Information Technology Governance

I. Purpose. The University of North Carolina and each of the constituent institutions depend on strategic and coordinated governance and management of information technology to fulfill the University’s mission. The University’s information technology and information resource needs continually evolve as new challenges, opportunities, and technologies emerge. Consistent with the governance and oversight responsibilities of the Board of Governors, the executive and administrative responsibilities of the president and the chancellors of the constituent institutions, and the role of the boards of trustees, as described in The Code of The University of North Carolina, the Board adopts this policy delegating and allocating authorities and responsibilities concerning information technology governance within the University of North Carolina System.¹

The purpose of this policy is to foster the efficient development and maintenance of strategically aligned information technology within known and acceptable levels of risk; to ensure an effective and consistent governance and management of information technology at each of the constituent institutions; and to encourage collaboration and shared service arrangements in areas of information technology management, where appropriate, among and between the constituent institutions and the University of North Carolina System Office (UNC System Office).

II. Definitions

A. “Board of Governors” or “Board” means the Board of Governors of the University of North Carolina.

B. “Board of trustees” means a board of trustees of a constituent institution of the University of North Carolina System.

B. “Chancellor” means the administrative and executive head of a constituent institution of the University of North Carolina, as described in Section 502 of The Code.

C. “Constituent institution” means one of the 17-degree/diploma-granting institutions that comprise the University of North Carolina.

D. “Information resources” means information owned or possessed by the University, or related to business of the University, regardless of form or location, and the hardware and software resources used to electronically store, process, or transmit that information.


¹ G.S. 116-11(13); Section 203 A(9) of The Code.
E. “Information technology (IT)” means the hardware and software resources owned, leased, or used by the University and its partners to store, process, or transmit University information. Information technology is a subset of the University’s information resources.

F. “Information technology governance” within the UNC System refers to the framework, policies, rules, standards, structures, and processes established to ensure that the University’s information technology supports the missions, goals, and objectives of the UNC System and each constituent institution; that information technology and information resources are managed in accordance with rules and policies; and that risks and threats to information technology and information resources are appropriately and effectively identified and addressed. IT governance encompasses the planning, prioritization, funding, evaluation, auditing, and security of information technology and information resources at each constituent institution and across the UNC System.

G. “Periodic” means occurring at a frequency deemed appropriate based on an on-going assessment of associated risks.

H. “President” means the chief administrative and executive officer of the University of North Carolina, as described in Section 501 of The Code, who reports to the Board of Governors. The president is responsible for executing the board’s policies directly, through the chancellors, and through the staff who report to the president.

I. “University” or “University of North Carolina System” or “UNC System” means the University of North Carolina, a body politic and corporate defined as a single public multi-campus University composed of 17 constituent institutions, the UNC System Office, and other educational, research, and public service organizations.

III. UNC System IT Governance Program Development; Principles and Guidelines

A. The president shall oversee the information technology governance program applicable to the UNC System and the constituent institutions.

B. The UNC System information technology governance program shall be developed, implemented, and maintained, subject to the president’s approval, by the UNC System’s chief information officer, who shall establish and update the program principles and guidelines on a regular basis in consultation with the UNC Chief Information Officer Council. The details of the information technology governance program shall be confidential and not considered a public record to the extent permitted by North Carolina law.

C. The information technology governance programs shall follow the UNC System requirements, which will include:

1. A defined framework or frameworks to guide the development and implementation of the governance programs; and

2. A set of principles and guidelines addressing planning, prioritization, funding, evaluation, auditing, disaster recovery, privacy, and security of information technology and information resources, risk assessments, risk management, oversight of distributed
IT resources, organizational and staffing models, reporting and lines of authority, and such other areas as may be appropriate for the UNC System and the constituent institutions.

D. The chief information officer, in consultation with leadership at the UNC System Office and the constituent institutions, shall make recommendations to the president at least annually concerning collaborations, shared services arrangements, staffing structures, and additional resources needed to assure that constituent institutions are able to achieve and maintain consistent and effective information technology governance programs.

IV. Information Technology Governance Program. Each constituent institution and the UNC System Office shall establish an information technology governance program consistent with the UNC System’s information technology governance program framework and principles.

A. The chancellor, or the president in the case of the UNC System Office, shall designate the institution’s chief information officer or other member of the chancellor’s senior staff, who will be responsible to the chancellor for oversight of information technology governance at the institution and implementation of the information technology governance framework and program as required by this policy.

B. The institution’s chief information officer shall be vested with such authority as is necessary to successfully oversee the information technology governance program and ensure the establishment and proper implementation and operation of the information technology governance program framework and principles.

V. Oversight of Information Technology Governance

A. The UNC System Office chief information officer shall work with the UNC System Office finance, audit, and legal staff, and the Chief Information Officers Council, to establish the process and criteria by which each constituent institution and the UNC System Office shall demonstrate that it is operating in accordance with the UNC System’s information technology governance program. The minimum criteria will include:

1. Demonstration of a comprehensive information technology governance program that encompasses both centralized IT and distributed IT consistent with the framework, principles, and guidelines established in accordance with Part III of this policy and include:

   a. A set of principles and guidelines concerning information technology matters necessary to the teaching, research, and service missions of the UNC System and the constituent institutions, including but not limited to: security and encryption standards; software standards; hardware standards; acquisition of information technology consulting and contract services; disaster recovery standards; risk management and compliance; networking; wireless technologies; and personal devices; and
   b. Guidelines and priorities for decision-making for information technology that align with the University’s strategic objectives.
2. Periodic self-monitoring and external monitoring of the institution’s compliance with all principles, standards, and guidelines;

3. Periodic audits of information technology and information resource issues by qualified auditors with specialized expertise;

4. Regular information technology risk assessments;

5. Periodic consideration of information technology matters by the audit/compliance/risk management committee of the institution’s board; and

6. Effective systems of accountability to identify and correct deficiencies.

B. The Board of Governors and the board of trustees of each constituent institution shall assign responsibility for oversight of IT governance to a standing committee of the board with audit responsibility.

1. Annual audit plan. The annual audit plans of the constituent institutions shall consider, as appropriate, audit activity focused on information technology matters, based on annual risk assessments.

2. Audits. The assigned committee with responsibility for IT governance shall review and discuss audit activity relating to information technology matters, and address issues of importance in information technology governance on a regular basis at its scheduled meetings.

3. Reporting. The assigned committee with responsibility for IT governance may request information and reporting related to the institution’s IT governance program. All audit reports involving information technology governance matters will be shared with the Committee on Audit, Risk Management, and Compliance (CARMC).

VI. Other Matters

A. Effective Date. The requirements of this policy shall be effective on the date of adoption by the Board of Governors.

B. Relation to State Laws. The foregoing policies as adopted by the Board of Governors are meant to supplement, and do not purport to supplant or modify, those statutory enactments which may govern the activities of public officials.

C. Regulations and Guidelines. These policies shall be implemented and applied in accordance with such regulations and guidelines as may be adopted from time to time by the president.
Information Security

I. Purpose

This policy directs UNC General Administration and the constituent institutions of the University of North Carolina to establish an information security program and designate a senior officer, accountable to the president or chancellor, who is responsible for information security. This policy also requires the Board of Governors and constituent institution boards of trustees to oversee information security.

II. Definitions

A. “Information security program” means policies, assessments, protocols, and trainings designed to govern the storage, accessibility, and security of information resources.

B. “Information resources” means information owned or possessed by the University, or related to business of the University, regardless of form or location, and the hardware and software resources used to electronically store, process, or transmit that information.

III. Establishment of Information Security Program

UNC General Administration and each constituent institution shall develop and maintain an information security program to preserve the security, confidentiality, accessibility, and integrity of information resources of UNC General Administration or the constituent institution. The programs developed by UNC General Administration and the constituent institutions must comply with the prevailing information security standard adopted by the Board of Governors standing committee assigned with audit responsibility. At a minimum, this program must include policies on the storage, use, and accessibility of information resources, regular risk assessments of existing information resources, a strategy statement setting forth priorities for managing identified information security risks, and incident response planning and notification procedures.

IV. Designation of Senior Officer with Information Security Responsibility

UNC General Administration as well as each constituent institution shall identify a senior officer accountable for overseeing implementation and periodic evaluation of the information security program. The identified senior officer shall be responsible for identifying and deploying all reasonable measures to maintain the security, confidentiality, accessibility, and integrity of information resources of UNC General Administration or the constituent institution. The senior officer, as an essential component of the officer’s designation, shall possess all necessary authority to implement and evaluate all aspects of the information security plan. The senior officer shall be accountable to the president or chancellor and responsible for reporting to the Board of Governors or the constituent institution’s board of trustees on matters related to information security upon request.

V. Oversight of Information Security

The Board of Governors and the board of trustees of each constituent institution shall assign responsibility for oversight of the institution’s information security program to a standing committee of the appropriate board with audit responsibility.

A. Audit Planning and Risk Assessment. Each institution’s internal auditor shall address information security in annual audit planning and risk assessment. The assigned committee shall ensure that information security is addressed in the annual audit planning and risk assessments that are conducted by the institution’s internal auditor.

B. Agenda Item at Regular Meetings. The assigned committee shall periodically include an agenda item for emerging information security matters at its regularly scheduled meetings.
C. Annual Report. The designated senior officer with information security responsibility shall present a report to the assigned committee, at least annually, on the institution’s information security program and information technology security controls.

VI. Other Matters
A. Effective Date. The requirements of this policy shall be effective on the date of adoption of this policy by the Board of Governors.
B. Relation to State Laws. The foregoing policies as adopted by the Board of Governors are meant to supplement, and do not purport to supplant or modify, those statutory enactments which may govern the activities of public officials.
C. Regulations and Guidelines. These policies shall be implemented and applied in accordance with such regulations and guidelines as may be adopted from time to time by the president.
User Identity and Access Control

I. Purpose. The security, privacy, and integrity of data and information systems is an operational priority for the University of North Carolina. Identity confirmation and access control techniques help mitigate the risk of unauthorized access to University data and information systems. This policy directs all University of North Carolina System constituent institutions to evaluate and conduct risk-based implementation of appropriate identity confirmation and access control techniques, such as multi-factor authentication, to control access to University data.

II. Risk-Based Implementation of Identity Confirmation and Access Control Measures. The UNC System chief information officer shall, in consultation with the Chief Information Officers Council, develop, maintain, and update standards for risk-informed identity confirmation and access control, such as multi-factor authentication, for use by constituent institutions and the UNC System Office. In the absence of multi-factor authentication, constituent institutions shall identify, implement, and document other appropriate measures to control access to sensitive data. Based on evaluation of the constituent institutions’ identity confirmation and access control techniques, the University chief information officer may identify constituent institutions that require additional resources or consultation to implement and maintain adequate measures and meet the requirements of this policy.

A. Each constituent institution and the UNC System Office shall, implement and maintain risk-informed techniques to confirm user identity and control access to University information systems and resources, in accordance with the standards developed and maintained by the UNC System chief information officer.

B. The chancellor, or the president in the case of the UNC System Office, shall designate the institution’s chief information officer or other member of the senior staff, who will be responsible for the oversight of the implementation and maintenance of user identity confirmation and access control techniques as required by this policy. The institution’s chief information officer shall be vested such authority as is necessary to successfully oversee all aspects of the user identity confirmation and access control program as it applies to staff, faculty, students, and other individuals with access to the institution’s information technology systems and information resources.

C. Each institution’s user identification and access control measures must sufficiently control access to sensitive University data such as personally identifiable information, personal health information, and information subject to state or federal laws or regulations.

D. The timing and application of user identification and access control measures, such as multi-factor authentication and other techniques, shall be conducted in accordance with the standards maintained by the UNC System chief information officer, and guided by a risk-based evaluation of university data and information systems.

E. The standards developed and maintained by the UNC System chief information officer and the standards and measures established by the constituent institutions in accordance with
those policies shall be confidential and not considered a public record to the extent permitted by North Carolina law.

F. The UNC System Office chief information officer shall work with the UNC System Office finance, audit, and legal staff, and the Chief Information Officers Council, to establish the process and criteria by which each constituent institution and the UNC System Office shall demonstrate that it is operating in accordance with the requirements of this policy.

IV. Other Matters

A. Effective Date. The requirements of this policy shall be effective on the date of adoption of this policy by the Board of Governors.

B. Relation to State Laws. The foregoing policies as adopted by the Board of Governors are meant to supplement, and do not purport to supplant or modify, those statutory enactments which may govern the activities of public officials.

C. Regulations and Guidelines. These policies shall be implemented and applied in accordance with such regulations and guidelines as may be adopted from time to time by the president.