Lecturer/Convenor:

Richard Boateng, PhD.

Email:
richard@pearlrichards.org

Office: UGBS RT18 (rooftop)
Class Website

• www.vivafrica.info
Objectives of the Session

• to ensure that students understand to develop, implement and maintain IT policy
• to enable students understand the basic framework to guide policy initiation, development, rollout, monitoring and retirement in organizations (eg. university institutions)
• to enable students understand decision models which can guide IT policy development
IT/IS Policy

• Policies are high level statements which ensure or guide compliance.
  – In relation to IS/IT strategy, policy may ensure compliance to the strategy
  – IS Security policy consists of high level statements relating to the protection of information and information producing resources across the business. It is critical that this is produced by or in consultation of top/senior management.
  – IT policies articulate the firm's vision, strategy, and principles as they relate to the use of information and information technology resources.

  University of Michigan - http://cio.umich.edu/policy/#development
IT/IS Policy and The Business

- IT/IS policy outlines roles and responsibilities, defines the scope of information needed by the organization, and provides a high level description of the controls that must be in place to facilitate the production and responsible usage of the information.

- For example, an IS security policy, “outlines security roles and responsibilities, defines the scope of information to be protected, and provides a high level description of the controls that must be in place to protect information. In addition, it should make references to the standards and guidelines that support it” (MindfulSecurity, 2009). An IT/IS policy is tends to demonstrate a commitment from senior management to produce, responsibly manage and protect information and information-related resources.

Standards, Guidelines and Procedures

• Standards consist of specific **low level mandatory controls** that help enforce and support the information systems policy.

• **Standards** help to ensure consistency and coordination in the design, development, implementation and usage of information systems across the business.

• For example, a password standard may set out rules for password complexity which will be applicable for all user login interfaces.

Standards, Guidelines and Procedures

- Guidelines consist of recommended, non-mandatory controls that help support standards or serve as a reference when no applicable standard is in place.

- Guidelines should be viewed as best practices that are not usually requirements, but are strongly recommended. They could consist of additional recommended controls that support a standard, or help fill in the gaps where no specific standard applies.

Standards, Guidelines and Procedures

• For example, a standard may require passwords to be 8 characters or more and a supporting guideline may state that it is best practice to also ensure the password expires after 30 days.

• In another example, a standard may require specific technical controls for accessing the internet securely and a separate guideline may outline the best practices for using the internet and managing your online presence.


Standards, Guidelines and Procedures

- **Procedures** are specific operational steps or manual methods that workers must follow to implement the goal of the written policies and standards.

- For example, a policy could describe the need for backups, for storage off-site, and for safeguarding the backup media.

- A standard could define the software to be used to perform backups and how to configure this software.

- A procedure could describe how to use the backup software, the timing for making backups, and other ways that humans interact with the backup system.


IT Policy Development and Administration Framework

**Guidelines to support IT Policy Development, Implementation and Maintenance:**
For example, to support the IT policy development process in Univ. of Michigan, a detailed framework was adopted. This is outlined as follows…
Framework for IT/IS Policy

Key Considerations

1. **Time:** Determines *when* to establish a policy, guideline or standard
2. **Criteria:** Determines the *criteria* for what should be in a policy, guideline or standards
3. **Method/Governance:** Creates a *collaborative methodology* for the drafting, approving, updating, and expiration of policies, standards, and guidelines
4. **Accessibility:** Documents and *publishes* policies, standards, and guidelines
5. **Action/Empower:** Serves as a *firm-wide* resource to consistently interpret and arbitrate policies
6. **Assurance/Evaluation:** *Measures* policy effectiveness and level of adoption
Outline of Framework

1. Authorization and Scope
2. Rationale
3. Principles
4. Roles and Responsibilities
5. IT Policy Governance and Approval
6. Stakeholder Involvement
7. IT Policy Structure and Criteria
8. Approach and Publication
9. IT Policy Life Cycle Process

Time
Criteria
Method/Governance
Accessibility
Action/Empower
Assurance/Evaluation
Authorization and Scope

Whose Responsibility for management of policy?
What is the Scope of the policy?

**UM**: The responsibility for IT policy management has been assigned to Information and Infrastructure Assurance (IIA). This includes:

1. Coordination of IT policy and underlying **development**, **dissemination**, and **education**.

2. **Review** and **analysis** of existing policies for **continued** applicability and effectiveness.

3. **Interpretation** of current policy related to specific issues, situations and incidents.

**Scope**: The IT policy framework covers all campuses. It applies to all users of U-M IT resources, including students, faculty, staff, and sponsored or guest users.

Rationale

What are the objectives of the policy?

IT 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 specifies:

1. **Structure and criteria** for what should be categorized as an IT policy, guideline, or standard;
2. A process for **initiating, reviewing, approving, and expiring** IT policies; and
3. **Ongoing roles and responsibilities** associated with IT policy development and maintenance.
Principles

What are guiding principles for development and maintenance of the policy?

The IT policy structure and process employ the following principles:

1. Initiation Criteria
2. Initiation Process
3. Action-Oriented Living Document
4. Decentralization and Centralization Development Approach
5. Interactive and Transparent Development Process
6. Flexibility with Focus on Functionality
7. Implementation and Interpretation
Principles

What are guiding principles for development and maintenance of the policy?

The IT policy structure and process employ the following principles:

1. **Initiation Criteria**: 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.

2. **Initiation Process**: 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.

3. **Action-Oriented Living Document**: 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.
Principles

What are guiding principles for development and maintenance of the policy?

4. **Decentralization and Centralization Development Approach:** 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.

5. **Interactive and Transparent Development Process:** 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**.
Principles

What are guiding principles for development and maintenance of the policy?

6. **Flexibility with Focus on Functionality**: 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.

7. **Implementation and Interpretation**: 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

Who will do what?

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 first level of governance approval.
Roles and Responsibilities

• **Chief Information Security Officer (CISO)/IIA Executive Director:** The CISO works with the IT Policy Manager and Lead to ensure alignment of the IT Policy program with strategic ITS and NextGen Michigan objectives and priorities. The Executive Director 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.
IT Policy Governance and Approval

How and Who governs the policy development and review?

The different levels of governance review and vetting of policies, standards and guidelines.

1. **CISO/IIA Executive Director**: Initial review of policies, guidelines, and standards

2. **IIA Council**: First level of governance review for IT policies, standards, and guidelines

3. **CIO**: Second level of governance review for IT policies; final approval of guidelines and standards before adoption and dissemination to campus

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

Who will be involved?

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.

Students, and student groups/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

How will they work together: policies, standards, guidelines and procedures?

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.

Example: 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.

Example: 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.

Example: 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

What are the procedures for dissemination?

IT policies will be documented and considered for approval as Standard Practice Guide (SPGs).

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.
IT Policy Life Cycle Process

What is the process for development and maintenance?

1. Identification, Planning and Initiation
2. Development, Review, and Approval
3. Rollout
4. Compliance, Review and Maintenance
5. Policy Retirement

Standards and guidelines may require fewer approvals than formal policies.
IT Policy Life Cycle Process

What is the process for development and maintenance?

Identification, Planning and Initiation

– Identify compelling need for new or updated policy/guidance.
– Determine whether the need should be satisfied by a policy, guideline, or standard – Use IT Policy Criteria Decision Tree (see class website)
– Identify sponsorship, stakeholders, working group members and their relevant roles
– Develop high level implementation impact analysis
– Obtain approval to proceed with draft policy (or guideline, standard)
– Prioritize and schedule policy work
IT Policy Life Cycle Process

What is the process for development and maintenance?

Development, Review, and Approval

- Draft initial policy (guideline, standard)
- Distribute to a small group of stakeholders for initial review and input
- Incorporate initial feedback
- Distribute to a larger group of stakeholders for review and input
- Post final draft on the IT policy website for general feedback
- Review and, where appropriate, incorporate feedback
- Present to appropriate governance entity for approval
- Obtain approval

IT Policy Life Cycle Process

What is the process for development and maintenance?

Rollout

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

Compliance, Review and Maintenance

– Monitor compliance and effectiveness of implemented guidance
– Review and implement modifications per annual review cycle (last revision and review dates shall be posted on each policy).
IT Policy Life Cycle Process

What is the process for development and maintenance?

Policy Retirement

- 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.

Standards and guidelines may require fewer approvals than formal policies.
Other Documents of Relevance

1. IT Policy Structure Definitions
2. Questions and Suggestions for IT Policy Planning Process
3. IT Policy Criteria Decision Tree
4. IT Policy Decision Matrix
5. IT Policy Decision Flow Chart
6. Samples from Other Universities
7. Sample Policy Background Template

See Class website