation. If a reasonable period of time has elapsed since their first report, and these workers believe that no action is being taken about an on-going serious condition, then they must report the problem to their immediate supervisor or the Internal Audit Manager. Before they make this second report, workers must give responsible department a reasonable period of time to remedy the situation.

AUC community members who report a cyber security incident, violation or problem within AUC may, at their sole discretion, have their identity held in strict confidence. This means that the whistleblower's identity will be shielded in all subsequent uses of the information, including investigations and resolutions of the matter. An exception to this shielding must be made in those cases where a government agency, such as a court of law, requires the disclosure of the whistleblower's identity.

History/Revision Dates

Origination Date: January 16th, 2018

Last Amended Date: January 16th, 2018

Next Review Date: April 2020