DRAFT OF 3-19-2018 - track changes

Administrative Policies and Procedures Manual -
Policy 2560: Information Technology (IT) Technologies Governance

Date Originally Issued: 08-01-2007

1. General

It is critical that the University's information technology (IT) resources, applications, and manpower 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 the University to excel in fulfilling all aspects of its 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 for decision making, 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 the roles and responsibilities of individuals and groups involved with IT governance to ensure effective input and decision-making pertaining to IT policies, standards, guidelines, processes, and procedures.

1.1. Information Technology Governing by this Policy

The term IT is applicable to a wide array of technology systems/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 learning).
- 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. UNM IT Governance Council

The IT Governance Council provides direction on IT issues, reviews, and approves the University's 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 information systems and services to include institution-wide strategic planning and budgeting for information technologies. 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. UNM IT Cabinet

The IT Cabinet advises and collaborates 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).

2.4. IT Managers Council

The IT Managers Council supports the development of University-wide IT policies and standards and the effective execution of collaborative, University-wide IT plans and projects. The IT Managers Council assures effective communications across enterprise-level IT organizations and works with IT agents to ensure alignment of departmental IT operations. Council members are appointed by the CIO and include senior managers in IT service provider organizations (e.g. ITS and High Performance Computing).

2.5. IT Agent Networking Group

The IT Agent Networking Group provides support for IT agents, facilitates cross-unit communication and collaboration, and assures Level 3 representation in IT governance. IT Agent Networking Group members are appointed by the CIO and include IT agents from Level 3 organizations as defined by Banner Finance (e.g. school or college level) who serve as the main point of contact with IT service provider organizations (e.g. ITS and High Performance Computing).

3. Overview of IT Policies, Standards, Guidelines, Processes, and Procedures

Policies, standards, guidelines, processes and procedures take a tiered approach to defining IT principles and providing IT-related direction to the University. The table below defines the differing levels of scope, authority, and compliance requirements for each category.

<table>
<thead>
<tr>
<th>Scope</th>
<th>Approval</th>
<th>Communication</th>
<th>Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Policies</td>
<td>University-wide, high-level policy</td>
<td>UNM President</td>
<td>All faculty and staff and students where applicable</td>
</tr>
</tbody>
</table>
4. UNM IT Policies

**UNM 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 information, and reduce unnecessary technology investment duplication. 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. They help ensure compliance with applicable laws and regulations, enhance the University’s mission, promote operational efficiencies, and/or reduce...
institutional risk. Due to regulatory and other requirements the Health Sciences Center (HSC) may have supplementing HSC IT policies that are overseen by the Associate Vice President for Knowledge Management & Information Technology, with review from the Knowledge Management and Information Technology program committees and other relevant authoritative bodies.

4.1. Development

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. Anyone wishing to propose an IT policy statement should send their request to the UNM IT Cabinet. If the Cabinet determines a need for a specific policy, it will assign individuals most closely involved with the subject matter to work with the UNM Policy Office to develop a preliminary draft. The preliminary draft will be reviewed by the IT Managers Council and then sent to the IT Agents Networking Group for comment. The Networking Group will forward their comments to the IT Managers Council for consideration. After the Council's review, the proposed policy is sent to the IT Cabinet and the IT Governance Council for endorsement. After endorsement, the UNM Policy Office will follow standard UNM protocol for approval of institutional policy. This protocol includes review by key areas selected based on the nature of the proposed policy, Deans Council, the President's Executive Cabinet, and the campus as a whole.

4.2. Approval and Communication

All UNM IT policies must be approved by the President in writing before distribution. Upon approval by the President, the policy is placed on the UNM Policy Website (www.unm.edu/~ubppm) and the campus is notified of the new policy via email. Information concerning the policy will also be posted on the CIO website.

4.3. Compliance

UNM 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. Individuals who fail to comply with University policy will be subject to disciplinary action up to and including discharge or dismissal from the University. Violations of IT policies should be reported to the Office of the CIO.

4.4. Review and Revision

IT policies will be reviewed by the IT Cabinet periodically to ensure policies are up-to-date and meeting the needs of the University. The development and approval requirements discussed in Sections 4.1 and 4.2 herein also apply to revisions of existing policy.
5. IT Standards

UNM 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.

5.1. Development

To ensure that IT standards effectively support the mission of the University and meet the needs of the University community, development of IT standards requires a broad base of participation and involvement of subject matter experts. Draft standards will be developed by the IT Managers Council and then sent to the IT Agents Networking Group for review and comment. The Networking Group will forward their comments to the IT Managers Council for consideration. The Council will publish the proposed standard on the CIO website and solicit comments from the campus. The IT Managers Council will update the standard based on campus comment and submit it to the IT Cabinet for review.

5.2. Approval and Communication

IT standards must be approved by the CIO in writing prior to distribution. Upon approval, ITS will notify all individuals impacted by the standard prior to its effective date and post the standard on the CIO website. When a new IT standard is issued, the standard will indicate the timeframe for compliance, based on but not limited to, criticality, funding limitations, and/or equipment replacement cycles. IT standards specific to the Health Sciences Center (HSC) are managed by the Associate Vice President for Knowledge Management & Information Technology and are published on the HSC website.

5.3. Compliance

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. To request an exception to an IT standard, submit a written justification to the CIO. For exceptions to HSC-specific IT standards, submit the justification to the Associate Vice President for Knowledge Management & Information Technology. Violations of IT standards should be reported to the Office of the CIO.

5.4. Review and Revision
IT standards will be reviewed by the IT Managers Council periodically to ensure standards are up-to-date and meet the needs of the University. The development and approval requirements discussed in Sections 5.1 and 5.2 herein also apply to revisions of existing IT standards.

65. 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.

6.1. Development

IT guidelines are developed by IT personnel in consultation with applicable users and based on industry practices.

6.2. Approval and Communication

IT guidelines must be approved by the CIO in writing. Upon approval, the CIO's Office will notify all individuals impacted by the guidelines and post the guidelines on the CIO website. IT guidelines specific to HSC are managed by the Associate Vice President for Knowledge Management & Information Technology and are published on the HSC website.

6.3. Compliance

IT guidelines are not mandatory, but failure to follow applicable IT 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).

6.4. Review and Revision

IT guidelines will be reviewed by the IT Managers Council periodically to ensure guidelines are up-to-date and meet the needs of the University. The development and approval requirements discussed in Sections 5.1 and 5.2 herein also apply to revisions of existing IT guidelines.

76. IT Processes and Procedures

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

7.1. Development
IT processes and procedures are developed by IT personnel in conjunction with applicable administrative personnel and are generally developed at the departmental and unit levels.

**7.2 Approval and Communication**

IT processes and procedures are usually designed in the course of application 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.

**7.3 Compliance**

Compliance with IT processes and procedures is critical to the correct functioning of the selected application. Any problems or issues associated with an IT process or procedure should be reported to fastinfo@unm.edu.

**7.4 Review and Revision**

IT processes and procedures are reviewed periodically for applicability and accuracy and updated as required in accordance with the associated application approval protocols.

**8. 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 University IT policies, standards, guidelines, and processes and are documented and communicated to departmental employees.

**9. 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 2090 ("Access to Administrative Computer Systems")