1. Regulation

1.1 The purpose of this Data and Information Regulation is to provide general guidance on the protection of University data and information being processed by manual as well as automated systems and the protection of the records and reports generated by these information processing systems.

1.2 Information is a vital component of University operations, and it is important to ensure that persons with a need for information have ready access to that information. It is equally important to ensure that measures have been taken to protect sensitive information against accidental or unauthorized access, modifications, disclosures, or destruction, in order to ensure the security, reliability, integrity, and availability of information. In addition, federal and state laws assign legal responsibility for the correct and appropriate use of information in order to protect a person's right to privacy.

1.3 This regulation sets forth the responsibilities for data and information security for all individuals and departments at North Carolina Central University who access, process, or have custody of university data.

2. Scope

2.1 Data trustees, stewards and custodians shall ensure that the standards for data security that affect their respective areas of responsibility are effectively implemented. The administrative duties associated with this responsibility shall be assigned by the respective vice chancellors to the owners of the data, who typically are the managers responsible for either the creation or collection of that data and/or the primary user of that information.

2.2 Owners of data are responsible for making decisions about the use and protection of information
in their custody. Areas of concern shall include:

2.2.1 The accuracy and completeness of data and information;
2.2.2 Classification of data as confidential (subject to privacy laws), sensitive (nonpublic salary information) or public;
2.2.3 The authorization process to permit access to the information and to terminate access when necessary;
2.2.4 The identification and minimization of risks and exposures;
2.2.5 The utilization of established procedures designed to protect information from unauthorized access or disclosure, whether accidental or intentional;
2.2.6 Communication of information protection procedures to authorized users;
2.2.7 Physical access to hard copy records, computer terminals and personal computers;
2.2.8 Providing procedural safeguards including backing up information for business continuity purposes; and
2.2.9 Evaluating security control procedures related to information in their custody.

2.3 The users/administrators of information include all persons who have been authorized to read, write or update information.

2.4 The users/administrators of information have the responsibility to:

2.4.1 Use the information only for the purpose that was authorized by the owner;
2.4.2 Comply with all controls established by the owner and those delegated by the owner to administer control procedures;
2.4.3 Avoid disclosure of confidential or sensitive information to unauthorized persons without the permission of the owner or vice chancellor;
2.4.4 Comply with the Family Educational Rights and Privacy Act of 1974 and the North Carolina Central University Privacy Policy; and
2.4.5 Have a signed Confidentiality Statement on file with ITS Planning and Programs.

3. Rule Enforcement
The CIO/CISO/Director shall be responsible for ensuring that appropriate data and information security procedures are published and distributed to all owners and users/administrators of university information (as defined above). This regulation and all supporting procedures and guidelines distributed pursuant to it shall serve as the standards of information and data security to be applied by owners and users/administrators and will be the basis for compliance monitoring, review, and audit. Failure of this policy can and or will result into owners/users/administrators losing part or full access.