Authorizations and Scope
The responsibility for university-wide IT policy management has been assigned to Information and Infrastructure Assurance (IIA). This includes:

- Coordination of IT policy and underlying development, dissemination, and education
- Review and analysis of existing policies for continued applicability and effectiveness.
- Interpretation of current policy related to specific issues, situations and incidents.

The IT policy framework covers all campuses, including Flint, Dearborn, and the Health System; unit-level policies and guidelines (including for the Flint and Dearborn campuses) are out of scope. University IT policies apply to all users of U-M IT resources, including students\(^1\), faculty, staff, and sponsored or guest users.

Rationale
Information technology policies articulate the university’s vision, strategy, and principles as they relate to the management and use of information and information technology resources, while supporting core academic, research, and teaching and learning missions. Further, IT policies also ensure compliance with applicable laws and regulations, promote operational efficiency, and manage institutional risk by specifying requirements and standards for the consistent management of IT resources across the university. This university-wide IT policy framework\(^2\) specifies:

- Structure and criteria for what should be categorized as an IT policy, guideline, or standard
- A process for initiating, reviewing, approving, and expiring IT policies
- Ongoing roles and responsibilities associated with IT policy development and maintenance

---

\(^1\) It is a principle of this IT policy framework that, wherever appropriate, policies should apply to all members of the university community, including students. Current articulation of IT policies that apply to students is awkward at best. The Statement on Student Rights and Responsibilities is the primary institutional document that defines appropriate use of IT resources by students. It does so by referring to the Proper Use SPG 601.07-0, which, like all SPGs, says that it applies to all faculty and staff. As this policy framework begins to be applied, IIA will work with the Office of the Vice President for Student Affairs to improve documentation of IT policies for students.

\(^2\) Best practices from other universities have been adopted in the development of this framework.
Principles

The IT policy structure and process employ the following principles:

• Policy work shall be initiated when there is a compelling need for new or revised policy. Triggers may include new technologies, new laws or regulations, or operational or compliance needs that are not appropriately covered by existing policies or guidance.
• Policies and guidance shall be implementable and sustainable. Impact analysis on both IT systems and end-users should be included in the policy planning and review processes.
• Any unit may request consideration of new IT policies or changes to existing policies that apply university-wide; the process to be followed for such consideration is outlined in this IT policy development and administration framework.
• IT policy development shall be accomplished via individual workgroups convened to address specific topics. Each team will include appropriate subject matter experts. IIA will provide a central coordination function to ensure consistency and to address policy dependencies.
• The policy development process shall be transparent. Input from stakeholders will be addressed and/or incorporated throughout the process. Preliminary/interim policies and guidelines will be posted and disseminated to solicit feedback.
• The policy development process shall be flexible. Circumstances may necessitate the publishing of best practices as a stop-gap to provide immediate guidance while a policy is being developed, vetted, and approved. In other cases, a policy may be established with detailed guidance to be provided at a later time.
• University-wide policies shall be considered a floor, not a ceiling. Unit-level policies, guidelines, standards, or procedures may be developed to supplement university-wide guidance. They must meet the minimum criteria set forth in university-wide policies and related guidance, but may be more restrictive.

Roles and Responsibilities

The roles and responsibilities defined below represent the staff positions or groups most directly involved in IT policy development.

Chief Information Officer (CIO): The CIO has overall responsibility for IT policy and policy development at U-M, and approves new and revised standards and guidelines based on the recommendation of the Executive Director.

IIA Council: The Council provides ongoing oversight and direction for IT policy program; sets policy development priorities; and reviews and approves new or revised policies as the second level of governance approval.

Chief Information Security Officer (CISO)/IIA Executive Director: The CISO works with the IT Policy and Compliance Lead to ensure alignment of the IT Policy program with strategic ITS, Office of the IO, and University of Michigan objectives and priorities. The CISO also serves as the liaison between the IIA staff managing the IT policy function and the CIO, the IIA Council, and the IT Council.

IT Policy and Compliance Staff: IT policy and compliance staff provide overall direction for the IT policy function, including responsibilities for identifying and prioritizing policy needs, ensuring appropriate campus involvement in policy development, and conducting research and benchmarking for emerging policy development.
The IT Policy and Compliance Lead provides day-to-day staff support for the policy development function, serves ex officio on policy development working groups, and plans and executes policy education and awareness efforts. Specifically, this includes managing an annual review and analysis of existing policies, standards, and guidelines for continued applicability and effectiveness; interpretation of current policies in response to unit/departmental inquiries or specific incidents.

**IT Policy Governance and Approval**

The IT governance structure established in 2010 is intended to set campus-wide priorities for IT services, resources, and facilities. An important foundation in support of these priorities involves reestablishing a campus-wide IT policy function.

The IT policy function shall reside with the Office of the Chief Information Officer, with delegated responsibilities to Information and Infrastructure Assurance for policy development, coordination, education, and maintenance.

The following identifies the different levels of governance review and vetting of policies, standards and guidelines (initially drafted by IT policy development working groups):

1. **CISO/IIA Executive Director**: Initial review of policies, guidelines, and standards
2. **CIO**: First level of governance review for IT policies; final approval of guidelines and standards before adoption and dissemination to campus
3. **IIA Council**: Second level of governance review for IT policies, standards, and guidelines
4. **IT Council**: Third level of governance review for IT policies; new or substantially revised policies require IT Council approval
5. **IT Executive Committee**: Final level of governance review for IT policies; policies recommended for adoption as a new or revised Standard Practice Guide require approval of the IT Executive Committee.

**Stakeholder Involvement**

Campus stakeholders will be engaged throughout the IT policy development process—in both individual and group settings—to ensure that all appropriate perspectives are accounted for and incorporated as feasible in final versions of new or revised policies, standards, and guidelines. IIA maintains a list of potential stakeholders to be involved at various stages in the IT policy life cycle process.

Specific individuals and groups will be identified during the planning and initiation phase of a given policy, standard, or guideline. Membership in policy development working groups will vary based on the primary content of a policy being developed. The IT Policy and Compliance Lead will serve ex officio and provide staff support to all working groups. In general, any faculty or staff member will be able to provide comments on draft and interim policies, standards, and guidelines on the IT policy web site. Specific stakeholders may be identified and solicited to provide input and review, while others may be only in the need to inform category.
Students, student groups, and student governments will have opportunities to provide input and feedback on draft policies, standards, and guidelines that deal with student code of conduct amendments or have the potential to impact availability of, or access to, IT resources for students.

**IT Policy Structure and Criteria**

Categories of university-wide guidance (see Appendix 1 for additional information about these categories):

- **University IT Policies** articulate the university’s values, principles, strategies, and positions relative to a broad IT topic. They are designed to guide organizational and individual behavior and decision making. They are concise, high-level, and independent of a given technology. University IT policies are mandatory. All new or substantially revised policies, once approved by the IT Executive Committee, will be submitted to University Audit for inclusion in the online Standard Practice Guide.
  
  **Examples:** Proper Use of Information Resources, Information Technology, and Networks
  
  Information Security Policy

- **University IT standards** specify requirements for becoming compliant with university IT policies, other university policies, as well as applicable laws and regulations. Standards may include technical specifications. Standards are mandatory.
  
  **Examples:** Domain Name System Standards
  
  IP Address Standards

- **University IT guidelines** provide guidance and best practices relative to a particular IT topic. They may accompany, interpret, or provide guidance for implementing IT policies, other university policies, or applicable laws and regulations. University IT guidelines are not mandatory.
  
  **Examples:** Guidelines for eDiscovery
  
  Privacy and Retention of Security Logs

- **IT Procedures** document “how to” accomplish specific IT tasks or use IT services. These procedures may be localized to reflect the practices or requirements of a specific unit.

**Approach and Publication**

The IT policy framework will create processes and structures that are consistent with the university Standard Practice Guide (http://spg.umich.edu/) and specifically apply to information and information technology policies.

IT policies will be documented and considered for approval as SPGs (see above). SPGs are currently pdf files; searchable web versions of IT policies and guidelines will be posted at the IIA SafeComputing IT policy web site so that they can be effectively operationalized and readily accessed by campus IT staff and departments. Multiple communication methods will be employed to widely disseminate policies and guidelines.

While it is necessary to provide a flexible policy/guidance structure that keeps pace with technological innovations, process simplicity will be balanced with concerns over legal exposure and assurance of stakeholder collaboration. Ultimately, this policy framework will result in a process that provides proper scoping, collaborative development, and structured vetting and approval.
IT Policy Life Cycle Process

The IT policy life cycle process is based on the Policy Development Process With Best Practices issued by the Association of College and University Policy Administrators, and applies to university-level guidance including policies, standards, and guidelines. Standards and guidelines may require fewer approvals than formal policies.

1. Identification, Planning and Initiation
   a. Identify compelling need for new or updated policy/guidance. Drivers may include new regulatory requirements, technology developments, operational needs, and identification of current issues or gaps. Request may come from any unit, central office, or IIA.
   b. Determine whether the need should be satisfied by a policy, guideline, or standard
      i. See Appendix 2: IT Policy Criteria Decision Tree
   c. Identify sponsorship, stakeholders, working group members and their relevant roles
   d. Develop high level implementation impact analysis
   e. Obtain approval to proceed with draft policy (or guideline, standard)
   f. Prioritize and schedule policy work

2. Development, Review, and Approval
   a. Draft initial policy (guideline, standard)
   b. Distribute to a small group of stakeholders for initial review and input
   c. Incorporate initial feedback
   d. Distribute to a larger group of stakeholders for review and input
   e. Post final draft on the IT policy web site for general feedback
   f. Review and, where appropriate, incorporate feedback
   g. Present to appropriate governance entity for approval (see table on p. 3)
   h. Obtain approval

3. Rollout
   a. Post and announce guidance (policy standard, guideline)
   b. Conduct educational activities
   c. Initiate implementation activities (efforts to develop/update standards and guidelines may be needed for some new policies)
   d. Determine ongoing review cycle (default review cycle is annual)

4. Compliance, Review and Maintenance
   a. Monitor compliance and effectiveness of implemented guidance
   b. Review and implement modifications per annual review cycle (last revision and review dates shall be posted on each policy). IIA, the policy owner, and OGC will generally be responsible for most policy reviews.

5. Policy Retirement
   a. As part of the maintenance and review process, policies, standards, and/or guidelines may be identified as out-of-date or no longer needed. They will be retired via the same process by which they were approved.
### Appendix 1: IT Policy Structure Definitions

<table>
<thead>
<tr>
<th>Category</th>
<th>Purpose</th>
<th>Applicability</th>
<th>Approval Authority</th>
<th>Communications Approach</th>
<th>Frequency of Change</th>
<th>Other Characteristics and Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>University IT Policies</td>
<td>• Have broad application throughout the university&lt;br&gt;• Articulate university’s values, principles, strategies, and positions&lt;br&gt;• Guide institutional decisions and direct individual behavior&lt;br&gt;• Support and enhance university’s mission&lt;br&gt;• Clarify requirements and exceptions&lt;br&gt;• Interpret and help comply with laws and regulations&lt;br&gt;• Help manage institutional risk&lt;br&gt;• Help promote operational efficiency</td>
<td>• University-wide, all campuses&lt;br&gt;• Typically apply to all users of university information resources (students may have separate policies/codes of conduct)</td>
<td>• One or more university executives (Provost, EVP/CFO, EVPMA)</td>
<td>• Formally published as SPGs&lt;br&gt;• Web version published on IT policy site</td>
<td>• Revisit annually</td>
<td>• Mandatory&lt;br&gt;• Independent of specific technologies&lt;br&gt;• Short, concise, clear&lt;br&gt;• Must be implementable and enforceable&lt;br&gt;• Consequences of non-compliance are typically provided&lt;br&gt;• Accountability for implementation must be specified&lt;br&gt;• Includes definition of terms (that are consistent across policies)&lt;br&gt;• Template (link tbd)</td>
</tr>
<tr>
<td>University IT Guidelines</td>
<td>• Provide guidance and best practices relative to a particular IT topic&lt;br&gt;• May accompany, interpret, or provide guidance for implementing IT policies or policy aspects</td>
<td>• University-wide, all campuses</td>
<td>• IT process owner for a given topic</td>
<td>• Web version published at IT policy site</td>
<td>• Revisit annually</td>
<td>• Not- mandatory, may provide alternative approaches&lt;br&gt;• May depend on specific technologies&lt;br&gt;• Generally high-level – do not include step-by-step process&lt;br&gt;• Typically reference a parent policy&lt;br&gt;• Template (link tbd)</td>
</tr>
<tr>
<td>Category</td>
<td>Purpose</td>
<td>Applicability</td>
<td>Approval Authority</td>
<td>Communications Approach</td>
<td>Frequency of Change</td>
<td>Other Characteristics and Notes</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>-----------------------------------</td>
<td>--------------------</td>
<td>-------------------------</td>
<td>---------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| University IT Standards                      | • May accompany, interpret, or specify requirements for implementing IT policies or policy aspects  
• Serve to accomplish compliance or risk mitigation  
• May interpret laws and regulations (for example, may specify acceptable encryption methods to accomplish HIPAA compliance)  
• May specify rules for using a specific IT service | University-wide, all campuses (for a given topic) | IT process owner for a given topic or IT service provider | Web version published at IT policy site | Revisit annually | • Mandatory  
• May depend on specific technologies  
• Clear and specific  
• Template (link tbd) |
| Procedures                                   | • Detailed step-by-step instructions  
• May implement policies or guidelines | As stated | Applicable IT service provider | Posted at appropriate web site | Revisit annually | • Out of scope for IT policy project  
• Must be consistent with IT policies and applicable standards |
| Campus IT Policies, Guidelines, or Standards  | • As defined above when unique campus-level requirements exist. For example, UMHS has a set of detailed campus-level policies to address HIPAA requirements. | Campus-wide (Health System, Flint, Dearborn) | Applicable campus authority | Posted at appropriate web site | | • Out of scope for IT policy project  
• Needed only when campus-level unique situations need special handling  
• Consistent with university policies but may be more restrictive |
| Unit-Level IT Policies, Guidelines, or Standards | • As defined above when unique unit-level requirements exist. For example, B&F has developed security policies that are more detailed than university-wide policies. | Unit-wide | Applicable campus authority | Posted at appropriate web site | | • Out of scope for IT policy project  
• Needed only when campus-level unique situations need special handling  
• Consistent with university policies but may be more restrictive |
Appendix 2: IT Policy Criteria Decision Tree

An IT Policy Decision Matrix and Decision Tree flow chart are available as planning guides and process reminders for policy development working groups. Both are based on the process flow described below.

IT Policy Decision Matrix (Appendix 3)
IT Policy Decision Tree Flow Chart (Appendix 4)

During the Planning and Initiation step of the IT policy life cycle process, the need for new or updated guidance may be triggered by various issues such as:

1. Laws, regulations or best practices which require new or updated guidance
2. Implementation of IT services or new technologies that require new or updated policies
3. Risk assessment, audits, and/or reviews of existing policies/guidance that reveal inconsistencies or gaps
4. Operational issues that require clarification of university’s position

The planning process involves stepping through a list of questions to determine whether there is a compelling need for a guidance effort and, if so, what type of guidance (policy, standard, guideline) needs to be created. Questions and suggestions for relevant decisions are listed below.

1. What are the consequences/risks of not having documented guidance covering this topic?
   a) Is there a legal requirement to have documented guidance?
   b) Are there operational issues that require clear statement of direction?
   c) Is there new technology (such as cloud computing) that requires university-wide guidance?
   d) Will documenting (and implementing) this guidance mitigate risks?

   If the answer to any of the above is “yes,” documented guidance may be necessary.

2. What are the consequences/risks of having documented guidance covering this topic?
   a) Is this guidance implementable?

       Does this guidance represent a strategy that we would like units to plan for, although it may not be currently implementable?

   b) Is there an existing policy (SPG) that already addresses this topic?

   c) Does the proposed guidance contradict (explicitly or implicitly) current university policy, bylaw, or other laws/regulations?

   If the guidance is necessary but not implementable across the university within a reasonable time frame, starting with guidelines (rather than a policy) is preferable. If there is a contradiction or inconsistency between the proposed guidance and existing policies or laws, further analysis is necessary with the participation of appropriate stakeholders to determine how to handle. An
existing policy may be obsolete or substantially out-of-date; therefore, updating or expiring the existing policy may be the appropriate option.

3. Should this guidance be mandatory? Is it technology-dependent?
   a) Is there a federal or state law requiring the university to follow this?
   b) Is there a contractual obligation for the university to follow this?
   c) Is there another reason why this should be mandatory?
   d) Will this guideline change when new technology is implemented? What part of the guidance is technology-dependent and what part can be stated as a general policy?

If the guidance is mandatory, implementable, and applicable across the university, and technology-independent, it should be stated as a policy. If it is mandatory, implementable, and applicable across the university, but specific to a particular technology, it should be stated as a standard. Another option is to create a combination of a short, high-level policy statement, and a detailed, technology-dependent standard.

4. Can the essence of this guidance be summarized in no more than one page?

Short, high-level policy statements will typically be documented as a policy. More detailed documentation can be provided as standards, guidelines, or procedures. If the guidance cannot be summarized succinctly, and an umbrella policy does not exist, it may need to be represented as a combination of a policy and guidelines or standards.

5. How often do policies and related guidance need to be reviewed in order to stay current and applicable?

Policies and related guidance should be reviewed annually at a minimum to ensure that policies are meeting legal and regulatory obligations, best practices, and keeping up with technological change.

6. Are policy exemptions or exceptions allowed?

Exemptions to policies and related guidance are generally not allowed. If an exemption is necessary, then the requesting party must comply with the policy exception process. This process will be maintained and coordinated by the IIA IT Policy Lead.

7. What determines whether a policy is university-wide or unit-level?
   a) Should this guidance apply university-wide to all users of university information resources?
   b) Should this guidance apply university-wide to all IT providers?

These questions do not determine the category (policy, guideline, standard) but rather the scope for applicability.
8. Is this guidance specific to information technology? What other campus domains are involved and who should be included in policy drafting and decision-making?

Sometimes, the implementation of an IT service may trigger the need for a policy that relates to multiple domains (HR, Student, other), and it may or may not involve IT decisions. It is important to assess this situation with the appropriate stakeholders and determine who should be the primary “owner” of the policy. There may be cases where an HR or Communications Office policy, for example, should be implemented containing an IT standard or guideline. **Examples:** Preferred Name Policy  
Web Privacy Policy or Web Accessibility Policy
Appendix 3: IT Policy Decision Matrix

Overview
This document outlines the decision points to determine if a policy, standard, or guideline is required.

Prerequisites
If the answer to any of the following is “yes”, then continue with the questions to determine what kind of documented guidance may be necessary.
- Is there a legal requirement to have documented guidance?
- Are there operational issues that require clear statement of direction or policy?
- Is there new technology (such as cloud computing) that requires university-wide guidance?
- Will risks be mitigated by documenting (and implementing) this guidance?

<table>
<thead>
<tr>
<th>Criteria</th>
<th>If Yes</th>
<th>If No</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Is it implementable across the University?</td>
<td>Continue to #2</td>
<td>Create a Guideline</td>
</tr>
<tr>
<td>2. Is it compliant with existing policies or laws?</td>
<td>Continue to #3</td>
<td>Conduct further analysis with participation of appropriate stakeholders to determine how to handle</td>
</tr>
<tr>
<td>3. Is it applicable across the University?</td>
<td>Continue to #4</td>
<td>Skip to #9</td>
</tr>
<tr>
<td>4. Can it stand more than 1 year without review?</td>
<td>Continue to #5</td>
<td>Skip to #9</td>
</tr>
<tr>
<td>5. Would there be only a low number of exceptions?</td>
<td>Continue to #6</td>
<td>Skip to #9</td>
</tr>
<tr>
<td>6. Is it independent of a specific technology?</td>
<td>Continue to #7</td>
<td>Create a Standard ** or ** Create a high-level Policy and a Detailed technology-dependent Standard</td>
</tr>
<tr>
<td>7. Does an umbrella policy not exist?</td>
<td>Continue to #8</td>
<td>Use the umbrella Policy ** and ** Create detailed Standard(s), Guideline(s), or Procedure(s)</td>
</tr>
<tr>
<td>8. Can it be summarized in approximately one page?</td>
<td>Create a Policy *** and *** Detailed Standard(s), Guideline(s), or Procedures, if needed</td>
<td>Create a high level Policy ** and ** A combination of Standard(s) and/or Guideline(s)</td>
</tr>
<tr>
<td>9. Is it mandatory?</td>
<td>Create a Standard</td>
<td>Create a Guideline</td>
</tr>
</tbody>
</table>
Appendix 4: IT Policy Decision Flow Chart
Appendix 5: IT Policy Program Framework Models

1. Indiana University policy process for university-wide IT policies
   http://informationpolicy.iu.edu/policies/process.shtml

2. Policy development process issued by the Association of College and University Policy Administrators
   http://process.umn.edu/acupa/projects/process/default.cfm

3. University of Wisconsin-Madison IT Policy Process
   https://wiki.doit.wisc.edu/confluence/display/POLICY/IT+Policy+Process

4. The Ohio State University Policy Development Process
   http://www.osu.edu/policies/about.php