DEFINITIONS

"***Integrity***" is the maintenance of, and the assurance of the consistency, accuracy, and trustworthiness of data over its entire life cycle. Any unintended change to data as the result of a storage, retrieval or processing operation, including malicious intent, unexpected hardware failure, and human error, is failure of data integrity.

STANDARD

1) Restricted Information must be protected from unauthorized alteration or destruction by implementing reasonable and appropriate measures to facilitate the maintenance of reliable systems, workflows, and data.
2) Technical and procedural mechanisms shall be implemented to corroborate that systems and data have not been altered or destroyed in an unauthorized manner. System and/or data owners will determine the type of mechanism(s) to employ as follows:
    a) Technical mechanisms. System and/or data owners shall implement electronic mechanisms (e.g., error-correcting memory, appropriate types of RAID arrays, uninterruptible power supplies, watchdog timers, cluster file systems, checksum technology, cryptographic hash functions, digital signatures, anomaly detection and file protection systems) when such mechanisms are available, employable and commensurate with the criticality and risk associated with the system and/or data.
    b) Procedural mechanisms. If technical mechanisms are not available or employable, or in order to augment technical mechanisms, system and/or data owners shall implement procedural mechanisms (e.g., manual data validation) when such mechanisms are appropriate, based on the criticality and risks associated with the system and/or data.
3) System and/or data owners shall establish mechanisms and procedures (e.g., backup verification, hardware and software reviews) to perform periodic checks of data and system functionality to identify integrity issues (e.g., corrupted data, failing hardware, software errors). The frequency of system and data integrity checks will be commensurate with the criticality and risks associated with the system and/or data.

EXCEPTIONS

Any exceptions from this standard must be approved by the UCLA Health Sciences Chief Compliance Security Officer.

QUESTIONS

1) If you have questions on how to implement integrity control for your system and/or data, please contact your IT Support Group.
2) If you have questions about this Standard, please contact the Office of ComplianceServices – Information Security (InfoSecAll@mednet.ucla.edu)

REFERENCES

HS Policy No. 9457, "*Minimum Security Standards for Network Devices*"
45 CFR § 164.312(c)(1), 164.312(c)(2), and 164.312(e)(2)

CONTACT

Chief Compliance Security Officer, Office of Compliance Services

REVISION HISTORY

Created Date: January 28, 2019