

---

Document title: **Log File Access and Retention Policy– February 2018**

Approval date: **February 2018**

Purpose of document: **This document addresses the management of access and retention of security log files.**

Office/department responsible: **Information Security Office, Office of Information Technology**

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]

---

## **Log File Access and Retention Policy**

---

### **Policy Statement**

---

Applications and systems logs are important to AUC for many business and compliance reasons, they need to be protected stored and retained adequately.

---

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

---

Due to the need of business to keep good standing digital systems and protect the data that it holds, accordingly managing and governing the logs access and retention became a must to keep AUC compliant, secure as well as achieving its business goals

---

### **Who Approved This Policy**

---

Nagwa Nicola, Chief Technology Officer

---

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

---

All AUC Staff and Faculty  
All Application Administrators  
All System Administrators  
All units/departments that deal with logs

---

## 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)

---

## Definitions

---

Term (alphabetical order)	Definition as it relates to this policy
Log files	Records (mostly text files) that are created automatically during system operation and contain entries about the events that happened in a system. They are vital for systems troubleshooting and analysis. For example Web Servers automatically save usage and activity information such as the date, time, IP address, HTTP status, bytes sent, and bytes received

---

## Policy/Procedures

---

Log files created by AUC systems and digital services should be kept and stored. All AUC systems and digital services should be configured to enable the proper level of logging details that is accepted to meet business, compliance, troubleshooting, information security needs

IT are considered data custodians, hence they are responsible for enabling and keeping the logs existing and authentic as well as any business user who has the ability to deal with logs

### **ACCESS TO LOG FILES**

While the usage logs covered under this policy do not contain personally identifying information, the logs are classified by AUC as confidential data. The reason for this is that the log files used in conjunction with other information that central IT has in its custody may allow us to associate specific information on the use of a service, such as specific Web page access, with a given individual's computer.

AUC will comply with a court order or valid subpoena that requests the disclosure of information contained in usage logs.

Information Security office is responsible for conducting Information security investigation and digital forensics activities with regards to any AUC's digital nature subjects. Also, the office is responsible for collecting and validating any digital information/logs and act as a central point of contact with any investigation parties whether internally or externally. Accordingly, Information Security office has the right to request data, meta data and technical

logs and history input from AUC system's owners and administrators within the investigation's scope and through a documented communication.

### **RETENTION OF LOG FILES**

Log file retention times are specified in the Retention Guidelines for Log Files. If a log file contains relevant information that is useful for future reference, a pending transaction, or as evidence of a management decision, it should be retained. If a log file is needed for these purposes, it is the responsibility of IT staff to move these specific logs to another central IT-owned system prior to the destruction of the log (even after it has reached its maximum retention time).

### **DESTRUCTION OF LOG FILES**

Log files must be destroyed in accordance with the Retention Guidelines for Log Files. All original, backups, and copies of logs should be destroyed. For this reason, log files should not be backed up to removable media and should stay on the centralized log server or the local file system of the machine on which they are generated. In addition, care should be taken to exclude log files from computer disk images. This policy recommends deleting log files as opposed to log entries. Logs should be destroyed in the most destructive and economical way available. Actual deletion method is specified in the Retention Guidelines for Log Files.

---

## **Related Information**

---

AUC Data Governance Policy

<https://documents.aucegypt.edu/Docs/Policies/Data%20Governance.pdf>

Information Security Policy

<https://documents.aucegypt.edu/Docs/Policies/Information%20Security%20Policy.pdf>

---

## **History/Revision Dates**

---

Origination Date: February, 2018

Last Amended Date: February, 2018

Next Review Date: April, 2019