University of Nebraska
LINCOLN | OMAHA | KEARNEY | MEDICAL CENTER

Effective: 12/31/17
Last Revised: 8/28/17

Responsible University Administrator:
Vice Chancellor for Information Services & CIO

Responsible University Office:
Information Technology Services

Policy Contact:
Chief Information Security Officer,
security@nebraska.edu

ITS-03 IT Risk Management Policy

Scope

This policy is applicable to all University of Nebraska academic and administrative sub-units, auxiliary units, and any affiliated organizations (collectively referred to as "Units") on all campuses that make use of any of the University's Information Technology (IT) infrastructure, systems or services.

Policy Statement

Reliable and secure technology is a critical necessity for the tripartite research, teaching and outreach mission of the University. All University data will be secured by ITS in a University Data Center, or the Unit will be required to provide a comprehensive review of their IT security.

ITS is responsible for delivering agile, scalable, and trusted technology services that meet the common, evolving needs of all campuses and units. This may include providing advice, contracting for commodity services via off-site providers, customized local services to meet specific academic and business needs or any number of additional services. Collaboration with University Procurement Services in the negotiation and contracting of services, whether they are to be hosted in the cloud, placed in one of our data centers or located off-site at a service provider's location is required to ensure the University will obtain the lowest price possible and adhere to all security considerations.

In order for IT services to be reliable, secure, and scalable for the needs of the entire University system; ITS is responsible for operating IT facilities that maximize physical security, provide reasoned protections from natural disasters, and minimize IT security risks for NU data and systems.

All Units of the University will deploy and use IT systems and services in a manner that vigilantly identifies and mitigates IT security risks, maximizes physical security for IT systems, and minimizes unacceptable risks to IT systems and data from natural disasters (collectively, "IT Risk").

A. The primary means of reducing and mitigating IT Risk at the University is for units to use the secure facilities, common IT infrastructure, and services managed by ITS to the greatest extent practicable for achieving their work.

B. To the extent that the primary means of IT Risk mitigation is not practicable for achieving a unit's work, the secondary means is for distributed IT providers to formally document, and obtain approval from ITS, the unit's role, responsibilities, and ongoing actions to mitigate IT Risk for the University.

Reason for Policy

The lifecycle of a university; admissions, registration, student life, teaching and learning, and business efficiency across the institution is dependent upon technology. As the university uses more data to inform decision-making and produces increasingly valuable data as part of our research mission, the vulnerability of our data increases. Downtime of any system, whatever the IT Risk that caused it, has a significant impact on the business of the University.

Meanwhile, the sophistication and frequency of attacks against IT systems and data continue to grow. The University handles tens of millions of cyber-attacks against our IT resources every day. The increasing number of IT security

incidents and documented threats create a concerning picture of a very sophisticated and persistent array of attacks against higher education. Adding to the sophistication and persistence, many attacks have been identified as coming from nation states, organized crime, and even corporate businesses. For both 2016 and 2017, the industry group for IT in higher education, Educause, has identified IT security as the most important issue that member institutions must address.

IT Risk has traditionally focused on servers and endpoint devices like desktop and laptop computers. Each of these devices represents a target for IT attacks and a liability for loss or damage of both the device and the data it has access to. These devices must be physically secured, powered, cooled, maintained, patched, and monitored for malicious activity. At any scale, service owners have key responsibility in understanding and properly identifying IT Risk so that adequate mitigations can be put in place. This is especially true in the case of data being consumed, created, or shared via that service.

The goal of this policy is to ensure that the University community minimizes, to the greatest extent practicable, the unnecessary creation of IT Risk while also enabling the productive work of all units. This requires a balanced approach to activities that (a) create IT Risk and (b) activities that help mitigate IT Risk to support the university's research, education, and outreach mission. The policy creates a framework and procedures to formally review and document units' IT Risk mitigation approaches and responsibilities.

Means to Reduce IT Risk:
The University continues to make substantial institutional investments in secure physical facilities, IT infrastructure, IT services, and professional staff with expertise in IT security and management to support the university's common IT needs. Use of these investments is the primary means to reduce IT Risk by having fewer physical devices as targets, fewer devices in less secure facilities, and more comprehensive and consistent practices to manage IT risk across the institution.

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 the University's secure data centers increase reputational, financial, and data loss risks for the University and may contribute to other risks/concerns for the University:

A. Increases risk of permanent data loss from natural causes, building failures (e.g., leaking pipes or cooling outages), 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. (University Data Centers provide protection from all of these risks).

B. Introduces avoidable risks of disruption of critical functions due to potential inadequate system maintenance, redundancy planning, and/or disaster recovery/business continuity planning.

C. Uses increasingly scarce resources to duplicate core services offered by ITS, many of which are offered in a highly automated fashion with full-time IT experts with formal security training; local resources can be redirected to supporting units' specific needs that require human attention and local expertise.

D. 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.

Exceptions:
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 ITS. The use of distributed IT providers is a means to achieve the goal of this policy and must follow the secondary means specifications including providing documentation of risk mitigation, responsibilities, prior to obtaining ITS approval. ITS reserves the right to monitor exceptions for adherence to mitigation factors and responsibilities..

The policy creates a framework to further the University's organizational partnerships for vigilant efforts to identify, manage and mitigate IT Risk for the entire University. It ensures that our collective risks for IT are understood, mitigated, managed and communicated. When fully implemented, this policy will ensure that the balance between IT Risk mitigation and residual risk to the University will be reviewed and approved by the appropriate unit leadership.

Procedures

A. *Information Technology Services:*
ITS is responsible for maintaining secure facilities; provisioning high-quality, secure, and reliable IT infrastructure; and providing common services with ample capacity and commensurate technical and user support. In particular ITS 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 lesser 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 advanced technical expertise, and physical access to secure facilities for approved distributed IT staff to access and manage their systems.
3. Actively engage with organizational units (through meetings, committees, surveys) to ensure the timely evolution of facilities, systems and services so that the University's IT assets continue to be protected by and responsive to a well-informed partnership of the university community.
4. Assist units for analyzing their local IT environment and identifying needs relative to current and future common service capabilities.
5. Assist units that wish to increase use of ITS services (moving physical devices to Data Centers, migrating services to virtual or cloud environments, etc.), and wish to increase the security of distributed IT services.
6. Assist units with their IT Risk Assessment process.

B. *Administrative/Academic Users and Auxiliary Units:*

Within one year of the adoption of this policy, all University Units and other such organizations that depend upon the University IT environment will perform an initial, comprehensive evaluation of their IT needs relative to the requirements of this policy. Following that review, organizational units will:

1. Determine what distributed IT systems and services are candidates for use of ITS services.
2. Develop a plan for policy compliance with target dates agreed to by the dean or director.
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 (CIO). Units will be required to establish and maintain appropriate capacity and expertise for risk mitigation, University policy compliance, and quality management of IT services that remain within an organizational unit.

C. Academic Uses:
Academic uses of University 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 distributed IT Risk mitigation vigilance.

Within one year of the adoption of this policy, all University academic units and other such organizations that depend upon the University IT environment will perform an initial, comprehensive evaluation of their IT needs relative to the requirements of this policy. Following that review, organizational units will:

1. Identify any unit level IT systems and services within an academic unit for teaching, research, and service that could be served by ITS services and those that are not practicable for use of ITS services.
2. Determine what distributed IT systems and services are candidates for migration to ITS or shared IT provider(s).
3. Develop an action plan for policy compliance with target dates agreed to by the dean or director.
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 / Vice Chancellor for Research, etc.) and the CIO. Units will be required to establish and maintain appropriate capacity and expertise for risk mitigation, University policy compliance, and quality management of IT services that remain in an organizational unit.

D. *Review Updates:*
The ongoing nature of IT services is such that new opportunities will continually arise and sometimes with short notice. It is expected that organizational units and ITS will proceed in a spirit of full partnership in taking advantage of these opportunities within approaches that comply with University policies, the spirit of IT-03, and vigilant IT Risk mitigation efforts. Organizational units are required to update the reviews of their IT needs every two years.

Definitions

A. *IT Risk*:
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.).

B. *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.

C. *Secure Facilities:*

University Data Centers located on the UNK, UNL, UNMC, and UNO campuses.

D. *IT Infrastructure and Common Services:*
Basic infrastructure components that will include core campus and inter-campus networks, connections to commodity Internet, Domain Name System (DNS), central Identity and Access Management services including Active Directory (AD), Lightweight Directory Access Protocol (LDAP), Shibboleth, Central Authentication Service (CAS) Single Sign On (SSO), Dynamic Host Configuration Protocol (DHCP), or any core technology-based services that are required by a significantly portion of University campuses and organizational units, whether provided directly by ITS or contracted for (Office 365, Canvas, Box, etc.).

E. *Distributed IT Provider:*

An IT function that provides support to a department, 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, a set of labs, a research center, administrative functions within a college, 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 IT systems and services.

Sanctions

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

Units which do not comply with the requirements to complete a comprehensive evaluation and the development of an action plan may be denied access to University IT resources.

Additional Contacts

Subject	Contact	Phone	Email

Responsible Parties

The CISO's are responsible for monitoring and enforcing this policy.

Forms

Application for a Secure Computing Zone (link)

Related Information

History

This is the original policy adopted regarding IT Risk

0.1 Created by Rick Haugerud