Lecturer/Convenor:

Richard Boateng, PhD.

Email:
richard@pearlrichards.org

Office: UGBS RT18 (rooftop)

IT Policy in Firms
Class Website

• www.vivaafrica.info
Objectives of the Session

• to ensure that students understand and differentiate between IT policy, standards and guidelines
• to enable students understand the basic types of IT policies required by organizations (eg. university institutions)
• to enable students understand the relationship between policy and strategy
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.**

IT/IS Policy and The Business

IS = IT + People + Processes + Business Policy/Structure

IS Policy = IT + People + Processes + Business Policy/Structure

IT Policy = Hardware + Software + Network Infrastructure
   (include users and relate to processes)

   a business mandate and must be driven by the top management

   IT policies interpret applicable laws and regulations and ensure that
   the policies are consistent with legal and contractual requirements in a
   firm, industry and the country. IT policies specify requirements and
   standards for the consistent use of IT resources across a firm.

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.


Standards, Guidelines and Procedures

- Policies are intended to last for up to five years, while standards are intended to last only a few years. Standards will need to be changed considerably more often than policies because the manual procedures, organizational structures, business processes, and information systems technologies mentioned in standards change so rapidly. For example, a network security standard might specify that all new or substantially modified systems must be in compliance with International Standards Organization (ISO) standard X.509, which involves authentication of a secure communications channel through public key cryptography. This standard is likely to be revised, expanded, or replaced in the next few years.


Web Policy

• Web policy is a set of high-level mandates for what must be done on the Web. Web policy is set by senior leadership and is created to protect the organization from risk. It holds the highest level of authority among standards and guidelines, and it sets the tone for related Web standards. Compliance with policy is required and enforceable. A policy for social media might include this kind of language:

• Any person posting information to a social media channel shall ensure that the information posted does not:
  – Conflict with our organization’s mission, objectives, and policies
  – Contain or link to libelous, defamatory, or harassing content, even by way of example or illustration

Web Standards

• Web standards are statements that define how the policy mandates will be accomplished. They are set by subject matter experts and are created to support quality execution. As a result, they are specific and detailed. Web standards are enforceable; complying with a standard is not optional. For example

Do not use your university .ug.edu.gh e-mail address to establish an account on a social media platform.

Guidelines

• Guidelines are considered best practices for what should be done on the Web. Guidelines are not mandates; complying with guidelines is optional.

  • Always pause and think before posting. If your comments give you pause, don’t post them.
Exploring key considerations for IT Policy

CASE STUDY

[University of Michigan Logo]
**Target User:** University of Michigan:

- The University of Michigan provides information technology resources to a large and varied group, including faculty, staff, students, and guests. **All members of this community are responsible** for using these resources in an effective, efficient, and ethical manner that does not interfere with the reasonable use by other community members or endanger the University's tax-exempt or legal status.

- In particular, University employees who deal with sensitive data are required to exercise due diligence with regard to privacy and security policies and practices.

- The information technology policies noted below apply to the **entire University of Michigan community and its guests.**

University of Michigan - http://cio.umich.edu/policy/#development
Drivers/Alignment: University of Michigan:

Several key drivers will help determine IT policy priorities. These include:

- **U-M environment:** Policies should align to core academic, research, learning and teaching, and administrative missions
- **NextGen Michigan:** Policies should support the reinvention of information technology at U-M and respond to emerging technologies
- **Legal and regulatory environment:** Policies should be in compliance with all statutory requirements
- **10 year-gap:** Policies need to be updated to properly account for the decade during which U-M has not had a comprehensive IT policy function
- **Risk environment:** Policies should satisfactorily account for an ever-changing array of environmental, technological, and operational risks
- **Best practices:** Policies should reflect industry and higher education best practices

University of Michigan - http://cio.umich.edu/policy/#development
Policy Oversight and Approval: University of Michigan

- The **Chief Information Officer** has oversight responsibility for IT policy. *Information and Infrastructure Assurance* (IIA), by delegation of the Chief Information Officer, coordinates the IT policy function for U-M, with responsibility for policy development, education, and maintenance; IIA maintains a complete repository of institutional IT policies, standards and guidelines.

- The **IT Policy Development and Administration Framework** specifies the process for drafting new—or revising old—IT policies. The **IT Council** and **University IT Executive Committee** have reviewed and approved the framework.
Policy Oversight and Approval: University of Michigan

• The U-M IT governance groups set campus-wide priorities for IT services, resources and facilities. Policies and standards and guidelines have different levels of final approval authority. Specifically:
  • The Chief Information Officer has final approval authority for IT guidelines and standards.
  • The IT Executive Committee has final approval authority for new or revised Standard Practice Guide policies.
  • Information and Infrastructure Assurance (IIA) is coordinating a campus-wide, systematic IT policy initiative.
Types of IT/IS Policy

General Policies
1. Proper Use
2. Privacy and Security
3. Data Management
4. Digital Copyright Compliance
5. Information Technology System Standards
6. IT Accessibility
7. Employees Rights and Responsibility

Emerging Policies (Technologies)
1. Web Policy
2. Social Media Policy
3. Mobile Usage Policy

1. IT Acceptable Use Policy
2. Bring Your Own Device

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

- General Information Technology Policies
- Student Information Technology Policies

http://goo.gl/sIUHe

University of Michigan - http://cio.umich.edu/policy/#development
General Information Technology Policies
University of Michigan

- **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.

- **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 and are mandatory.

- **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.

- **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.

University of Michigan - http://cio.umich.edu/policy/general-policies.php
General Information Technology Policies
University of Michigan

Proper Use

• These policies deal with protecting the rights of the community in regard to access to the information resource infrastructure, sharing of information, and security of intellectual products.

1. Proper Use of Information Resources, Information Technology, and Networks at the University of Michigan
2. Guidelines for Implementing the Proper Use Policy of the University of Michigan: Responsible Use of Technology Resources (R1103)
3. Policy and Guidelines Regarding Electronic Access to Potentially Offensive Material (SPG 601.16)
4. U-M Internet Publishing Policies, Guidelines, and Instructions
General Information Technology Policies
University of Michigan

Privacy and Security
These policies deal with protection of the information assets controlled by the University of Michigan.

1. Information Security Policy (SPG 601.27)
2. Information Security Incident Reporting Policy (SPG 601.25)
3. Social Security Number Privacy Policy (SPG 601.14)
4. Identity Misrepresentation (SPG 601.19)
5. Privacy and the Need to Monitor and Access Records (SPG 601.11)
6. Acquisition, Use and Disposition of Property (Exclusive of Real Property) (SPG 520.1)
7. Privacy and Retention of Security Logs Guidelines
8. Guidelines for eDiscovery at the University of Michigan
General Information Technology Policies
University of Michigan

Digital Copyright
This site deals with the University of Michigan's compliance with the digital copyright protection provisions of the Digital Millennium Copyright Act and the Higher Education Opportunity Act.

• Digital Copyright Compliance

These policies deal with use and distribution of copyrighted software programs.

• Management of Copyrighted Software (SPG 601.03-1)
• Ownership and Use of Computer Software (SPG 601.03-0)
Student Information Technology Policies
University of Michigan

These websites address IT policies and issues that apply specifically to students.

Statement of Student Rights and Responsibilities
• Student rights and standards of conduct

ResComp Conditions of Use
• Required agreement for use of the Residential Computing Network in University Housing

Digital Copyright Compliance
• Compliance with U.S. copyright laws and safe and lawful peer-to-peer file sharing

IT Accessibility
• University of Michigan's commitment to supporting those with accessibility needs

General Information Technology Policies
University of Michigan

Data Management

These **policies** deal with management and protection of the University of Michigan's institutional data resources.

- Institutional Data Resource Management Policy (SPG 601.12)
- Responsibility for Maintaining Information Technology Backup and Recovery Procedures (SPG 601.07-1)

This **Standard** sets expectations for compliance with respect to sensitive regulated data that fall under federal or state laws or regulations:

- Sensitive Regulated Data: Permitted and Restricted Uses

This **Guideline** sets expectations for fiduciary and stewardship responsibilities in the management of U-M information resources:

- University of Michigan Statement on Stewardship

University of Michigan - http://cio.umich.edu/policy/general-policies.php
Framework for IT/IS Policy

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

University of Michigan - http://cio.umich.edu/policy/#development
IT Policy Development and Administration Framework

Next Class