What is IT Policy?

IT Policy establishes expectations of behaviors for users and providers of IT.

Areas of IT Policy:
- Cybersecurity
- Identity and Access Mgt.
- Information Networking
- Intellectual Property
- IT Accessibility
- IT Resource Management
- Records and Information Mgt.

Definitions:
- **Policies** are short stable statements of what people must or must not do.
- **Guidelines** are optional recommendations, more changeable than policies.
- **Procedures** document "how to" implementation details, changed as needed.
- **Standards** are measurable criterion for consistency, used to review progress.
- **Principles** express intentions and values to guide future decision-making.

The IT Policy Process emphasizes compelling need, transparency, and sufficient collaboration, practical implementation. (See reverse side.)

### Current Initiatives and Projects
- Continuous Diagnostics and Mitigation
- Credential Security Policy
- Cybersecurity Risk Management Policy
- Network Firewall Policy
- Web Accessibility

### Ongoing Initiatives
- Policy Forums
- Policy Knowledge Base
- Policy Planning & Analysis Team
- Web Accessibility Coordinating Group

### Completed Initiatives
- Restricted Data Management
- Revision of Information Incident Reporting Policy
- List of all initiatives…

### Program Development
- Thirty-five quarterly IT policy forums
- Principles and procedures for IT Policy
- Policy development Wiki
- Policy Glossary

### Websites
- [https://kb.wisc.edu/itpolicy/](https://kb.wisc.edu/itpolicy/)
- [https://wiki.doit.wisc.edu/confluence/display/POLICY/Home](https://wiki.doit.wisc.edu/confluence/display/POLICY/Home)

Published IT Policies
- IT Policy Development
IT Policy Process - Steps and Principles
September 12, 2017

Steps

The goal of the process is to ensure that there is compelling need, transparency, sufficient collaboration, and practical implementation.

1. Plan  The CIO’s Office, Responsible Executives(1), Sponsors, and community representatives prioritize and initiate policy development.

2. Recommend  Representative stakeholders consider possible development of policy and procedures, and make recommendations to the Sponsors.

3. Propose  Guided by the recommendations, the PAT analyzes and the Responsible Executives submit a proposal for development of policy to the ITSC(2) for approval.

4. Draft  Guided by the proposal, a small team drafts the policy and procedures in consultation with representative stakeholders. The PAT analyzes the draft.

5. Endorse  Advisory groups, IT governance groups, and the ITSC review and endorse the policy and procedures. Changes are incorporated by the drafting team.

6. Approve  The ITC(3) and UW-Madison decision-makers approve the policy and procedures. The drafting team incorporates amendments. It becomes UW-Madison policy.

7. Deploy  The Responsible Executives work with service providers and community representatives to enable efficient and effective compliance.

8. Comply  Responsible Executives, service providers, and community leaders motivate and monitor compliance.

9. Review  Community representatives and service providers are consulted during review and revision.

(1) Responsible Executives have the lead on a policy.
(2) Information Technology Steering Committee.
(3) Information Technology Committee.

Cardinal Principles

The goal of the cardinal principles is to create and maintain wide-spread compliance with IT policy. All other principles and practices of IT policy support or elaborate upon the cardinal principles.

1. Compelling need  The need for the policy and procedures is sufficiently compelling to motivate collaboration and practical implementation.

2. Transparency  The policy development process is sufficiently transparent to enable collaboration and practical implementation.

3. Collaboration  There is sufficient collaboration to produce a widely agreed upon policy and the requirements for a practical implementation.

4. Practical implementation  The deployed implementation of the policy and procedures is sufficiently practical to enable efficient and effective compliance.