NORTH CAROLINA AGRICULTURAL AND TECHNICAL STATE UNIVERSITY

SEC. VII-Data 1.0

DATA CLASSIFICATION POLICY

ADMINISTRATIVE POLICY

PURPOSE

University data are institutional information acquired or created on behalf of North Carolina Agricultural and Technical State University by such entities as divisions, departments, organizations, and their personnel. Mandates of federal laws, state laws, industry standards, and contractual agreements set out what and/or how data are protected. University policies are sometime derived from these governing controls. The purpose of this policy is to provide users with data classification governance in order to protect University data from unauthorized use including but not limited to acquisition, access, disclosure, retention, and disposal.

SCOPE

This policy applies to University data in typed, printed, written, electronic, and/or verbal formats regardless of how data are communicated, how data are transmitted, and/or whether data are saved to storage media such as hard drives or CDs.

POLICY

Classification: University data are classified as either **restricted** or **public**.

- **Restricted Data**: Data for which the highest levels of protection apply due to the risk or harm that may result from improper data acquisition, access, disclosure, retention, and/or disposal. This includes data protected by mandates of federal laws, state laws, industry standards, and contractual agreements. Regulations and Standards that the University

users must abide by include but are not limited to the ones listed in the Regulations and Standards table in this policy.

- **Public Data**: Data for public use that has neither disclosure nor access restrictions. This includes data governance mandated by the North Carolina Public Records Act which is listed in the Regulation and Standards table.

  Examples of public data include but are not limited to the following: directory information, press releases, posted course schedules, annual reports, University website information with unrestricted access, University announcements, and publications (i.e. newsletters, magazines, etc.).

Responsibilities: Security measures for data are set by the defined roles below.

- **Data Steward**: A data steward is the manager of data that are acquired and/or created. A data steward classifies data as restricted or public, how data can be used including disclosure, who can access the data, how the data can be accessed, data access privileges, data retention, and data disposal.

- **Data Custodian:** A data custodian is entrusted with the care of data by a data steward. Data stewards must work with data custodians to develop and implement policies and procedures for requesting and maintaining access to data. These policies and procedures shall be developed taking into account the risk associated with the specific data and/or system being accessed. A data custodian implements applicable controls such as data security, physical security, backup and recovery. A data custodian, when applicable, grants access to data based upon authorization from a data steward.

- **Data User**: A data user requests access to data from a data steward. A data steward entrusts a data user to create data, modify data, or delete data while maintaining the integrity of the data and complying with policies and procedures established to protect data.

Data Retention and Disposition: Data stewards are responsible for establishing as well as communicating retention and disposal policies and procedures. The University General Records Retention and Disposition Schedule govern the institutions of the University of North Carolina System on the retention, destruction, transfer, or disposal of records. It is accessible on the University Archives Department website (http://www.library.ncat.edu/resources/archives/records.html). The University Archives Department assists offices with records management.

ENFORCEMENT

Non-compliance with a federal or state law can have severe financial consequences for the University and the person(s) responsible for the negligence. The following penalties could occur as a result of non-compliance:

- With the Family Education Rights and Privacy Act (FERPA), federal funding could be lost to the University, including grants and financial aid.
- With Gramm-Leach-Billey Act (GLBA), the University could be fined up to $100,000.
- With the Health Insurance Portability and Accountability Act (HIPAA), the fine could range from $50,000 to $250,000 and a one to two year prison term for the individual responsible for non-compliance.
- With the Payment Card Industry Data Security Standard (PCI DSS), the University may no longer be permitted to accept credit card payments and also may receive a fine up to $500,000 per incident.

Enforcement of this policy includes the following:

- Divisional and departmental assessments
- External and internal audit compliance
- Federal and state laws and regulations, University policies, and industry standards

University sanctions for individuals cited for unauthorized use may result in one or more of the following:

- Suspension of computing and networking privileges
- Misconduct review
- Termination of employment
- Student suspension or dismissal
- Breach of contract/agreement filed against vendors, contractors, guests, and alumni

For University students and employees, the sanctions will be administered in accordance with governance from the student handbook, the faculty handbook, Human Resources, and the Office of State Personnel procedures, as appropriate.

References:

Regulations and Standards Table: All users of University data are responsible for understanding and complying with the protection of data elements and records listed in the table as well as all other listed requirements.

Name:	Family Educational Rights and Privacy Act (FERPA)		
Description:	Protects students' privacy by prohibiting disclosure of education records without adult consent		
Type:	Federal Law	**Reference(s):**	http://www.ncat.edu/registrar-office/ferpa/index.html http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html http://www2.ed.gov/policy/gen/guid/fpco/pdf/ht12-17-08-att.pdf
Some of the protected data elements/records:	• Social Security number • educational record • photograph if op-out not disclosed nor proper notice provided	• other personable identifiable information (PII) • student identification number since it is used in some cases to solely authenticate identity • non-directory information	
Name:	Health Insurance Portability and Accountability Act (HIPPA)		
Description:	Protects patient health and medical information; applies to health care providers		
Type:	Federal Law	**Reference(s):**	http://www.hhs.gov/ocr/privacy/
Some of the protected data elements/records:	• health/medical record	• other health/medical identifiable information	
Name:	Payment Card Industry (PCI) Standard		
Description:	Protects credit card information		
Type:	Industry Standard	**Reference(s):**	https://www.pcisecuritystandards.org/ https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf
Some of the protected data elements/records:	• primary account number (PAN) • PINs (storage not permitted)	• card verification codes (storage not permitted) • cardholder name, service code, and/or expiration date are protected when used with PAN; used includes stored, processed	

Name:	North Carolina Identity Theft Protection Act		
Description:	Requires entities to protect customer information to prevent identity theft		
Type:	State Law	**Reference(s):**	http://www.ncleg.net/enactedlegislation/statutes/pdf/byarticle/chapter_75/article_2a.pdf
Some of the protected data elements/records:	• Social Security number • driver's license number • banking information	• credit card information • other personal information	

Name:	The Gramm-Leach-Bliley Act (GLBA)		
Description:	Protects consumer financial information		
Type:	Federal Law	**Reference(s):**	http://www.ftc.gov/os/2002/05/67fr36585.pdf http://www.gpo.gov/fdsys/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf
Some of the protected data elements/records:	• account numbers • credit card number • deposit/transaction information	• personable identifiable information (PII)	

Name:	The North Carolina Public Records Act		
Description:	Protects certain records from public disclosure including personally identifiable information.		
Type:	State Law	**Reference(s):**	http://www.ncpress.com/ncpa/AG%20booklet%204-8-08.pdf and N.C.G.S, 126-22 et seq. http://www.ncleg.net/EnactedLegislation/Statutes/HTML/ByArticle/Chapter_126/Article_7.html
Some of the protected data elements/records:	• Social Security number • certain criminal investigation records • certain records about industrial expansion	• certain state tax information • certain trade secrets • records containing certain communications between attorneys and their government clients • most personnel records	

Name:	Red Flag Rule		
Description:	Prevent identity theft		
Type:	Federal Law	**Reference(s):**	http://www.ftc.gov/bcp/edu/microsites/redflagsrule/index.shtml http://www.northcarolina.edu/legal/policies/red_flag/index.htm
Some of the protected data elements/records:	• Social Security number	• driver's license number • banking or other financial information	

	• date of birth	• government passport number

Data Classification Policy (http://policy.uncg.edu/data/)

Data Classification Policy (http://ocio.osu.edu/policy/policies/policy-on-institutional-data/data-classification/)

US Department of Education (http://www.ed.gov/technology/draft-netp-2010/FERPA)

Wikipedia
(http://en.wikipedia.org/wiki/North_Carolina_Identity_Theft_Protection_Act_of_2005)

_____

Date Original is Effective: Upon approval

Approved by Chancellor

First approved: May 16, 2012
Revised

Suggestions on Safeguarding University Data

Data stewards, data custodians, and data users can comply with protecting University data by applying practices including but not limited to the following list:

- Do not leave paper documents unattended; protect them from the view of passers-by or office visitors; be mindful that personnel such as Housekeeping and/or Facilities may have to enter your office when you are not present.
- Close and lock office doors when away from your office.
- Add a "Restricted" or "Confidential" label or watermark to documents.
- Do not leave keys, access codes, access cards, etc. to file drawers, storage locations, electronic systems, etc. in unlocked desk drawers, in cabinet key slots, or other areas.
- Do not share access credentials (i.e. passwords, PINs, etc.).
- Store paper documents and storage media (i.e. USB drives, CDs, etc.) in a secure location(s).
- Shred paper documents when they are no longer needed, making sure that such documents are secured until shredding occurs. If a shredding service is employed, the service provider should have clearly defined procedures in the contractual agreement that protect discarded information, and ensure that the provider is legally accountable for those procedures, with penalties in place for breach of contract.
- Immediately retrieve documents from copy machines, fax machines, and printers.
- Do not discuss restricted data outside of the workplace or with anyone who does not have a University business need to know. Be aware of the potential for others to overhear communications in offices, on telephones, and in public places like elevators, restaurants, and sidewalks.
- Ensure that electronic equipment containing restricted data is securely transferred or disposed of in a secure manner.
- Immediately report the theft, lose, or abuse of data and electronic computing equipment to the University Police Department. The theft, loss, or suspected compromise of restricted data should be immediately reported to IT Security & Audit.
- Physically secure systems that contain restricted data from unauthorized access and use. Implement access controls including encryption.
- Grant only the necessary access to users that are needed to perform job functions.
- Exercise the principles of least privileges and separation of duties when granting access to data.
- Verify third party protection, access, disclosure, retention, and disposal of data.
- Use encryption or certificates when transmitting and accessing restricted data. Recommended secure methods include https, secure shell (scp/sftp), ssl, ftps, IPSec, S/MIME, and password-protected data.
- For intellectual property data, in addition to this policy, consult with the Office of Legal Affairs.
- For proprietary research data, in addition to this policy, consult with the Division of Research.
- Terminate user access to data when access is no longer warranted; modify user access to data when the user's role changes.

References:

- Data Classification Policy (http://ocio.osu.edu/policy/policies/policy-on-institutional-data/data-classification/)
- Encrypting Lotus Notes (http://publib.boulder.ibm.com/infocenter/domhelp/v8r0/index.jsp?topic=/com.ibm.help.domino.admin.doc/DOC/H_ENCRYPTING_OUTGOING_MAIL.html)
- Guidelines for Safeguarding Information (http://www.brown.edu/cis/policy/safeinfo.php