NJIT

New Jersey Institute of Technology
University Policies and Procedures **Date of Issue: July, 2016**

Subject: **Records Retention Policy**

POLICY STATEMENT

This policy addresses the proper retention and management of NJIT's records, as defined below, in accordance with N.J.S.A. Title 47 (Public Records) and N.J.A.C. 15:3 et seq (Records Retention) and other related statutes, including FERPA, HIPAA and OPRA. The State Division of Archives and Records Management require all public entities to preserve their records and prohibits their destruction except in accordance with its Schedule for Four Year Colleges. The following guidelines will promote the efficient identification and administration of records for proper storage or disposal, elimination of accidental destruction of records, and reduction of the unnecessary storage of records.

This policy applies to all university departments, offices, administrators, faculty and staff. All NJIT employees responsible for the creation, maintenance, receipt, storage, or use of university records must familiarize themselves with this policy and the record retention schedule(s) pertinent to the records within their purview.

DEFINITION OF UNIVERSITY RECORD

University records for the purposes of this policy are defined as any record created, produced, executed or received by any university department, office or employee in the course of institutional activity. NJIT records may include papers, correspondence, books, plans, microfilm, maps, photographs, sound and moving image recordings, and other documentary materials.

University records may also be created or stored through non-tangible electronic means; such records may encompass both analog and digital information formats. Electronic records may include but not be limited to emails, text messages, word processing documents, digital photographs, video recordings, formatted data, databases, and records existing in a university computing cloud.

Regardless of format or creation, all university records are considered property of NJIT. The retention schedule for university records is attached to this policy for guidance purposes. No document list or schedule can be exhaustive and any determination regarding the

identification, storage, retention, or disposal of any record not identified on the schedule must be made in consultation with the Custodian of Records.

ADMINISTRATION OF RECORDS POLICY

The General Counsel, or his/her designee, shall be responsible for the administration of this policy. Under the Office of General Counsel's direction, all department heads and supervisors are responsible for ensuring that university records in his/her unit are stored or disposed of in a manner consistent with this policy.

All requests for the disposal of university records shall be made in writing to the Custodian of Records and must include the proposed method of disposal. No records shall be destroyed or disposed until the Custodian of Records has approved the request in accordance with law. Additionally, the Custodian of Records may determine that certain university records may not be disposed of, even where the retention period has been reached, because the disposal of the records may violate contractual obligations, the records are related to current or potential litigation or investigation/audit, and/or the records have significant or historical value to NJIT.

In the cases of current or potential litigation, NJIT is under a legal obligation to preserve all records related to the litigation. The Office of General Counsel will issue a litigation hold letter to the relevant employees directing them to preserve all related evidence within their control. Any litigation hold will override record retention schedules or disposal requests. Employees who have been notified of a litigation hold may not alter or destroy any record that falls within the scope of the litigation hold.

Records containing research or information related to protected health information are also subject to HIPAA regulations. Protected health information means individually identifiable health information that relates to the past, present or future health or condition of an individual, the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual and identifies or could reasonably be used to identify the individual. Protected health information excludes individually identifiable health information found in (a) education records covered by FERPA and (b) employment records held by a covered entity in its role as an employer.

MANAGEMENT OF RECORDS

All university records must be properly maintained during their retention period via means that ensure their accessibility, security, and protection from damage, theft or destruction. Records that are considered unnecessary for current university use may be stored with an authorized vendor for offsite storage. While records must be made easily retrievable for examination or use by appropriate employees, measures should be taken to protect confidential information, including personally sensitive and/or protected health information, from unauthorized access. Confidential information includes records that contain an individual's name together with personal identifying information such as his/her social security number, financial account, credit card, or password. Confidential information should be safeguarded and secured at all times.