Title: Data Protection & Retention Policy
Policy Number: E1005
Responsible Office: ITS
Originally Issued: April 2019
Last Revised Date: July 2022
Last Reviewed: July 2022

TITLE OF THE POLICY
Data Protection & Retention Policy

PURPOSE OF THE POLICY
The purpose of this Policy is to ensure that necessary records and documents of Wake Technical Community College (WTCC) are adequately protected and maintained and to ensure that records that are no longer needed by WTCC or are of no value are discarded at the proper time and in accordance with Wake Tech Policy and applicable legal requirements. This Policy is also for the purpose of aiding employees and staff in understanding their obligations in protecting electronic documents - including e-mail, Web files, text files, sound and movie files, PDF documents, or other formatted files.

APPLICABILITY
This policy applies to all WTCC staff and systems involved in collecting, managing, and storing information assets (whether written or electronic).

POLICY STATEMENT
Data protection and retention are critical components of the data management lifecycle. The data and records listed within this policy will be retained for as long as there is a business need, or as required by applicable compliance, regulatory and legal standards. In addition, the data must be appropriately safeguarded to ensure only authorized individuals with legitimate business reasons can access it. As data retention can become costly, it will be disposed according to the Data Retention Schedule contained within the policy. This policy addresses required basic security and privacy controls, as well as reflecting the constraints placed upon WTCC by legislation and regulations.

DEFINITIONS

Word/Term	Definition
Asset	Property owned by a person or the college. Examples: laptops, servers, cellphones, cameras, and storage devices.
Cipher Suite	A set of methods (algorithms) used to secure a network connection.
College network	Any asset, system or network (physical, wireless, or other) owned and operated by Wake Tech.
Data	Information that is submitted or collected by Wake Tech through the course of business.
Encryption	The process of encoding data in a way that only authorized parties can access it, and unauthorized parties cannot.
File Permissions	A set of controls applied to electronic files that assign permissions or access rights to specific users or groups that limit the ability to view, change, navigate or execute the contents.

Insecure	Not protected by college services, including, but not limited to; antivirus, event logging, intrusion prevention, access controls, and physical locks or other security.
Internet of Things (IOT)	Any device connected to the internet that's enabled to send or receive data, usually lacking a user interface. *Examples*: Amazon Alexa, Raspberry Pi, and Apple HomeKit.
Public Records	Any record, regardless of physical form or characteristics, made or received in connection with the transaction of public business.
Regulatory Standards	Benchmarks created by a regulatory agency, created to enforce the provisions of a legislation. *Examples*: GLBA, PCI, and FERPA.
Retention	The continued possession, use, or control of data.
Sensitive Information	Any information or set of data that could have an adverse impact on an individual, or the college, in the event of exposure.
User	Any individual or third party accessing the Wake Tech network or other college owned assets.

PROCEDURES

Information Classification

All data is classified into one (1) of three (3) information classifications:

- Public
- Confidential
- Restricted

Public

Applies to information that is a public record under applicable law and has been approved by WTCC management for release to the public. By definition, there is no such thing as unauthorized disclosure of this information, and it may be disseminated without potential harm.

Confidential

Applies to less-sensitive business information that is intended for use within WTCC. Its unauthorized disclosure could adversely impact WTCC or its students, suppliers, business partners, or employees.

Restricted

Applies to the most sensitive business information that is intended for use strictly within WTCC. Its unauthorized disclosure could seriously and adversely impact WTCC, its students, its business partners, and its suppliers. This includes Personally Identifiable Information (PII, also known as Personal Data) or other sensitive information (see below for definition by NIST– reference Appendix A for more information).

1. PII is any information about or that can be directly attributed to an individual and processed or maintained by WTCC;
2. Any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and
3. Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Due to the potential personal or business impact arising from misuse, or unauthorized access to or use of, Confidential and Restricted data, it is only stored in secure environments. As such, PII and other sensitive data will not be stored or processed on publicly accessible or insecure assets, including, but not limited to;

work or personal laptops, tablets, cellphones, Internet of Things devices (IOT), portable media (USB, CD, Floppy-Disk), or other non-college owned devices. Further, these data types are prohibited from being emailed, texted, or otherwise transported outside of the College network. If there is a legitimate college need to transport these types of data, proper encryption and security mechanisms will be used to ensure confidentiality (reference Portable Device section).

Any incidents, or potential incidents, involving Confidential or Restricted data will be subject to an investigation as outlined in the Cybersecurity Program and Incident Response Policy.

Maintenance of Records

All platforms used by WTCC to create, receive, transmit or manage electronic records, including e-mail clients, social media platforms, and cloud computing platforms, shall conform with all Department of Natural and Cultural Resources policies and all applicable IT security policies.

Security of the system and the records it holds is maintained in the following ways:

- Access rights are managed by the IT department and are assigned by a supervising authority to prevent unauthorized viewing of documents.
- Either the information technology system can separate confidential from non-confidential information, or data creators must organize and name file systems in such a way to identify confidentiality of the documents.
- Folders with confidential information are restricted, and access rights to confidential data are carefully managed using least privilege and strict access controls. Confidential material is redacted before it is shared or otherwise made available.
- Physical access to computers, disks, and external hard drives is restricted.
- All system password and operating procedure manuals are kept in secure storage.

WTCC maintains documentation that describes system procedures, practices, and workflows. This documentation also identifies system software and hardware and captures the system environment in terms of the organizational structure, functions and responsibilities, and system processes. Documentation is reviewed and updated by IT staff annually or upon implementation of a new information technology system.

Retention Requirements

Under the direction of the CIO, the Cyber Security Engineer or another designee shall:

- Implement data retention and disposal guidelines limiting data storage and retention times to those that are required for legal, regulatory, and business requirements
- Ensure automatic or manual processes exist for the secure destruction of paper and electronic records when no longer needed
- Follow specific retention requirements for sensitive data as set forth by this policy
- Identify retention periods for log files and audit trails
- Define and enforce email retention requirements

Different types of records require varying retention periods. In addition to describing how long various types of information must be maintained, retention procedures shall specify:

- Steps used to archive information and locations where this information is processed and stored.
- The appropriate destruction of electronically stored information after the identified retention period.

Additionally, WTCC utilizes strong encryption and cipher suites to protect Confidential and Restricted information, as outlined in the 'Encryption' section of this policy.

Data Retention Schedule

Records retention and management is an important component of the compliance process. WTCC needs to store and manage information on general operations, student records, and finance as part of day-to-day activities. As part of a retention scheme, classes of documents are retained on different schedules based on various criteria.

In certain instances, individual departments may have unique record retention requirements outside of documented groups. These shall be documented independently as part of internal processes and procedures, such as "Learning Management System (LMS) Records Retention Schedule" in Chapter 8 of the Employee Handbook. Such requirements may include contractual obligations with customers or business contacts or data retention requirements to maintain business operations. In some instances, departments may need to retain electronically stored information for a historical archive with a different retention schedule than listed below.

During the appropriate retention period for electronic records, archived data must be retrievable. Doing so shall require the following protocols to be in place:

- As new software and/or hardware is implemented, ITS support staff shall ensure new systems and file formats can read legacy data. This may require that older data be converted to newer formats.
- Data that is encrypted must be retrievable. WTCC shall implement key management procedures that ensure encrypted data can be decrypted when needed.

When establishing record retention periods, WTCC shall rely on (in order of precedence):

- Applicable federal guidelines, laws, statutes, and Regulatory Standards
- State guidelines, recommendations, rules, and statutory requirements
- Any WTCC policy and procedure enhancing existing federal and state retention periods

The listing below is not representative of every record type maintained at the college and is specific to ITS.It is expected that as technology evolves, so too does the need to retain additional data types from more complex systems. As such, additional sets of data may be retained internally and may be available upon request.

Data Type	Data Retention Schedule	Description
Email	All messages and other items moved to archived storage will be permanently deleted after five (5) years.	All electronic mail messages will be automatically copied to archived storage as soon as they are sent or received by the email gateway.
Social Media	At least (1) year from the creation date.	Any publicly visible posting, either sourced internally or externally, on any social media page owned by the College.
Instant Messaging	At least (1) year from creation date.	Any Microsoft Teams or Skype messages that

		contain sensitive information or select key words.
Event Logs	At least (1) year from the creation date for forensics and PCI compliance.	All event and security logs created from activity on a computer system.
Audit Reports & Materials	At least (3) years from the date of the audit.	All audit reports, audit materials, correspondence, and other working papers.
Enterprise Resource Planning (ERP) Data	Retained Indefinitely	All data stored or processed within the ERP solution, to be used for tax laws, regulations, and other legal requirements.

Data Loss Prevention

All Confidential and Restricted data within the College's possession cannot be transmitted externally, without being subject to Data Loss Prevention (DLP) policies, rules, and technical controls. This is to ensure that information is only being shared with authorized parties, for authorized business purposes. As such, it limits the possibility of a sharing data outside of the College. This is performed by using several technical and administrative controls together, including IPS, IDS, firewalls, anti-virus systems, inbound and outbound email filtering, system controls enforced by group policy, and Role Based Access Controls (RBAC).

Encryption

WTCC uses software encryption to protect Confidential Information. To provide the appropriate security while balancing throughput and response times, encryption key lengths should use current industry standard encryption algorithms for Confidential Information. These encryption keys will be retained for as long as the encrypted data remains on the College network. The use of proprietary encryption algorithms is not allowed unless reviewed by qualified experts outside of the vendor in question and approved by WTCC management.

Data at Rest

Hard drives that are not fully encrypted (e.g., disks that one or more un-encrypted partitions, virtual disks) but connect to encrypted USB devices, may be vulnerable to security breach from the encrypted region to the unencrypted region. Full disk encryption avoids this problem and shall be the method of choice for user devices containing Confidential Information or PII. Additionally, such data is also protected by NTFS and other file permissions, whereby only users with appropriate access can access the data.

Data in Transit

In-transit encryption refers to transmission of data between endpoints. The intent of these policies is to ensure that Confidential Information or PII transmitted between companies, across physical networks, or wirelessly is secured and encrypted in a fashion that protects student Confidential Information or PII from a breach. The following practices and procedures shall be adhered to when sending data:

- Formal transfer policies, protocols, procedures, and controls are implemented to protect the transfer of information using all types of communication and transmission facilities.
- Strong cryptography and security protocols (e.g., TLS, IPSEC, SSH, etc.) are used to safeguardConfidential Information or PII during transmission over open public networks.
- Confidential Information or PII transmitted in e-mail messages are encrypted.

Portable Devices

Portable devices (e.g., smart-phones, flash cards, SD cards, USB file storage, CD-ROM) represent a specific category of devices that contain data-at-rest. Many incidents involving unauthorized exposure of Confidential Information or PII are the result of stolen or lost portable computing devices. The most reliable way to prevent exposure is to avoid storing Confidential Information or PII on these devices.

However, in situations requiring Confidential Information or PII to be stored on such devices, encryption and file permissions reduce the risk of unauthorized disclosure in the event that the device becomes lost or stolen. To further mitigate the risk of data loss, these devices will be kept in a physically secure location with only authorized parties having access. Additionally, data will be deleted as soon as operationally viable and will not be connected to insecure assets.

Data Destruction and Disposal

All computer desktops, laptops, hard drives, and portable media must be processed through ITS for proper disposal. Paper, hard copy, and electronic records shall be disposed of in a secure manner as outlined below.

Physical Print Media

Printed media shall be disposed of by one (or a combination) of the following methods:

- *Shredding* - Media shall be shredded using cross-cut shredders
- *Shredding Bins* - Disposal shall be performed using locked bins located on-site using a licensed and bonded information disposal contractor
- *Incineration* – Materials are physically destroyed using licensed and bonded information disposal contractor

Electronic Media

Electronic media consists of; physical disks, tape cartridge, CDs, printer ribbons, flash drives, printer and copier hard-drives, virtualized storage, etc. These types of media shall be disposed of by one of the methods:

- *Overwriting Magnetic Media* - Overwriting uses a program to write binary data sector by sector onto the media that requires sanitization
- *Degaussing* - Degaussing consists of using strong magnets or electric degaussing equipment to magnetically scramble the data on a hard drive into an unrecoverable state
- *Physical Destruction* – implies complete destruction of media by means of crushing or disassembling the asset and ensuring no data can be extracted or recreated

IT documentation, hardware, and storage that have been used to process, store, or transmit Confidential Information or PII shall not be released into general surplus until it has been sanitized and all stored information has been cleared using one of the above methods. In the event that records are requested for litigation, all data destruction and disposal will be immediately ceased until the litigation or investigation is over.

Availability of Records for Outside Inspection

WTCC recognizes that during the course of legal proceedings and government investigations, requests may be made, and subpoenas may be issued for pretrial discovery of records and materials, and regarding the information technology system used to produce records and related materials. Provided that such requests and subpoenas are valid, and the College is required to make records and materials available, records must be available for production and/or inspection and audit by government representative for the full period required

by law and approved records retention schedules, regardless of the life expectancy of the media on which the records are stored. Records must continue to exist when litigation, government investigation, or audit is pending or imminent, or if a court order may prohibit specified records from being destroyed or otherwise rendered unavailable.

WTCC will also permit inspection and/or coping of records and materials when required by North Carolina's public records law (N.C. G.S. § 132). WTCC should produce the records created and used in the course of business, maintaining established folder structure as applicable. WTCC should produce records in any format it can produce if asked by the requesting party; however, WTCC is not required to create or compilea record that does not already exist.

Compliance and Liability
It is the responsibility of each Manager and Director to ensure enforcement with the policies above. Additionally, computer users should not bring in unauthorized computers, wireless access devices, or laptops for connection to the administrative network.

The College will not be liable for personal data, such as social security numbers, that resides on a non-college issued laptop or other storage device under the employee or student's control. Such devices cannot be controlled by the College, and the computer user accepts responsibility and liability for the security of their personal data. It is important that such users take necessary security measures to protect their personal device, such as using an anti-virus solution, keeping their PC updated, and being aware of the content they view or download.

Any violation of the Data Protection and Retention Policy can result in disciplinary actions in accordance with Wake Tech's Employee Handbook, including restriction or possible loss of privileges, suspension, termination, or referral to law enforcement. The Office of the CIO shall verify compliance with this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner. If you believe that sensitive data may have been comprised, please notify ITS and the Chief Information Officer immediately.

Complying with this policy will increase the reliability and accuracy of records stored in information technology systems and will ensure that they remain accessible over time. Exhibiting compliance with this policy will enhance records' admissibility and acceptance by the judicial system as being trustworthy.

RELATED POLICIES, PROCEDURES, REFERENCES, FORMS, OR TERMS

Type	Name	Location
Reference	Payment Card Industry Data Security Standard (PCI-DSS) version 3.2.1	Perform web search for "PCI 3.2.1" https://www.pcisecuritystandards.org/document_library
Reference	State Archives of NC – Digital Records Policies and Guidelines	Perform web search for "State archives of NC". https://archives.ncdcr.gov/government/digital-records/digital-records-policies-and-guidelines
Policy	Learning Management Systems (LMS) Records Retention Schedule	Employee Handbook – Chapter 8 https://go.waketech.edu/employee/er/eh/Pages/Chapter-8-Information-Technology-Services.aspx

CONTACT INFORMATION

Subject	Contact	Telephone	E-mail / Web Address
Policy Clarification	Information Technology Services	(919)866-5100	its-leadership@waketech.edu

E1005 _ Data Protection & Retention Policy

APPENDIX A:

NIST Special Publication (SP) 800-122
Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)

"PII is —any information about an individual maintained by an WTCC, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Examples of PII Data:

- The following list contains examples of information that may be considered PII.
- Name, such as full name, maiden name, mother's maiden name, or alias
- Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, patient identification number, and financial account or credit card number
- Address information, such as street address or email address
- Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or small, well defined group of people
- Telephone numbers, including mobile, business, and personal numbers
- Personal characteristics, including photographic image (especially of face or other distinguishing characteristic), x-rays, fingerprints, or other biometric image or template data (e.g., retina scan, voice signature, facial geometry)
- Information identifying personally owned property, such as vehicle registration number or title number and related information
- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information)."