http://policies.iu.edu/policies/categories/information-it/it/IT-28.shtml

IT-28 Cyber Risk Mitigation Responsibilities

Draft revision 2 April 2013

Scope

This policy is applicable to Indiana University's (IU) academic and administrative subunits, auxiliary units, and any affiliated organizations (collectively referred to as "Units") on all campuses that make use of IU's information technology infrastructure.

Back to top

Policy Statement

1. University Information Technologies Services (UITS) is responsible for operating facilities that maximize physical security, provide reasonable protections from natural disasters, and minimize cyber security risks for IU data and systems.

   UITS is also responsible for provisioning an evolving set of information technology infrastructure and services that meet the common, evolving needs of all campuses and units. This may include contracting for services via cloud and off-site services providers that offer desirable and secure common services of value to the IU community.

2. All Units of Indiana University will deploy and use IT systems and services in ways that vigilantly mitigate cyber security risks, maximize physical security for IT systems, and minimize unacceptable risks to IT systems and data from natural disasters (collectively, "Cyber Risks").

   a. The *primary* means of reducing and mitigating Cyber Risks at IU is for units to use the secure facilities, common information technology infrastructure, and services provided by UITS *to the greatest extent practicable* for achieving their work.

   b. To the extent that the primary means of Cyber Risk mitigation is not practicable for achieving a unit's work, the *secondary* means is for Group-level and Unit-level IT providers to formally document their role, responsibilities, and ongoing vigilance to mitigate Cyber Risks to IU.

Back to top

Reason for Policy

Cyber Risks to the University are Increasing

By 2013, it is clear that Indiana University faces a rising array of Cyber Risks from an increasingly connected world. Cyber security incidents and documented threats demonstrate a growing technical sophistication and acceleration that have substantially raised the risk profile to essential IU information and technology systems. These risks are particularly significant since cyber attacks are increasingly coming from organized criminal enterprises, corporate businesses, or branches of foreign governments. Escalation of these risks seems likely as networks connect more types of devices that make more desirable targets for malicious activities.

This rise in cyber security risks joins the well-known risks of physical security for systems (protection from theft or misuse), natural disasters, and even building failures (e.g., broken water pipe). Losses of irreplaceable data from these risks or long system recovery times could have highly detrimental consequences to the work of IU.

Every additional physical computing device – particularly servers that are a primary target for cyber attacks – increases Cyber Risk as it adds a potential target and is another device that must be physically secured, powered, cooled, maintained, patched, and monitored for malicious activity. A compromised server in one unit may be used for malicious activity inside the IU network in ways that disrupt the work of other units. Compromised devices can be used as part of maliciously controlled "bot" networks that are used to attack other systems within and beyond IU. Thus, reducing the number of physical computing devices while still achieving unit goals is one important approach for mitigating IU's collective Cyber Risks.

The goal of this policy is to ensure that the IU community minimizes to the greatest extent practicable the *unnecessary* creation of Cyber Risks while also enabling the productive work of all units. This requires a balanced approach to activities that (a) create Cyber Risks and (b) activities that can help mitigate them. Both enabling and mitigating are essential for the diverse IT services required for the university's research, education, and service mission. The policy creates a framework and procedures to formally review and document units' Cyber Risk mitigation approaches and responsibilities.

Means to Reduce Cyber Risks

Indiana University has made substantial institutional investments in secure physical facilities (IU Data Centers), IT infrastructure, IT services, and professional staff with expertise in cyber security to support the university's common IT needs. Use of these investments is the primary means to reduce Cyber Risks by having fewer physical devices as targets and fewer devices in less secure facilities.

Thus, whenever practicable, establishing *physical* security for servers in a highly secure, 24 x 7 monitored, protected facility is an essential first step for risk mitigation. Servers that operate outside of IU's secure data centers increase reputational, financial, and data loss risks for the University and may also contribute to other risks/concerns for IU:

1. Increases risk of permanent data loss from natural causes, building failures (e.g., leak in pipes or cooling outage), or malicious acts if data that are stored outside the Data Centers are not backed up to a remote and highly secure data storage facility. (The IUB Data Center is the only IT facility within IU designed to withstand a category 5 tornado).
2. Introduces avoidable risks of disruption of critical functions due to potential inadequate system maintenance, redundancy planning, and/or disaster recovery planning.
3. Uses increasingly scarce resources to duplicate core services offered by UITS, many of which are offered in a highly automated fashion with full-time IT experts with formal security training; local resources may be better spent on units' needs that require human attention and local expertise.
4. Increases the University's use of energy and carbon footprint as the use of virtualized servers and aggregation of power/cooling in the data centers make them the most energy efficient facilities for housing IT systems on campus.

The policy also recognizes that unique needs for some faculty-led research and teaching (academic uses) or unique administrative uses may not be practicable within the common IT infrastructure and services provisioned by UITS. The use of Group-level and Unit-level IT providers is a secondary means to achieve the goal of this policy.

The policy creates a framework to further IU's organizational partnerships for vigilant efforts to manage and mitigate Cyber Risks for the entire University. It ensures that IU's collective risks for information technology are understood, mitigated, and managed. When fully implemented, this policy will ensure that

appropriate leaders within the University have reviewed and approved the balance of Cyber Risk creation and mitigation for every unit of IU.

Back to top

Procedures

University Information Technology Services:

UITS is responsible for maintaining secure facilities; provisioning high-quality, secure, and reliable information technology infrastructure; and providing common services with ample capacity and commensurate technical and user support. In particular UITS will:

1. Continue its funding philosophy that minimizes to the greatest extent practicable specific chargeback for IT systems and services to organizational units. Where it is necessary to pass specific costs to an organizational unit, the rates will reflect the lessor of (a) the actual, scaled cost for the provided service or (b) the full cost of a highly comparable service in the marketplace.
2. Provide technical expertise when necessary, and physical access to secure facilities for appropriate group-level and unit staff to access their systems.
3. Continually and broadly engage with organizational units through a variety of means (meetings of representative staff, university / campus / school-level faculty committees, users, administrators, interviews, surveys, etc.) to ensure the timely evolution of facilities, systems, and services so that the University's IT assets are protected by a university-wide and well-informed partnership of that community.
4. Provide assistance to units for analyzing their internal information technology environment and needs relative to current and planned common services capabilities.
5. Provide assistance to units that wish to increase use of UITS services, and wish to increase the security of Group-Level IT services.

Administrative Uses and Auxiliary Units:

Within two years of the adoption of this policy, all IU administrative and auxiliary units and other such organizations that depend upon the IU information technology environment will perform an initial, comprehensive evaluation of their information technology needs relative to the requirements of this policy. Following that review, organizational units will:

1. Determine what unit-level information technology systems and services are candidates for use of UITS or group-level information technology provider(s).
2. Develop a plan for policy compliance with target dates agreed to by the unit head or delegate.
3. Prepare a formal risk assessment and risk mitigation plan to be discussed and approved jointly by the unit head (e.g., Dean of a school, Vice President, Director, etc.) and the Chief Information Officer & Vice President for IT. Establish and maintain appropriate capacity and expertise for risk mitigation, IU policy compliance, and quality management of IT services that remain in an organizational unit.

Academic Uses:

IU Academic uses of systems, software, and services for research and education merit especially broad faculty discretion in how to best achieve these critical parts of the university's mission. In support of this discretion, heads of academic units may formally choose to take responsibility for broad categories of academic uses by providing sufficient resources for group- or unit-level Cyber Risk mitigation vigilance.

Within two years of the adoption of this policy, all IU academic units and other such organizations that depend upon the IU information technology environment will perform an initial, comprehensive evaluation of their information technology needs relative to the requirements of this policy. Following that review, organizational units will:

1. Identify any office-level, lab-level, or group-level information technology systems and services within an academic unit for teaching, research, and service could be served by UITS services and those that are not practicable for use of UITS services.
2. Determine what unit-level information technology systems and services are candidates for migration to UITS or group-level information technology provider(s).
3. Develop a plan for policy compliance with target dates agreed to by the unit head or delegate.
4. Prepare a formal risk assessment and risk mitigation plan to be discussed and approved jointly by the unit head (e.g., Dean of a School, Vice Chancellor / Provost / President for Research, etc.) and the Chief Information Officer &/ Vice President for IT. Establish and maintain appropriate capacity and expertise for risk mitigation, IU policy compliance, and quality management of IT services that remain in an organizational unit.

Review Updates:

The ongoing nature of IT services is such that new opportunities will continually arise and sometimes on short notice. It is expected that organizational units and UITS will proceed in a spirit of full partnership to taking advantage of these opportunities within approaches that comply with IU policies, the spirit of IT-28, and vigilant Cyber Risk mitigation efforts. Formal reviews will be updated every two years.

Back to top

Definitions

Cyber Risks: Collective label for IT security risks, physical system security risks, and risks arising from natural disasters or potential infrastructure failure (broken water pipes, cooling failures, etc.).

Services Unique to a Specific Organizational Unit or Across a Group of Units: those services that are highly specific to the academic, administrative, or research operations of a unit or a small set of units. Examples include computers connected to scientific, lab, and medical devices.

Secure Facilities: UITS IU Bloomington Data Center and the IUPUI Advanced Cyberinfrastructure Facility (Informatics and Communications Technology Complex).

Information Technology Infrastructure and Common Services: Common infrastructure components, including, but not limited to, core and inter-campus networks, commodity Internet connections, Domain Name System (DNS), central authentication, Dynamic Host Configuration Protocol (DHCP), phone switches, etc.; or core technology-based services required by a significant portion of IU organizational units, whether provided directly by UITS or contracted (electronic mail, web page delivery, etc.).

Group-level Information Technology Provider: An IT function that provides support to a group of departments or other units that have similar and unique IT needs. Examples are an IT support function that supports all of the academic departments and administrative functions within a school, or across a single vice-president's set of responsibilities. The capacity of the IT support unit, resources, and expertise of the staff within it must be adequate to effectively manage the information technology systems and services.

Unit-level Information Technology Provider: An IT function that provides support to a department, lab(s), or other units that have similar and unique IT needs. Examples are an IT support function for a set of labs

or a research center. The capacity of the IT support unit, resources, and expertise of the staff within it must be adequate to effectively manage the information technology systems and services.

Back to top

Sanctions

Failure to comply with IU information technology policies may result in sanctions relating to the individual's use of information technology resources or other appropriate sanctions via IU personnel and student policies.