1. Purpose

1.1 The purpose of this policy is to establish a structure for all Information Security documents, including policies, regulations and rules. The goal of this policy is to establish the overarching policy for all IT assets including but not limited to: computers, servers, network, data or any information assets of North Carolina Central University (“NCCU” or “University”)

1.2 The IT regulations and rules provide the additional guidance as it relates to specific technologies and systems. This policy gives NCCU and the Chief Information Officer (CIO) the right to create, modify these or other regulations and rules.

2. Scope

2.1 This policy applies to all users of any information system or information system components of NCCU, including all students, faculty, administrators, staff, alumni and visitors of NCCU.

3. Policy

3.1 The University will comply with federal, state and local laws and ordinances, as well as the regulations and guidelines of the University of North Carolina General Administration, regarding information security.

3.2 The Information Technology Services (ITS) regulations and rules are approved by the NCCU Chief Information Officer in consultation with the IT Security Council and Executive Leadership Team and University Planning Council.

3.3 This policy is based on information security best practices and standards of practice for
information security management.

4. Rules Enforcement

4.1 Compliance with all University policies is critical. If these policies and the security processes are not followed, the University could be subjected to fines and other penalties that would hinder the operation of the University.

4.2 Any member of the University community who violates this policy, regulations or rules may be subject to disciplinary action by the University. The University may take action at its discretion to address any violation(s) under this policy, up to and including termination.

4.3 Any violation of this policy, or ITS regulations and rules, by a University student is subject to the Student Code of Conduct in the student handbook. For employees, any violation of this policy is "misconduct" under EHRA policies (faculty and EHRA non-faculty) and "unacceptable personal conduct" under SHRA policies, including any appeal rights stated therein. Violations of law may also be referred for criminal or civil prosecution. Additionally, violations of this policy may result in termination or suspension of access, in whole or in part, to University information systems, where such action is reasonable to protect the University or the University information infrastructure.

4.4 Information Technology Services (ITS), in cooperation with other University authorities and administrators, will enforce this policy, and establish standards, procedures, and protocols in support of the policy.

4.5 The office of the CIO has the responsibility for this policy. The Director of Security and Compliance is responsible for the monitoring of this policy to insure that all University constituents are compliant to this policy and other regulations that fall under the authority of this policy.

4.6 The information security policies, regulations and rules are reviewed annually to ensure effectiveness and suitability given the changing information technology security environment.