FAYETTEVILLE STATE UNIVERSITY

DATA CLASSIFICATION AND HANDLING
(replaces *Information Classification and Handling*)

Authority:	Issued by the Chancellor. Changes or exceptions to administrative policies issued by the Chancellor may only be made by the Chancellor.
Category:	Information Technology
Applies to:	●Administrators ●Faculty ●Staff ●Students
History:	Approved – August 29, 2024
Related Policies:	●Information Security
Contact for Info:	Vice Chancellor for Information Technology and Chief Information Officer | (910) 672-1200

I. PURPOSE

Members of the University community have a responsibility to protect the confidentiality, integrity, and availability of information collected, processed, stored, or transmitted, regardless of the location or medium on which the information resides. Information must be classified and handled according to its value, legal requirements, sensitivity, and criticality to the University. Safeguards must be established and implemented relative to the information's classification, protecting information from unauthorized access, modification, disclosure, and destruction.

This policy takes into consideration that certain types of information must be disseminated more widely than others in order to fulfill the educational, research, and public-service missions of the University. It is intended to provide a uniform classification guide for the tracking and adequate protection of University owned information resources.

II. DEFINITIONS

The following acronyms/definitions are used in this Policy:

- **Availability** shall mean the degree to which information and critical College services are accessible for use when required.

- **Confidentiality** shall mean the degree to which confidential University information is protected from unauthorized disclosure.

- **Control** shall mean safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets. Controls help to reduce the risk of damage or loss by stopping, deterring, or slowing down an attack against an asset.

- **Control Statement** shall mean statements provided in addition to classification labeling to further restrict or clarify how the information is to be handled, e.g. "To be Opened by Addressee Only" or "Classified Public after 01/01/2020".

- **Family Educational Rights and Privacy Act (FERPA)** shall mean the Family Educational and Privacy Act of 1974 (FERPA) is a federal law that protects the privacy of student education records.

- **General Data Protection Regulation (GDPR)** shall mean the General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). It also addresses the export of personal data outside the EU and EEA areas. The GDPR aims primarily to give control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

- **Gramm-Leach-Bliley Act (GLBA)** shall mean the Gramm Leach Bliley Act (GLBA) is a law that applies to financial institutions and includes privacy and information security provisions that are designed to protect consumer financial data. This law applies to how higher education institutions collect, store, and use student financial records (e.g., records regarding tuition payments and/or financial aid) containing personally identifiable information.

- **Health Insurance Portability and Accountability Act (HIPAA)** shall mean the Health Insurance Portability and Accountability Act of 1996 was created primarily to modernize the following of healthcare information, stipulate how Personally Identifiable Information maintained by the healthcare and healthcare insurance industries should be protected from fraud and theft, and address limitations on healthcare insurance coverage.

- **Information Resource** shall mean data, information and information systems used by the University to conduct University operations. This includes not only the information or data itself, but also computer, network, and storage systems used to interact with the information.

- **Information Security** shall mean the protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional. The focus is on the confidentiality, integrity, and availability of data.

- **Integrity** shall mean the degree to which the accuracy, completeness, and consistency of information is safeguarded to protect the business of the University.

- **Payment Card Industry (PCI)** shall mean credit card number (also referred to as a primary account number or PAN) in combination with one or more of the following data elements:

    - Cardholder name
    - Service code
    - Expiration date
    - CVC2, CVV2, or CID value
    - PIN or PIN block
    - Contents of a credit card's magnetic stripe

- **Personally Identifiable Information (PII)** shall mean any information about an individual maintained by an agency, 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.

- **Protected Health Information (PHI)** shall mean any information in a medical record that can be used to identify an individual, and that was created, used, or disclosed in the course of providing a health care service, such as a diagnosis or treatment.

- **Security Breach** or **Security Compromise** shall mean an unauthorized intrusion into a University information resource where unauthorized disclosure, modification, or destruction of confidential information may have occurred.

- **Security Incident** shall mean attempted or successful unauthorized access, use, disclosure, modification, or destruction of information; interference with information system operation; or violation of information security policy.

III. DATA CLASSIFICATION TIERS

Data classification tiers are as follows:

A. Non-Sensitive Information

Tier 0 and Tier 1 information is "Non-Sensitive Information" for the purposes of interpreting existing University policies, standards, procedures, and other documents. It is incumbent upon organizational units handling any sensitive information to evaluate classification and control, and to apply stricter standards when appropriate.

1. Tier 0: Public Information

There are no disclosure restrictions on Tier 0 information. The following are examples of Public Information:

- Information published on public-facing University websites, including marketing materials, department or program descriptions, press releases, and requests for research participation;
- Business Information, once transferred to Archives, may become Public Information;
- Annual Clery Reports.

2. Tier 1: Business Information

Some Tier 1 Business Information, as defined in the North Carolina Public Records Act, may be available to the public, although such information typically is considered operational information intended primarily for internal use. Business Information is that which may be routinely communicated to outside parties with no contractual or other restrictions in the course of University business.

The following are examples of Business Information elements:

- Memos, correspondence, meeting minutes, contact lists, or procedural documentation (not otherwise restricted);.
- Budget or purchase records, including reports, vendor catalogs or brochures, or chemical safety records such as Employee Right-To-Know reports.
- Grant proposals and supporting documentation once the grant is completed.

B. Sensitive Information

Tier 2 and Tier 3 information is "Sensitive Information" for the purposes of interpreting existing University policies, standards, procedures, and other documents. It is incumbent upon University units handling any sensitive information to evaluate classification and control, and to apply stricter standards when appropriate.

Information that may not otherwise fall into a protected category may be declared sensitive information by the University.

1. Tier 2: Confidential Information

Tier 2 Confidential Information is the default classification of University information until determined otherwise. Confidential Information includes information that the University is required by law, regulation, contract, policy, or other governing requirements to keep confidential.

The following are examples of Confidential Information elements:

- Education records such as grades and class schedules
- The University's proprietary information including, but not limited to, intellectual research findings, intellectual property, financial data and donor/funding sources not otherwise classified under this standard
- Confidential personnel file information protected by the N.C. Human Resources Act, including criminal background check results
- Attorney-client communications
- Information subject to a confidentiality agreement
- Information protected by contractual agreements or non-disclosure agreements such as vendor product roadmaps, bid documents sealed for a limited time

2. Tier 3: Restricted Information

Tier 3 Restricted Information includes any information that the University has a contractual, legal, or regulatory obligation to safeguard in the most stringent manner. Unauthorized disclosure or loss of this information often requires review and approval of the General Counsel’s Office.

The following are examples of Restricted Information:

- Education records such as disciplinary conduct reports, student health information, sexual assault reports, passports, or financial aid information
- Some types of Federal Policy for the Protection of Human Subjects "Common Rule" data that remains identifiable
- Personal Health Information as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Information covered by the North Carolina Identity Theft Protection Act of 2005
- Payment Card Industry (PCI) information related to merchant activity
- Export controlled information (ITAR/EAR)
- Information covered by the Gramm-Leach-Bliley Act (GLBA)
- Information protected by contractual obligations such as vendor information security documentation
- Passwords
- Social Security Numbers

IV. REQUIRED CONTROLS FOR HANDLING OF SENSITIVE INFORMATION

The University is committed to responsible handling and protection of University information. The classification level determines the information security controls that must be applied to protect an information resource and the procedures that must be followed when collecting, processing, storing, transmitting, or destroying the information resource. Data Steward and Users must notify the ISO if they discover information is not being adequately protected according to its classification.

Tier 0 public information is information that can be disclosed to anyone inside or outside of the University and therefore, does not have any special handling requirements other than typical safeguards to protect it against unauthorized modification, destruction, or loss.

While Tier 1 information is not available to the public and is typically operational information intended primarily for internal use, it also does not have any special handling requirements other than typical safeguards to protect it against unauthorized modification, destruction, or loss. Tier 1 information is that which may be routinely communicated to outside parties with no contractual or other restrictions in the course of University business.

Tier 2 and Tier 3 information, as defined above in this Policy is considered sensitive and as such, must follow the below standards for handling and transmission.

A. Access

Access to sensitive information shall be limited to University faculty, staff, students, and third parties with a specific need-to-know. All requests for access must be approved by the responsible Information Owner with Data Stewards being required to regularly review user access and remove individuals who no longer have a need-to-know Additionally, individuals obtaining access to sensitive information will be required to sign a written confidentiality agreement in situations where such is required by law or University/unit policy/procedures.

Also, the following will be required for access to sensitive information:

- Access must be authorized on an individual basis.

- The University Password policy must be followed.
- File system access control features must be used to limit access.
- Access for terminated and transferred individuals must be removed immediately.
- Access controls must be reassessed annually and updated as necessary.

B. Clear Desk Requirements

All papers and physical materials containing sensitive information must be cleared from the user's desk and locked away in a drawer, file cabinet, or file storage room when not in use. Additionally, computer screens must be locked when not in use.

C. Distribution

Distribution of sensitive information is limited to only faculty, staff, and third parties with an approved business need-to-know and who have signed a written confidentiality agreement. Any student personally identifiable information shall be distributed in accordance with the University's Student Education Records (FERPA) policy.

D. Storage on Personal Devices

Storage of University-owned sensitive information on personal devices is prohibited.

E. Storage on Other Media

1. On University-Owned Systems

Sensitive information should be stored in secured databases or on secured file servers with file system access control features applied to limit access.

Sensitive information must not be stored on portable devices. Additionally, sensitive information must not be copied to non-University off-line media (e.g., USB flash drives, CDs, DVDs, etc.). Information stored in secured University off-line media must be encrypted, labeled "CONFIDENTIAL," and stored in a secure location. Key/combination access should be limited to authorized individuals.

2. On Internet-based Hosting/Storage/Sharing Sites

Storage of University-owned information on the Internet or Cloud-based Hosting/Storage/Sharing Sites and Solutions is prohibited unless there is either a contractual agreement approved by the Division of Legal, Audit, Risk and Compliance (LARC) and ITS between the University and a service provider. Any storage of information outside of the University owned/administered environment must be encrypted.

Cloud storage of University-owned data is only permitted in OneDrive using an ITS provisioned account if access to the files/data in question is not shared in a way that violates this policy.

3. Storage of Physical Documents

Physical documents containing sensitive information should be stored in a locked enclosure (desk drawer, file cabinet, or other secure containers) or in secure file or storage rooms when not in use. Key/combination access should be limited to authorized individuals.

F. Sent via Email

Sensitive information may be sent or forwarded to employees authorized to receive such information. A business purpose must exist in order for a University employee to send out sensitive information to an external source via email. The message containing the sensitive information must be encrypted. Sensitive information being sent via email should be sent as an attachment and not as message text.

G. Sent via Physical Mail

Sensitive information should be hand-delivered if being delivered to an on-campus unit/employee; however, sensitive information may be sent via US Mail to individuals external to the University. Whether sent via hand-delivered or U.S. Mail, sensitive information should be sent in a sealed envelope and labeled as either "confidential" or "to be opened by addressee only."

H. Data Transmission

Sensitive information must be sent over secure channels (VPN, SSL) or through secure, ITS approved file transfer. The information must be encrypted prior to transmission if secure channels are unavailable, and the recipient site must ensure that the sensitive information at rest will remain encrypted.

I. Facsimile (Fax)

Faxing is authorized only if a government agency requires that such sensitive information be faxed, otherwise the faxing of sensitive information is expressly prohibited.

J. Person-to-Person Calls/Face-to-Face Interaction

Sensitive information must only be discussed between authorized parties when there is a business need for the other party to have such information. No matter how the information is presented, employees shall ensure that the individual being provided with the sensitive information is an authorized representative of the organization.

K. Voicemail

Under no circumstance shall sensitive information be left on a voicemail system.

L. Record Retention

Information must be retained and disposed of as required by the University Record Retention Policy.

M. Backups

Backups of sensitive information require the same level of protection and handling as the original information. Backup media must be stored in a secure location and must be encrypted if transported outside the University.

N. Disposal

Sensitive information must be disposed of in accordance with the UNC System's Records Retention policy and as follows:

1. Printed Sensitive Information

Printed sensitive information must not be placed in normal office trash cans or non-secure recycling bins. Printed sensitive information must be disposed of by placing it in locked recycling bins designed for sensitive information or shredded with a cross-cut shredder.

2. Hard Drives and USB Drives

To ensure that sensitive information is not inadvertently exposed, magnetic hard drives and USB flash drives must be securely wiped using approved wiping tools/programs prior to re-deploying or sent outside the University for maintenance or repair. Additionally, magnetic hard drives and USB flash drives must be securely wiped or degaussed using approved tools/programs prior to disposal.

3. Other Media

CDs and DVDs containing sensitive information must be securely disposed of by shredding, chipping, or breaking the disc into multiple pieces.

Magnetic tape and diskettes containing sensitive information must be securely disposed of by degaussing, incineration, or shredding.

O. Inventory

All electronic repositories of sensitive information must be identified, documented, and reported to the CISO annually by the respective unit head.

V. ROLES AND RESPONSIBILITIES

Members of the University community share the responsibility for protecting the confidentiality and security of data. The following describes the duties and responsibilities of employees who are responsible for ensuring compliance with this Policy.

A. Chancellor, Vice Chancellors and Deans

The Chancellor, Vice Chancellors, and Deans shall be responsible for protecting all University information resources within their respective units as follows:

- Maintaining an appreciation of the risks associated with the loss of confidentiality, integrity, or availability of information resources used in their office or department.
- Determining the proper levels of protection, through consultation/coordination with the ISO, for office or department information resources and ensuring necessary safeguards are implemented.
- Ensuring all information resources used by the office or department are assigned an Information Owner.
- Promoting information security awareness in the office or department and ensuring all staff participate in relevant security and privacy training.
- Ensuring office and department staff understand information security expectations and act reasonably to protect University information resources.

- Ensuring end-user access to information resources is appropriate for the user's job function, is administered securely, and is regularly reviewed and audited.
- Ensuring office and department staff compliance with the requirements of the Information Security Program.

B. <u>Associate Vice Chancellor for Human Resources</u>

The Associate Vice Chancellor for Human Resources shall be responsible for the following:

- Collaborating with the CISO to educate incoming employees (including temporary and contract employees) regarding their obligations under this Policy and to provide on-going employee training regarding data security.
- Ensuring that terminated employees no longer have access to the University's systems that permit access to sensitive or confidential information resources.
- Advising appropriate disciplinary measures in response to a violation of information security policies.

C. <u>Information Security Office/Officer (CISO)</u>

The Chief Information Security Office/Officer has authority and responsibility for Operation and management of the University's Information Security Program.

The CISO is required to perform or delegate the following information security responsibilities:

- Establish, document, and distribute information security policies, standards, procedures, and guidelines.
- Coordinate with the Office of Risk and Compliance to implement a risk assessment process to identify, analyze, and mitigate risks to the University's information resources.
- Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of policy violation, breach, or compromise incidents.
- Implement practical and effective technologies and services to ensure the security of the University's information resources, networks, and computing infrastructure.

- Disconnect any device or disable any account believed to be involved in compromising the security of the University's information resources until the device or account no longer poses a threat.
- Develop and implement an information security awareness program to be offered periodically to all University faculty, staff, and students.

D. Data Stewards

A Data Steward has primary responsibility for overseeing the collection, storage, use, and security of a particular information resource. In cases where a Data Steward is not identified for any information resource, the cognizant Vice Chancellor or Dean shall be deemed the Data Steward.

A Data Steward is responsible for the following:

- Ensuring information resources are assigned a security classification and labeling (including control statements) as such, where appropriate.
- Clearly identifying Confidential and Internal Use Only information when sharing or providing individuals, departments, or third parties with access.
- Establishing security requirements and expectations for information resources within their ownership:
    - Information User authentication
    - Information User access lifecycle management (request, approve, provision, review, and revoke)
    - Record retention
- Providing training and awareness specific to information protection and handling of their Confidential and Internal Use Only information.
- Maintaining an inventory of their information resources, including all applications that collect, process, store, or transmit their information. Conducting periodic entitlement and attestation reviews of access granted to Confidential and Internal Use Only information.
- Reviewing, at least annually, information classification based on changes in value, legal requirements, sensitivity, or criticality to the University and updating as appropriate.
- Establishing procedures for data destruction. Performing risk assessments, at least annually, of information resources to review requirements as needed to address changing risks, University requirements, or laws and regulations.
- Ensuring compliance with regulatory requirements such as FERPA, GDPR, GLBA, HIPAA, PCI, and other State, Federal, and contractual requirements that may apply.

E. Information Users

Information Users shall be responsible for the following:

- Reviewing, understanding, and complying with all relevant University information security policies, standards, procedures, and guidelines.

- Providing appropriate physical security for information technology equipment, storage media, and physical data.
- Ensuring sensitive or confidential information is not distributed or accessible to unauthorized persons.
- Protecting the confidentiality of personal passwords, never sharing under any circumstance. Logging off from all applications, computers, and networks, and physically securing printed material, when not in use.
- Immediately notifying the IT Services Help Desk and the ISO of any incident that may cause a security breach or violation of the *Information Security* policy.
- Abiding by the requirements of the *Information Security* policy.

F. Information Technology Services (ITS)

ITS staff has primary operational responsibility for information systems that receive, create, store, handle, or discard information. ITS shall be responsible for the following:

- Implementing information security technologies, controls, and services to protect information resources as required by the Information Security Policy.
- Granting and revoking user rights to information resources and privileged user access to information systems as directed by the ISO or information resource owners.
- Ensuring availability and recovery of information resources.
- Abiding by the requirements of the Information Security Policy.

G. Third Parties

Third parties executing business on behalf of the University, in lieu of or in addition to University employees, must agree to follow the information security policies of the University. Third parties are expected to protect University information resources to the same degree expected from University employees.

Third parties may only access University information resources where there is a business need, only with approval of information resource owners and the CISO, and only with the minimum access needed to accomplish the business objective.

An appropriate summary of the information security policies and the third party's role in ensuring compliance must be formally delivered to the third party prior to access being granted, with provisions made to grant access in a secure manner. In these cases, third parties shall be subject to the same policies and practices as other members of the University community, unless an exception is granted by the CISO.

H. Third Parties – Outsourced Services

Contracts with third parties for outsourced services must include provisions that govern the handling and proper security of all University information resources. These provisions should clearly define the requirements of the third party for protection of the University's information, and where possible, should provide the University the ability to audit the third party as needed to ensure information is appropriately protected.

University units must provide oversight of all outsourced service providers to ensure their policies and practices regarding information protection are consistent with University policies.

Third parties will be audited as needed to ensure compliance. University information resources must be protected whether used, housed, or supported by the University's workforce or by third parties.

The Policy provisions pertaining to contracts will be addressed on a go-forward basis. There is no expectation that existing contracts will be renegotiated to comply with these requirements.