A. Definitions

1. Policies and Related Documents

These working definitions are used in IT policy at UW-Madison. They are intended to help people understand what is required, what is recommended, and how to interpret documents in practice. They are not formal definitions.

**Policies** are short stable statements of what people must or must not do.
- Policies are mandates.

**Guidelines** are recommendations, more changeable than policies.
- Guidelines are not mandatory, they are good advice.

**Procedures** document "how to" implementation details, changed as needed.
- They are mandatory if mandated by policy, otherwise they are recommended procedures.

**Principles** express intentions and values to guide future decision-making.
- They are written in general terms and are intended to be open to interpretation.

**Standards** are measurable criterion for consistency, used to review progress.
- They usually contain a mix of policies, guidelines, procedures, and principles.

**Best Practices** are a consensus among many different organizations based upon experience.
- They usually contain a mix of all the above.
2. IT Policy

UW-Madison Information Technology policy (IT Policy) encompasses UW-Madison policy and implementation plans that govern the efficient and effective development and use of IT resources to help meet the needs of UW-Madison research, instruction, and administration, in compliance with applicable laws, regulations, UW System policies and other external mandates.

The UW-Madison Information Technology Committee (ITC) defines the scope of IT Policy and implementation in consultation with the Vice Provost for Information Technology, IT Governance, and the other Offices, Schools, Colleges, and Divisions that publish UW-Madison policies.

The Policy Planning and Analysis Team (PAT) is a subcommittee of the ITC. The PAT assists the ITC and IT leadership on all matters related to IT policy.

3. IT-related Policy

In addition to policies specifically identified as UW-Madison IT Policy, many governance groups, Offices, Schools, Colleges, and Divisions develop and issue policy at UW-Madison. The Policy Planning and Analysis Team cooperates with them to help ensure consistency among all policies that include significant IT components or implications.

4. Policy Portfolios

IT policies, IT-related policies, and other related documents are organized into flexible policy portfolios. The portfolios help people understand how policies are related, and help the PAT and others manage policies in different subject matter areas. The portfolios currently include:

- Access Control
- Acquisition and Development
- Configuration and Maintenance
- Contingency Planning
- Copyright and Intellectual Property
- Digital Accessibility
- Education, Training and Awareness
- Electronic Records Management
- Monitoring and Mitigation
- Networking and Telecommunications
- Privacy
- Risk Management

B. Policy Statement

IT Policy will be developed at UW-Madison using the IT Policy Principles and Procedures described in this document.
C. Overview

1. Scope and Authority
IT policy development is a collaborative process that is integrated with UW-Madison shared governance and IT governance. IT policies are reviewed and approved by governance bodies that have institution-wide representation. The authority of shared governance and IT governance gives IT policies institution-wide scope and authority.

2. Purpose
IT Policy establishes expectations for UW-Madison IT resource users and providers. It helps meet internal university needs in compliance with applicable laws, regulations, UW System policies, and other external mandates. The overall purpose of IT Policy is to help reduce institutional risk and increase the effectiveness of IT in support of the mission of the institution.

3. Compliance Strategy
To help achieve compliance, IT policy is developed and implemented in a transparent and collaborative manner to ensure that policies are both necessary and practical. Compliance is proven in daily operations with periodic assessment, reporting, and risk informed management decisions.

4. Vice Provost for Information Technology
The Office of the CIO is the administrative home of IT policy. The Vice Provost for Information Technology (VP IT) provides leadership in IT policy, publishes the documents, and helps enable compliance.

5. Information Technology Committee
The Information Technology Committee (ITC) is the shared governance committee for policy and planning of IT throughout the University. All IT policies must be approved by the ITC.

6. IT Governance
IT Governance is a structure and process at UW-Madison to address Information Technology decision making—setting priorities, determining policy, setting and spending the budget, and evaluating effectiveness. IT Governance advisory groups review and endorse IT policies and policy-related documents such as guidelines and standards.

7. Policy Planning and Analysis Team
The Policy Planning and Analysis Team (PAT) is a subcommittee of the ITC. The PAT assists the VP IT, the ITC, and IT Governance in all matters related to IT Policy. The PAT Charter defines the mission, guiding principles, scope, roles and responsibilities, membership, and operations.
D. Cardinal Principles

The “Cardinal Principles” encourage compliance and are vital for the success of IT Policy development and implementation at UW-Madison.

1. Compelling Need – Motivates discussion and collaborative development.
2. Transparency – Enables discussion and collaborative development.
3. Collaboration – Surfaces requirements and encourages a willingness to comply.
4. Practical Implementation – Enables the knowledge and ability to comply.

The diagram illustrates how adhering to the cardinal principles helps UW-Madison develop IT policies that achieve wide-spread compliance. Non-adherence with the cardinal principles during development and deployment tends to result in non-compliance with the resulting policies and implementation.
Principle 1 – Compelling Need

There will be compelling need for IT policies and the individual requirements within those policies. Compelling need motivates collective activity. Without compelling need, participation and resource allocation are insufficient to produce effective policy. The principle of compelling need ensures that:

- policies are developed and implemented when reliance upon voluntary guidelines and procedures is insufficient.
- policies are not developed solely for completeness of policy coverage, unless complete coverage is required by institutional need or outside mandates.
- compelling need applies, not just to an entire policy, but to individual mandatory provisions of a policy. Provisions that lack a compelling need should not be mandatory.

What is compelling?

Compelling need is a shared perception. To test this: If the need is truly compelling, it should be possible to communicate and develop a broad perception of the importance and need.

Principle 2 – Transparency

The IT Policy Process and implementation will be transparent, so that all interested stakeholders can be aware of the current status and are able to provide input.

Published policies and documents are Public Data. Drafts and process documents are Internal Data and should widely available internally and easy to find. Meetings and agendas should be published ahead of time, and notes should be recorded and published in a timely manner.

Principle 3 – Collaboration

The IT Policy Process and implementation will be collaborative and will engage representative stakeholders to ensure that the policies are both necessary and practical. Effective collaboration incorporates input from many sources. Examples include:

- UW-Madison Strategic Plan
- IT Strategic Plan
- Shared governance
- IT Governance
- IT Policy Forums
- Policy Planning and Analysis Team
- Policy Stakeholder Teams
- Advisory Groups

Principle 4 – Practical Implementation

Implementation of policies will enable efficient and effective compliance. Without practical implementation, resource barriers will prevent compliance. Practical implementation ensures that:
any person or unit that makes a good faith effort to comply will be able to comply in an
efficient and effective manner.

• the policy and implementation plans will include exceptions or exception procedures to
cover reasonable cases where compliance is not efficient and effective.

• the principle of practical implementation applies, not only to an entire policy, but to
individual mandatory provisions of a policy. Provisions that lack a practical
implementation should not be mandatory.

What is practical?
Practical implementation is a shared perception. To test this: If the implementation is truly
practical, it should be possible to communicate and develop a broad perception of practicality.

E. Roles

1. The UW-Madison community
The whole UW-Madison community is affected by IT policies. The community is represented
throughout the policy development and implementation through participation in IT Policy
Forums, advisory groups, IT Governance, and the ITC, all of which draw members or
participants from the UW-Madison community.

2. UW-Madison leadership at all levels of the institution
Managers at all levels of the institution are accountable and responsible for compliance and
enforcement of IT policies in a manner identical to their normal management responsibility for
compliance and enforcement other types of policy or work rules that apply to the unit they
manage.

3. UW-Madison IT resource users and providers
Users and providers of UW-Madison IT resources are accountable and responsible for
compliance with IT policies that apply to them or to the resources they use or provide.

4. Information Technology Committee
The Information Technology Committee (ITC) is the shared governance committee for policy
and planning for Information Technology throughout the university. See the ITC charge for
more details. The ITC:

a. Reviews and approves IT policies and implementation plans. The ITC may consult with
the University Committee regarding review and approval.

b. Retains the option to review and approve other IT Policy-related documents such as
guidelines or standards.

c. Provides committee oversight of the Policy Planning and Analysis Team, which is a
subcommittee of the ITC.
5. IT Governance

IT Governance is a structure and process at UW-Madison to address Information Technology decision making—setting priorities, determining policy, setting and spending the budget, and evaluating effectiveness. IT Governance includes four advisory groups that represent different constituencies:

- The Divisional Technology Advisory Group (DTAG)
- The Infrastructure Technology Advisory Group (ITAG).
- The Research Technology Advisory Group (RTAG)
- The Teaching and Learning Technology Advisory Group (TLTAG)

The Information Technology Steering Committee (ITSC) is chaired by the VP IT and consists of the chairs of the technology advisory groups and other IT leaders. The ITSC is a decision-making body that advises the IT Governance Executive Board.

IT Governance reviews and endorses IT policies, implementation plans, and other IT Policy-related documents such as guidelines, and standards. To that end, IT Governance may employ cross-group subcommittees to efficiently address IT policies issues.

6. Advisory Groups

There are several subject matter-specific advisory groups. Some are subcommittees of IT Governance groups, while others are distinct from IT Governance. These groups review relevant IT policies, statements of principles, and IT Policy-related documents such as implementation plans, guidelines, and standards.

7. Vice Provost for Information Technology

Vice Provost for Information Technology (VP IT), or designee:

a. administers the IT Policy Program, provides staff support for the IT Policy Office, and provides administrative oversight of the Policy Planning and Analysis Team.

b. issues IT Policy in cooperation with the ITC which approves IT Policy. IT Policy is published and maintained by the IT Policy Office in a suitable policy repository.

8. Responsible Executives

Each IT Policy has one or more Responsible Executives (RE). For example, the Chief Information Security Officer (CISO) is a RE for Cybersecurity, and the Director of the Office of Compliance and ADA Coordinator is a RE for Digital Accessibility.

a. A RE has the lead during the IT policy development and implementation. This lead RE submits proposals and draft policies for review, endorsement, and approval.

b. One or more RE may administer resource allocations and projects involving institutional infrastructure and other support necessary to enable compliance with policy.
9. Policy Planning and Analysis Team

The Policy Planning and Analysis Team (PAT) is a subcommittee of the ITC. The PAT assists the ITC, IT Governance, and the VP IT on all matters related to IT Policy. The PAT:

- helps identify, organize, and prioritize IT Policy initiatives.
- helps estimate the impact of current and proposed IT policies.
- helps monitor, guide, and improve the IT Policy Process.
- helps publish, maintain, and communicate IT Policy.
- maintains the IT Policy Principles and Procedures, (this document).

F. Process

The IT Policies Principles and Procedures

To achieve compliance, IT policy is developed and implemented in a transparent and collaborative manner to ensure that policies are both necessary and practical. This creates a foundation for compliance.

The IT Policy Principles and Procedures, (this document,) detail a nine step IT Policy Process adapted from Cornell University.

The IT Principles and Procedures define a process that where policies are achievable and contribute to the environment of compliance:

- manages the entire policy life-cycle in a deliberate manner.
- ensures that only necessary policies are developed.
- is committed to transparency, collaboration, and practical implementation.
- aligns with institutional and divisional goals and needs.
- responsibly uses resources during the IT Policy Process.
- ensures that policies and related documents remain consistent.
- estimates policy impact and adapts requirements accordingly.
- ensures there is appropriate review, revision, and approval.
IT Policy Development Process

The process spans the full policy lifecycle including initial planning, development, and deployment, ongoing communications and compliance assessment, and periodic review and revision.

1. Plan

The VP IT’s Office, Responsible Executives (RE), Sponsors, and community representatives identify needs, prioritize, estimate impact, and initiate development.

2. Recommend

Representative stakeholders discuss the policy and implementation, refine the impact estimate, consult with advisory groups, and make recommendations to the Sponsors.

3. Propose

Guided by the recommendations, a small drafting team (DT) writes a proposal to develop a policy. The PAT analyzes the proposal. The RE submits it to the ITC.

4. Draft

Guided by the proposal, the DT drafts the policy and implementation and consults with stakeholders and advisory groups. The PAT analyzes the documents, and the RE submits them to IT Governance.

5. Endorse

IT Governance advisory groups review and endorse the policy and implementation. The DT incorporates changes.

6. Approve

The ITC approves the policy and implementation. The DT incorporates amendments.

7. Deploy

The VP IT issues the policy. The RE works with service providers and the community to deploy a practical implementation that enables efficient and effective compliance.

8. Comply

The RE, university management, and community leaders motivate and monitor compliance. Compliance is proven in daily operations with periodic assessment, reporting, and risk informed management decisions.

9. Review

Service providers and representative stakeholders are consulted during review. Revision repeats the earlier steps of the process in abbreviated form. The extent of abbreviation depends upon the impact of the revisions. Policies are retired when obsolete.
 Provisional Policies

The VP IT may issue provisional IT policies that are effective immediately. This is usually done as a result of an urgent situation that requires a document be issued before it is possible to fully approve it using the normal IT Policy Process.

An IT Policy is provisional until the ITC reviews and approves it. Until then, an expiration date is specified in the document. Provisional IT policies expire after that date, unless the ITC takes action to approve the policy, approve a revision of the policy, or extend the expiration date.

A provisional IT Policy is all other respects identical to any other IT Policy. Users and providers of IT resources are obligated to comply, and compliance may be enforced by management for any instances of non-compliance that occur during the period up to the expiration date.

Statements of principles, and other IT Policy-related documents such as implementation plans, guidelines, and standards may also be treated as provisional and given expiration dates. Any requirements, (i.e. mandates,) in such documents are treated exactly the same as a provisional policy.

G. Supporting Principles

1. Planning principles

IT policies will address issues that are important to the whole institution. When planning policy development it is necessary to ensure there is:

- compelling need, as described in cardinal principle 1.
- strategic alignment, as described in cardinal principle 3.
- appropriate scope, e.g. campus-wide rather than division-specific.
- executive sponsorship to assure alignment with leadership expectations.

2. Development principles

Voluntary compliance with policies is preferred. This is much easier to achieve if the community is involved throughout the development and implementation process. This requires:

- transparent process, as described in cardinal principle 2.
- inclusive representation, as described in cardinal principle 3.
- appropriate review, revision, and approval as described in cardinal principle 3.
- practical implementation as described in cardinal principle 4.

3. Resource management principles

The IT Policy Process will be both deliberate and timely. The fastest path to publishing a policy might not be the fastest path to achieving compliance with that policy.

Collaboration, transparency, and practical implementation take time. Rather than skip steps in the process, it is better to adjust the time and resources allocated to each step by considering:

- pre-existing consensus, which if higher may require less discussion.
- impact on the institution, which if higher or lower may require more or less discussion, research, and testing.
- complexity, which may require more or less discussion, research and testing.
- urgency of need, which may permit less time for discussion, research and testing.
Appendix A – References

IT Policy Office     policy@cio.wisc.edu
Published IT Policies  https://kb.wisc.edu/itpolicy/
Glossary     https://kb.wisc.edu/itpolicy/glossary
Wiki for IT Policy Development  https://wiki.doit.wisc.edu/confluence/display/POLICY/
RACI Chart and Swim Lane Diagram  
https://wiki.doit.wisc.edu/confluence/display/POLICY/IT+Policy+Process+RACI+Chart
IT Policy Process Roles and Deliverables  
https://wiki.doit.wisc.edu/confluence/display/POLICY/IT+Policy+Process+Roles+and+Deliverables

Appendix B - History

The IT Policy Process was created between 2003 and 2007. It has been in continual operation since then, incorporating incremental improvements along the way.

In 2015 the UW-Madison process was significantly enhanced by adopting leadership and governance elements of the policy process used at Cornell University. Cornell is a leader in higher education policy and is particularly strong in computer policy and law.

- 2003-2007, IT Policy Process was created by drawing upon practical experience in development and implementation of five different initiatives.
- 2007, original presentation of process at the first IT Policy Forum in August 2007.
- 2008, original Policy Planning Team refined the process.
- 2009, original version of the IT Policy Principles and Procedures.
- 2012, renumbered the steps of the process, (step 0 became step 1, etc.,) and improved the process diagram. No substantive changes in the principles, procedures, or process.
- 2015, adapted the Cornell policy process for use at UW-Madison. This was a substantive change to better engage University leaders when proposing and approving policy.
- 2016, updated the terminology and improved readability. No substantive changes in the principles, procedures, or process.
- 2018, major changes due to creation of IT Governance and re-chartering of the Policy Planning and Analysis Team to become a subcommittee of the ITC. Added definitions and a policy statement. (This document functions as the policy on IT policy development and must be approved by the ITC.) Substantially re-organized the roles. Expanded the description of provisional policies due to increased need to meet externally mandated deadlines, while remaining true to the collaborative approach to policy development. No substantive changes to the principles or process.
- 2019, added compliance strategy. Approved by the ITC.