3356-4-09.2 Storage of electronic data.

(A) Policy statement. Electronic data is a strategic asset of Youngstown state university ("university") and is critical to the success of the university. The university, through its information technology services ("ITS"), utilizes technologies to ensure data integrity and to prevent data loss and unauthorized access of data.

(B) Purpose. To protect the electronic data and information belonging to or held by the university through the establishment of acceptable data storage resources and the minimum acceptable standard of university network data storage.

(C) Scope. This policy applies to all university employees, students, affiliates, and all others granted access to university data or information systems.

(D) Definitions.

(1) "Network Storage." Network accessible service(s) provided by the university and maintained by ITS for the purpose of electronically retaining university data.

(2) "University data." Any and all data and records created, collected, stored and/or managed in connection with the operation and management of the university. Unless superseded by specific regulations, university policy, terms of sponsorship or other agreements, the university owns all research data generated or acquired by university employees (faculty and staff) or non-student trainees or fellows (not employed by the university) through research projects conducted at or under the auspices of the university, regardless of funding source.

(3) "Store." Electronically commit data as retrievable records.

(E) Parameters.

(1) The university's ITS office will establish, and when appropriate, revise guidelines and/or best practices for the required storage of university data on university network storage and/or cloud/hosted storage as vetted and approved by ITS. As part of this service, ITS will work to ensure best practice backup, security, disaster

readiness and continuity of university data. By design, access to data on network store(s) will be appropriately and significantly enhanced.

(2) ITS will facilitate connectivity to appropriate network storage at the time university computers are deployed on-campus for faculty and staff. Correspondingly, ITS will implement systems and services such that data is stored appropriately within those systems.

(3) Storage associated with cloud/hosted service(s) as approved by ITS will also be acceptable.

(4) University employees choosing to store data locally in addition to required network storage are responsible for the setup, care, maintenance, and migration of such data.

(5) This policy does not modify or eliminate responsibilities identified in rule 3356-4-02 of the Administrative Code (see university policy 3356-4-02, "Surplus property") or any other applicable administrative rule or university policy.

(6) Guidelines and requirements for the storage of electronic data are available on the ITS home web page.

(F) Security Incident. Individuals granted access to university data or information systems must report any known security incident or any incident that is likely to cause a disclosure of sensitive information to unauthorized parties by contacting the university's tech desk. Security incidents include but are not limited to the theft or loss of a computer device, the introduction of malicious software, or other misconfiguration that may lead to unauthorized access to confidential or sensitive information.

(G) Enforcement. The university reserves the right to monitor network traffic, perform random audits and to take other steps to ensure the integrity of its information and compliance with this policy.

(H) Violations. Violation(s) of this policy may result in appropriate disciplinary action, up to and including termination, temporary or permanent restrictions on information access/networks, and criminal and/or civil action.

Effective: 8/6/2018

CERTIFIED ELECTRONICALLY

Certification

07/26/2018

Date

Promulgated Under:	111.15
Statutory Authority:	3356
Rule Amplifies:	3356