REG - 70.00.2 - DATA AND INFORMATION REGULATION

Authority: Chancellor	Responsible Office: Information Technology Services

Number:	REG - 70.00.2 - DATA AND INFORMATION REGULATION
History:	Effective Date: February 15, 2006 ; Reformatted/Updated: March 15, 2016; Revised: January 24, 2018
Related Policies/Sources:	International Organization for Standardization (ISO) 27002, NIST 800-60, Health Insurance Portability and Accountability Act of 1996 (HIPAA), Family Educational Rights and Privacy Act (FERPA), 2017 NCCU Faculty Handbook , North Carolina State Human Resources Act, NC Identity Theft Protection Act, North Carolina Public Records Act, NC Statewide Information Security Manual, University General Records Retention and Disposition Schedule, NCCU REG 70.00.4 Responsible Use Regulation , NCCU REG 01.01.6 University Record Retention and Disposition Schedule Regulation, NCCU REG 80.06.15 Faculty and Non-Faculty EHRA Employees Conflicts of Interest and Commitment Regulation, Data Handling Guidelines for University Data Classified as Levels Appendix,
Contact Info:	Information Technology Services, 919-530-7423

1 Regulation

1.1 The purpose of this regulation is to establish the classification levels for University Data. This regulation applies to all University Data, and to all administrative and user-developed computing systems that may access or utilize University Data. Further, it provides the guidelines to establish a security framework to protect University Data.

1.2 Confidentiality, availability and integrity of University Data will be maintained at all times.

1.3 This regulation defines custodianship and custodial responsibility of all University Data. Data owners and custodians are expected to identify and

protect such data in accordance with University policies, regulations and rules and state and federal laws and regulations.

1.4 This regulation also ensures that the level of security applied to networks, systems and data is appropriate for the level of risk associated with disclosure, corruption, improper modification or loss of University Data.

2 Scope

2.1 This regulation governs the classification levels, management and accessibility of all University Data regardless of the environment where the data resides. This includes central servers, college or departmental servers, individual personal computers, mobile devices and data residing on any other medium (paper printouts, thumb drives, tape, disk drives, etc.). Administrators of servers that process University Data are expected to apply industry best practices to ensure appropriate security of that data. Network administrators are expected to apply best practices to ensure that the network is protected, available and secure from breach. Users of University information technology resources are expected to comply with this regulation along with other University policies, regulations and rules and applicable state and federal laws and regulations.

2.2 Section 7 of this regulation defines the classification levels assigned to different types of University Data according to confidentiality. Identification and classification of University Data allows the appropriate degree of protection to be applied. Another goal of this regulation is to apply University security controls consistently for data of similar sensitivity across various University colleges and departments.

2.3 This regulation does not address confidentiality as it relates to release of University Data or other information under state public records laws or other legal requirements such as subpoenas, court orders or special exceptions to privacy laws.

2.4 Nondisclosure of University Data

2.4.1 As a condition of employment, data users are expected to access University Data only in the performance of their assigned duties, to respect and adhere to the confidentiality and privacy of individuals whose records they access and to abide by all applicable laws or policies with respect to access, use or disclosure of information. University Data may not be disclosed or distributed in any medium unless required by an employee's assigned duties. University Data may not be accessed or used for personal gain or to satisfy personal curiosity.

2.4.2 Certain employees may be exposed to confidential information in the normal performance of their assigned duties. The exposure could either be incidental to or material in the performance of their duties. Therefore, the University may, based upon the likelihood of exposure to confidential information, require that certain employees also sign a confidentiality statement.

3 Definitions

3.1 **University Data** is defined as all information content related to the

business of North Carolina Central University ("NCCU" or "University") that exists in electronic, digital form, and information that exists in other forms (*e.g*. ink on paper). "Data" includes but is not limited to text, graphics, video, audio, still images, databases, and spreadsheets.

3.2 **Access to data** is the ability to view, retrieve, alter, or create data.

3.3 **Sensitive Data** is defined as University Data classified by the relevant Data Custodian as requiring additional controls and safeguards during processing, storage or transmission.

3.4 The **University Data Classification Framework** defines the classification levels for common elements of Sensitive Data in use at the university. Sensitive Data may be protected by legal act, statute or contractual provisions against unwarranted disclosure. Data Custodians may further declare other University Data as "Sensitive Data" for legal or ethical reasons, for data for which unwarranted disclosure would represent a high degree of business risk to the University, for issues pertaining to personal privacy, or for proprietary considerations. Data included in the University Data Classification Framework may include:

3.4.1 Information that is required to be protected under the terms of a research grant or other University contract or agreement; and

3.4.2 Data that is relevant to planning or managing an administrative or academic function of the university.

3.5 **Data Custodians** are generally comprised of the following areas within the University: managers and administrators of computer systems and servers where data resides? and managers and applications programmers of software systems and web applications that store, modify or provide access to that data. Each of these groups share a custodial responsibility to assure that the confidentiality, integrity and accessibility of University Data is maintained at all times within the parameters defined by the Data Owner; University policies, rules and regulations; and State and Federal requirements.

3.6 **Data Owners** are those that have oversight responsibility for data management related to University functions managed/administered/run by the units and personnel reporting to them. The Data Owner is the entity, department, or administrative workgroup that is responsible for assurance that the data is accurate and complete. The Data Owner, due to legal, legislative, or ethical constraints, may also, after consultation with others, make the determination that access to certain elements of the data is limited.

4 Authority Over Data

4.1. NCCU University Authority and Rights

The University has authority over use of the University's physical computer assets. NCCU is the legal custodian of all University Data.

4.2. Chancellor's Delegation of Responsibility

The Chancellor delegates responsibility for data management at the University

as specified in Section 5.3 of this regulation. The Chancellor and Chancellor's designees are responsible for protecting University Data at the level appropriate for its sensitivity.

5 Data Management

5.1 Confidentiality, integrity and accuracy of University Data is the responsibility of the data owner as prescribed by all pertinent laws and regulations.

5.2 To obtain information related to University business, a supervisor or other University official may have access to University Data for work-related purposes, providing that the owner of the data is not available to produce the data and approval to access another's system has been expressly approved in advance by the employee's immediate supervisor, next-level supervisor or administrative head of that division.

5.3 Roles and Responsibilities

5.3.1 Chief Information Security and Compliance Officer

The University's Chief Information Security and Compliance Officer has responsibility for THE development, practice and enforcement of the information security policies, regulations, rules and procedures of the University. The Chief Information and Compliance Officer will also coordinate security efforts for other departments within the University. This position reports to and is supervised by the University's Chief Information Officer (CIO).

5.3.2 Data Owners and Data Custodians are collectively responsible for the management of all University data. Their decisions with regard to University data management must be made in compliance with this regulation and other University policies, regulations and rules and applicable state and federal laws and regulations.

5.3.4 List of Data Owners

5.3.4.1 Provost and Vice Chancellor for Academic Affairs

5.3.4.2 Vice Chancellor for Administration and Finance

5.3.4.3 Vice Chancellor for Student Affairs

5.3.4.4 Vice Chancellor for Advancement

5.3.4.5 General Counsel

5.3.4.6 Chief Human Resources Officer

5.3.4.7 Chief Information Officer

5.3.4.8 Director of Athletics

5.4 Data Custodians

5.4.1 Each Data Owner will assign Data Custodians to be responsible for data management within his or her area of responsibility. Data Custodians have the primary responsibility for the accuracy, privacy, and security of the University

Data under his/her responsibility. All University Data must have an identified Data Custodian.

5.4.1.1 Data Custodians shall be responsible for evaluation, approval or disapproval of requests for access to data within his/her assigned oversight.

5.4.1.2 Data Custodians are responsible for determining the degree of access (interactive query only, interactive update, downloading of specific data to user, etc.) to be granted to specific users, and for assuring compliance with access security standards.

5.4.1.3 Data Custodians shall be responsible for defining or describing each data element, to the extent required by public records laws, for which they have oversight. This definition shall be done in coordination with Information Technology Services (ITS) department.

5.4.1.4 Data Custodians should give consideration to the value of data in terms of its confidentiality and criticality to the conduct of University business. Security plans and procedures shall be implemented with emphasis dictated by the determined data value.

5.4.1.5 Data Custodians are the initiation point for any request for modification to the data for which they have responsibility.

5.4.1.6 Data Owners are persons who are assigned specific data management responsibilities by the Data Custodians. Data Custodians typically will manage access rights to data they oversee. Each Data Custodian may delegate specific custodial responsibilities for different subsets of data under his/her custody.

5.4.2 Application Sponsors are those University employees who are responsible for approving the functionality of a particular University application, and for controlling the protection of the data within that application. Application Sponsors will be appointed by the primary Data Owner associated with the data that their application accesses.

5.4.3 Application Security Certification

Application sponsors of all University applications that handle Sensitive Data will certify their applications on an annual basis to indicate that Sensitive Data displayed and/or stored by the application is identified and suitably protected. This certification process will be administered by the ITS Director of Security and Compliance.

6 User Responsibilities

6.1 User of University Data

6.1.1 Users of University Data include but are not limited to the following categories:

6.1.1.1 University employees (faculty/staff) permanent and temporary;

6.1.1.2 Students; and

6.1.1.3 All third-party affiliates (Contractors and Vendors).

6.1.2 Individual University users play a critical role in ensuring the security of

University data. Ultimately, only the user can prevent unauthorized access and ensure responsible use of the data. Proper use of data, including assurance of security and privacy, is a job requirement for all University employees, is a condition of volunteer service, should be included in all University agreements providing access to University Data, and is expected under the Student Code of Conduct.

6.1.3 Users are responsible for the following actions:

6.1.3.1 Storing data under secure conditions appropriate for the data classification level;

6.1.3.2 Making every reasonable effort to ensure the appropriate level of data privacy is maintained;

6.1.3.3 Using the data only for the purpose for which access was granted; and

6.1.3.4 Maintaining the security IDs and/or passwords by not sharing with other persons.

7 Data Classification Levels

7.1 All University Data residing on University computers, or on backup media retained for the purpose of business continuity and disaster recovery, is subject to the N.C. Public Records Act, unless an applicable exception applies. It is the responsibility of the Data Owner to identify elements of all data records for which the Data Owner has responsibility of stewardship to determine the level of protection that the data element requires. If a data element requires protection from access or disclosure, it is the incumbent responsibility of the Data Owner to inform the appropriate Data Custodians of that requirement.

7.2 Data classification levels range from Level 0 (public) to Level 3 (highly restricted). Any data other than Level 0 data is considered to be non-public data for the purposes of this regulation. The four classification levels are:

7.2.1 Level 0—Public data includes, but is not limited to: Advertising, product and service information, directory listings, published research, presentations or papers, job postings, press releases.

7.2.1.1 University data that is purposefully made available to the public.

7.2.1.2 Disclosure of Level 0 data requires no authorization and may be freely disseminated without potential harm to the University.

7.2.2 Level 1 – Internal data includes, but is not limited to: Budget and salary information, personal cell phone numbers, internal departmental policies and procedures, internal memos, incomplete or unpublished research. Note: While some forms of internal data can be made available to the public, the data is not freely disseminated without appropriate authorization.

7.2.2.1 University owned or managed data that includes information that is not openly shared with the general public but is not specifically required to be protected by statute or regulation.

7.2.2.2 Unauthorized disclosure would not result in direct financial loss or any

legal, contractual, or regulatory violations, but might otherwise adversely impact the University, individuals, or affiliates.

7.2.2.3 Level 1 data is intended for use by a designated workgroup, department, or group of individuals within the University.

7.2.3 Level 2 - Confidential/Sensitive data includes, but is not limited to: Student data that is not designated as directory information, passport data, personal financial information, certain research data (e.g., proprietary or otherwise protected), personally identifiable information (PII) such as name, birthdate, address, employee or student ID, etc. where the information is held in combination and could lead to identity theft or other misuse.

7.2.3.1 University owned or managed data that is confidential business or personal information for which unauthorized disclosure could have a serious adverse impact on the University, individuals or affiliates.

7.2.3.2 Level 2 data is intended for a very specific use and should not be disclosed except to those who have explicit authorization to review such data.

7.2.3.3 There are often general statutory, regulatory or contractual requirements that require protection of the data.

7.2.3.4 Regulations and laws that affect data in Level 2 include, but are not limited to, the Family Educational Rights & Privacy Act (FERPA), the State Human Resources Act (SHRA), and the Graham-Leach-Bliley Act (GLBA).

7.2.4 Level 3 - Highly Restricted University owned or managed data that is highly restricted business or personal information, for which unauthorized disclosure would result in significant financial loss to the University, impair its ability to conduct business, or result in a violation of contractual agreements or federal or state laws or regulations.

7.2.4.1 Highly restricted data includes, but is not limited to: Social Security Numbers, payment card numbers, medical records, restricted information protected by nondisclosure agreements, restricted research data.

7.2.4.2 Level 3 data is intended for very limited use and must not be disclosed except to those who have explicit authorization to view or use the data.

7.2.4.3 There are often governing statutes, regulations, standards, or agreements with specific provisions that dictate how this type of data must be protected.

7.2.4.4 Regulations and laws that affect Level 3 data include, but are not limited to, the Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry Data Security Standard (PCI DSS).

8 Guidelines for Appropriate Data Handling

8.1 Whether data is downloaded from a system or application within NCCU’s protected infrastructure or acquired by some other means, individuals must ensure that the security of the data is protected appropriate to the level of its classification.

8.2 Level 3 Data

8.2.1 Due to its restricted nature, Level 3 data requires special handling. Some units may handle Level 3 data as part of their business processes; however, that data should not be exported or stored outside of its secured location without express permission of the data or system owner. Additionally, some research data is highly sensitive in nature or subject to special contractual requirements and its handling should be coordinated through the Chief Information Security and Compliance Officer.

8.2.2 While a limited number of enterprise applications, such as Banner, hold highly restricted Level 3 data, access to this data is tightly controlled via specific permissions and management authorization. If an employee is unsure whether a unit's business data may be stored in one of these systems, clarification should be sought from a member of management within the unit or the Data Custodian for the unit.

9 Additional Guidelines for Data Handling Based on Classification

9.1 Data Handling Guidelines for University Data Classified as Levels 0 through 2

9.1.1 The Data Handling Guidelines for University Data Classified as Levels 0, 1, or 2 are designed to help members of the NCCU community make decisions about appropriate data handling for University Data classified as levels 0 through 2. University Data belonging to multiple classification levels must be treated according to the highest level of sensitivity.

9.2 Application of Best Practices to Secure University Data
All servers, desktop, mobile and portable devices that are used to process, store, or transmit sensitive University Data not intended for public disclosure will use appropriate encryption, as approved by ITS, to protect it from unauthorized disclosure.

9.3 Data Protection

9.3.1 End users of devices that process, store or transmit Level 2 University Data are prohibited from downloading applications on those devices that would pose a threat to the confidentiality, integrity and availability of that data.

9.3.2 The University periodically performs vulnerability scans on its network and devices connected to it in order detect threats that would be detrimental to the data contained therein. When threatening data vulnerabilities are discovered the owner of that data has no more than thirty (30) days to remediate the issues found.

9.4 Device Encryption Requirement

9.4.1 Sensitive personally identifiable information must be safeguarded by the use of Full Disk Encryption as approved and implemented by ITS. Only those devices that process, store or transmit PII in motion or at rest must be encrypted (*e.g.* desktop PCs of departments, mobile devices and drives). These devices include but are not limited to: Laptops, Notebooks, Netbooks, Mobile and portable computing devices, such as tablets, smart phones and personal digital assistants. Removable Media such as CDs, DVDs, memory sticks (flash

drives), tape media, or any other portable device that stores data.

9.4.2 Data owners must insure that security controls are put in place to protect the confidentiality and integrity of data contained on removable storage media throughout the life of those storage media, including disposal.

9.4.3 Departments shall authorize the assignment of portable personal computers to employees and require that users comply with all NCCU information technology security policies when using the portable devices. Portable devices covered by this regulation are those that connect to the NCCU technological network and/or store University Data. Departments shall implement appropriate safeguards to ensure the security of laptops and other portable computing devices. When a laptop is outside of an individual's work space, data on the laptop must be backed up, and the backup must be kept separate from the laptop. Each department shall be responsible for identifying what University Data will be backed up and defining the procedures for backing up mobile computing data. Personnel who use a University laptop/portable computer shall ensure that the laptop/portable computer and the information it contains are suitably protected at all times. Mobile devices shall:

9.4.3.1 Be physically secured when the users have taken them out of an individual's workspace;

9.4.3.2 Be labeled with tamper-resistant tags identifying the device as property of NCCU or a permanently engraved serial number or both;

9.4.3.3 Comply with all applicable security requirements for desktops;

9.4.3.4 If not protected by encryption software, the BIOS password on such devices must be enabled if technically possible with the assistance of ITS as necessary;

9.4.3.5 Use current antivirus software to scan for malware;

9.4.3.6 Have regular backups; and

9.4.3.7 Have firewalls configured to comply with State and agency policies.

9.4.4 Departments shall define rules and/or procedures for authorized personnel to securely access systems from off-site. Rules and procedures shall include the following:

9.4.4.1 Use of agency-approved virus prevention and detection software;

9.4.4.2 Use of personal firewalls that are configured to block unauthorized incoming connections;

9.4.4.3 Securing home wireless networks, and properly using other non-State Wi-Fi connections;

9.4.4.4 Protecting mobile computing devices and portable computing devices such as smart phones, tablets, and portable storage devices such as compact disks (CDs), digital video disks (DVDs), media players (MP3 players), flash drives, or other similar devices that are used to conduct the public's business;

9.4.4.5 Use of virtual private networking (VPN) software in order to allow

secure access to University Data; and/or

9.4.4.6 Use of encryption products to protect data stored on off-site systems, if applicable.

9.4.5 Departments shall require personnel received training from ITS for properly accessing systems from off-site and for keeping antivirus software and personal firewall software up to date with the latest signature files and patches.

9.4.6 Require instructions and training from ITS for protecting confidential information transferred to, processed on or stored on non-State-issued systems, such as personal computers at home.

9.4.7 Department employees who are authorized to work from home shall ensure that they comply with all NCCU regulatory requirements relevant to working offsite. Personnel shall take extra precautions to ensure that confidential information stored on personal computers or electronic devices is not divulged to unauthorized persons, including family members. For purposes of this regulation, "mobile communication devices" includes mobile phones, IP phones, pagers, smart phones, tablets, etc. Some of these devices are multifunctional and may be used for voice calls, text messages, email, Internet access, and may allow access to computers and/or networks.

9.4.8 Confidential University Data transmitted, accessed, and/or stored on mobile communication devices shall be appropriately secured.

9.4.9 The amount of personal conversations and/or personal business on department-provided mobile communication devices shall be controlled in accordance with the respective department's procedures. Authorized users must report loss of University-owned data processing equipment to the campus police within twenty-four (24) hours of the loss.

9.4.10 Personnel using department-provided mobile communication devices shall do the following:

9.4.10.1 Adhere to NCCU Responsible Use Regulation;

9.4.10.2 Adhere to the encryption standards specified within this regulation, if applicable;

9.4.10.3 Change the default password for connecting to a wireless enabled device (*e.g.,* Wi-Fi or Bluetooth) on applicable mobile communication devices; and/or

9.4.10.4 Disable wireless functionality on appropriate devices with wireless functionality if it is not in use.

10 Enforcement

10.1 The University's Chief Information Security and Compliance Officer has the authority to report failure to comply and violations of this regulation to the Chief Information Officer for further adjudication and escalation if necessary.