Table of Contents

Log-in Monitoring 1
University Internal Standard 1

Log-in Monitoring

University Internal Standard

OIT has an internal standard for logging, monitoring and auditing that applies to all servers managed by CU Denver OIT. Click her to view the version that was effective as of July 1, 2017. Please contact OIT's Risk and Compliance team for the most up to date version.

According to the standard the following details are logged and saved on a centralized logging server for at least six months:

1. Timestamp
2. Event, status, and/or error codes
3. Service/command/application name
4. User or system account associated with an event
5. Device used (e.g. source and destination IPs, terminal session ID, web browser, etc)

The events related to the following categories are logged:

1. Operating System(OS) Events
2. OS Audit Records
3. Application Account Information
4. Application Operations
5. File Access (files containing ePHI or Highly Confidential information)

HIPAA Policy 9.3 Auditing
http://www.ucdenver.edu/research/Research%20Administration%20Documents/9.3%20Auditing.pdf

From:
https://wiki.cu.studio/ - **SEHD Wiki**

Permanent link:
https://wiki.cu.studio/policy/data_privacy/log-in_monitoring?rev=1559759098

Last update: **2019/06/05 18:24**