1. General

The University’s information technologies (IT) resources must be managed in a manner that enables the University to apply new technologies and adopt new processes effectively and efficiently while enhancing and encouraging the innovation required for fulfilling all aspects of the University’s mission. To accomplish this goal, an IT governance framework has been developed based on a collaborative model that includes transparency, formal input, review, and approval processes, recognizing that the University has certain healthcare components, including an academic health center, that have regulatory and business obligations that compel administering differing levels of physical, technical, and administrative privacy and security requirements from those in other areas of the University. This policy describes the governance framework and defines roles and responsibilities to ensure effective input and decision-making pertaining to IT policies, standards, guidelines, processes, and procedures.

1.1. Information Technologies Governed by this Policy

The term IT is applicable to a wide array of technology services used throughout UNM, both centrally managed by UNM Information Technologies (UNM IT) and locally managed by individual units not affiliated with UNM IT. For the purposes of this policy, the term includes but is not limited to:

- Telecommunications, Internet/network access, and facilities infrastructure (e.g., voice and data networks and supporting cable plant).
- Computing (e.g., end user devices, servers, and development environments for productivity and high performance computing).
- Enterprise-wide applications and user services (e.g., Banner, email).
• Instructional technology (e.g., classroom media systems and services, online learning/distance education).
• Video (e.g., CATV, video applications on the network, security video).
• Peripheral technologies (e.g., printing and scanning).
• Information security (e.g., information security assessments).

2. Roles and Responsibilities

Roles and responsibilities for the individuals and groups involved with IT governance at UNM are described in the following sections.

2.1. IT Governance Council

The IT Governance Council provides direction on IT issues, reviews and approves the UNM IT Strategic Plan, and provides a conduit for communicating IT issues throughout the University. The IT Governance Council consists of representatives from UNM’s executive administration appointed by the University President, and oversees and provides escalation for the following advisory boards:

- IT Academic Technologies Advisory Board
- IT Administrative Technologies Advisory Board
- IT Research Technologies Advisory Board
- IT Funding Task Force

The Chair of each advisory board serves on the IT Governance Council and is responsible for providing advisory board recommendations on strategic direction, operational guidelines, policies, standards, and priorities as defined in the Board’s respective charter. The University President may add or remove advisory boards as needed.

2.2. UNM Chief Information Officer (UNM CIO) and the Health Sciences Center CIO (HSC CIO)

The UNM CIO provides leadership, integrative management, and direction for the University's shared IT services to include institution-wide strategic planning and budgeting for IT. The UNM CIO also oversees coordination of all IT related functions across the University. The UNM CIO serves as the University’s senior spokesperson on issues related to information technologies and serves as a member of the President’s executive cabinet. In order to allow for the delivery of patient care and other activities at the HSC consistent with state and federal regulatory obligations relative to physical, technical, and administrative safeguards, the HSC CIO is responsible for IT governance and standards for HSC delivered technology services (https://hsc.unm.edu/about/cio/information-security/policy.html).

2.3. IT Joint Operations Committee

The IT Joint Operations Committee provides an opportunity to collaborate on cross-campus (Main and HSC) technology efforts. The goal of these collaborations is to improve services for users, realize cost savings from joint purchasing, exchange
The IT Joint Operations Committee is co-chaired by the UNM CIO and the HSC CIO, and includes equal representation from UNM IT groups and the HSC component IT groups.

2.4 UNM IT Officers

IT Officers manage the administration of IT services for one or more designated areas of the University, typically for a college, school, branch campus, or administrative unit. As a part of the Office of the CIO, IT Officers report to the Associate Director of IT Campus Outreach and Engagement for overall direction while receiving area-specific priorities and guidance from administration within their designated areas. The IT Officers are responsible for fulfilling area-specific technology requirements and priorities while working with campus-wide IT resources to ensure effective and efficient solutions and services. The IT Officers advocate the area’s strategic initiatives and differentiated needs within the UNM IT service framework while ensuring appropriate use of institutional resources to develop and deliver streamlined solutions.

3. IT Policies

IT policies are designed to provide the University community with unifying statements that describe fundamental IT principles, the reasoning behind the principles, and institutional procedures necessary for implementation. The development of effective policy statements requires both input from individuals who have extensive knowledge on the subject matter and input from individuals affected by the policy.

IT policies contain governing principles that mandate or constrain actions and have University-wide application. The policy will state applicability to students, staff, faculty, and/or visitors and compliance is mandatory. If exceptions are allowed, the authority and procedure for requesting an exception will be delineated in the policy.

4. IT Standards

IT standards are based on industry best practices designed to ensure that IT resources are effectively managed in support of the University’s mission of education, research, and public service. IT standards define procedures, processes, and practices designed to provide an efficient, effective IT system; protect confidential information; minimize security risks; ensure compliance with federal and state laws and regulations, and facilitate an open, interoperable, accessible IT infrastructure that meets the needs of students, faculty, staff, and the University community. The development of effective IT standards requires both input from individuals who have extensive knowledge on the subject matter and input from individuals affected by the standard. The type of technology addressed in the standard will determine the groups or individuals required to comply with the standard. Some standards such as password standards will apply to all users, whereas others may apply only to system administrators. Each standard will define those individuals who are required to comply with the standard. Failure to comply with a standard may damage a system, risk security, result in loss of IT privileges, and/or disciplinary action.
5. IT Guidelines

IT guidelines are directives and specifications, similar to standards, but advisory in nature. In essence, IT guidelines constitute recommendations that are not binding; however, it should be noted that failure to comply with IT guidelines may result in damage to a system and/or inefficient processes. The development of effective IT guidelines requires both input from individuals who have extensive knowledge on the subject matter and input from individuals affected by the guideline.

IT guidelines are not mandatory, but failure to follow applicable guidelines may result in less effective system performance and may negatively impact an individual’s job or academic performance. IT guidelines may evolve into IT standards with the appropriate steps and communication (see Section 4).

6. IT Processes and Procedures

IT processes and procedures provide electronic and manual mechanisms for IT-related functions or job duties.

IT processes and procedures are usually designed in the course of project development activities and are approved as part of the overall project approval. These processes and procedures are documented in accordance with industry standards and communicated in conjunction with the associated project.

Compliance with IT processes and procedures is critical to the correct functioning of the selected application.

7. Departmental IT Policies, Standards, Guidelines, Processes, and Procedures

Colleges, schools, branch campuses and departments may establish additional departmental information technologies policies, standards, guidelines, and processes provided they comply with IT policies, standards, guidelines, and processes and are documented and communicated to their employees.

8. Related Policies

UAP 1100 (“Development and Approval of Administrative Policies”)
UAP 2500 (“Acceptable Computer Use”)
UAP 2510 (“Computer Use Guidelines”)
UAP 2520 (“Computer Security Controls and Access to Sensitive and Protected Information”)
UAP 2530 (“Remote Electronic Input to the Financial Accounting Systems”)
UAP 2540 ("Student Email")

UAP 2550 ("Information Security")

UAP 2580 ("Data Governance")

UAP 2590 ("Access to Administrative Computer Systems")