Name of Policy: Technology backup, disaster Readiness, and recovery policy **Policy Number**: 3364-65-09 **Approving Officer**: President **Responsible Agent**: Vice President, CIO/CTO **Scope**: All University organizational units	**Revision date:** September 11, 2020 **Original Effective date**: July 28, 2008

☐	New policy proposal	☒	Minor/technical revision of existing policy
☐	Major revision of existing policy	☐	Reaffirmation of existing policy

(A) Policy statement

Information technology is an integral part of how the university carries out its mission. The university is committed to ensuring that vital technology resources and information stores are appropriately prepared to support recovery and business resumption efforts following accidental deletion, system corruption, and/or physical loss or damage.

(B) Purpose

To ensure that the university's technology procurement and development life cycle incorporates disaster recovery and back-up methodologies that will enable recovery and subsequent business resumption following accidental or malicious deletion, system corruption, and/or physical loss or damage.

(C) Scope

Compliance with this policy is mandatory for all university organizational units that create, store, process, transmit, or receive data vital to the university's mission, and for all university organizational units which procure, develop, operate, maintain, or dispose of technology assets vital to the university's mission, including telecommunications and network

infrastructure, data center environmental controls, servers, data storage systems, workstations, and other devices.

(D) Backups

Reasonable backups of data and technology assets vital to the university mission must be prepared at appropriate intervals and be reasonably available for restoration for an appropriate retention period. Except as otherwise determined by the vice president, CIO/CTO or delegate, a full or incremental system backup prepared daily is considered reasonable if the backup is available for at least two weeks (fourteen calendar days) from the time taken and stored not less than three miles from the site of the original data or technology asset.

(1) All data and technology assets sited within the university's main campus university computing center ("UC") or health science campus Dowling Hall ("DOW") datacenters are backed up by Information Technology via an appropriate mechanism at reasonable intervals and retained for reasonable periods of time.

(2) Data and technology assets owned, operated, or maintained under a contractual arrangement, including "cloud" service providers of infrastructure, platforms, or software are backed up subject to the terms of the service provider's contractual agreements with the university.

(3) Except as directed by the vice president, CIO/CTO or delegate, data and all other technology assets, including servers, workstations and other device assets not sited within the UC or DOW datacenters are not backed up by Information Technology. Until directed otherwise by the vice president, CIO/CTO or delegate, backup of data or technology assets vital to the university mission must be accomplished by an operator or other user of the asset. In such cases, Information Technology is not responsible for the loss of data saved to a workstation or device. To minimize risk of loss of vital data, such data should be saved to network shares provided by Information Technology.

In addition to the requirements set forth in this policy, the conduct of backup activities must comply with all other university policies and applicable privacy, security, and compliance obligations, including

those university policies concerning the encryption and secure destruction and sanitization of data and electronic storage media.

(E) Disaster readiness

Data and technology assets vital to the university mission must be made reasonably prepared to respond to an accidental or malicious deletion, system corruption, and/or physical loss or damage event. Except as otherwise determined by the vice president, CIO/CTO or delegate, reasonable preparations include system backups as described in this policy, current hardware and software support contracts, and reasonable availability of personnel versed in operation and restoration of the asset or data.

(F) Disaster recovery

Data and technology assets vital to the university mission must be recovered within a reasonable time in the event of accidental or malicious deletion, system corruption, and/or physical loss or damage. Except as otherwise determined by the vice president, CIO/CTO or delegate, a reasonable recovery is initiated within one business day of discovery of an accidental deletion, system corruption, and/or physical loss or damage event.

(G) Applicable guidance

Consult the following authorities for specific requirements for backup, disaster readiness, and recovery of data and technology assets within the university's clinical environments:

(a) CFR §164.308, §164.310, and §164.312 for the University's HIPAA covered entity components;

(b) Joint Commission standard IM.2.30 for continuity of information

Approved by: /s/ Gregory C. Postel, M.D. Interim President September 11, 2020 Date Review/Revision Completed by: Senior Leadership Team Vice President, CIO/CTO	**Policies Superseded by This Policy:** • *3364-65-04, effective date December 10, 2012* • *Policy number changed from 3364-65-04 to 3364-65-09 effective January 12, 2017* Initial effective date: July 28, 2008 Review/Revision Date: December 10, 2012; January 12, 2017, September 11, 2020 **Next review date: September 11, 2023**