University of Nebraska

LINCOLN | OMAHA | KEARNEY | MEDICAL CENTER

Effective: 12/31/20
Last Revised: 6/4/19

Responsible University Administrator:
Vice President for Information Services & CIO

Responsible University Office:
Information Technology Services

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

IT Risk Mitigation Policy (ITS-03)

1. Scope

1.1. This policy is applicable to all University of Nebraska (University) 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 Institutional Data, Information Technology (IT) infrastructure, systems or services.

2. Policy Statement

2.1. Reliable and secure technology is a requirement for the tripartite research, teaching and outreach mission of the University. Security and reliability of technology depend on an ongoing program to minimize unacceptable risks to IT systems and data from intentional, accidental, natural, legal, and reputational risk (collectively "IT Risk"). For a service to be considered reliable, it must be consistently available and usable by the entirety of its intended audience.

2.2. The University Information Technology Services (ITS) organization is established as the University's default organization responsible for provisioning and managing an evolving portfolio of reliable and secure technology and IT resources that minimize IT Risk and meets the needs of all campuses and Units.

2.2.1. The University has adopted the NIST family of information security controls (800-53, 800-171, CSF) to address stakeholder needs and current threats to the university's operations, assets, individuals, and partner organizations. ITS is responsible for conducting ongoing risk analysis and management.

2.2.1.1. Risk analysis: provides the basis for deciding what to do about risks that have been identified, or risk treatment. Risk treatments include risk mitigation, risk assignment (or transference), risk avoidance, and risk acceptance.

2.2.1.2. Risk management: consists of three main elements: threat identification, risk analysis and risk treatment.

2.2.2. ITS will collaborate with University Procurement Services in the negotiation and contracting of services. The IT services span a range of cloud, local, or off-site locations to ensure the University will obtain the lowest price possible and adhere to all security considerations.

2.3. All Units will deploy and use IT systems and services in ways that vigilantly mitigate IT Risk and meet the University's requirement for reliable and secure data.

2.3.1. Primary Means: the Primary Means of reducing and mitigating IT Risk at the University is for Units to use the portfolio of reliable and secure technology provided by ITS to the greatest extent practicable for achieving their work.

2.3.2. Secondary Means: 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 Unit-level IT providers to collaborate with the ITS Information Security Office to provide a comprehensive and regular review of their IT security.

3. Reason for Policy

3.1. 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.
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.

3.2. 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, contract terms, and management to support the university's common IT needs both on premise and from hosted services. 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 contract language and practices to manage IT risk across the institution.
Thus, whenever practicable, establishing physical and/or contractual 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 or preferred contract terms and conditions increase IT Risk for the University and may contribute to other risks/concerns for the University:

3.2.1. 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 or contract terms and conditions provide protection from these risks).

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

3.2.3. 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.

3.2.4. 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.

3.3. Exceptions:
The policy recognizes that some faculty-led research and teaching (academic uses) or unique administrative uses have unique needs that may not be practicable within the common IT infrastructure and services provisioned by ITS. To meet the goal of this policy, provision of these Unique Services should follow the Secondary Means (2.3.2) specifications; including providing documentation of risk mitigation and responsibilities prior to obtaining ITS approval. ITS reserves the right to monitor exceptions for adherence to mitigation factors and responsibilities.

3.4. 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.

4. Procedures

4.1. Information Technology Services:
ITS is the primary organization 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:

4.1.1. Continue its funding philosophy that minimizes to the greatest extent practicable specific chargeback for IT systems and services to Units. Where it is necessary to pass specific costs to an 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.

4.1.2. Provide advanced technical expertise, advice from legal counsel, procurement support, and physical access to secure facilities for approved Distributed IT staff to access and manage their systems.

4.1.3. Actively engage with 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.

4.1.4. Assist Units for analyzing their local IT environment and identifying needs relative to current and future common service capabilities.

4.1.5. 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.

4.1.6. Assist Units with their IT Risk Assessment process. The University of Nebraska maintains a system-wide IT Risk Assessment process. The process includes an information gathering questionnaire covering a variety of technology risk areas. The process is based upon NIST 800-53, NIST 800-171, and NIST CSF. Upon completion of the questionnaire, an ITS Security Team member will review results, evaluate and assign risk ratings, inventory control gaps and create and monitor action plans for mitigation.

4.2. 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, Units will:

4.2.1. 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 Unique Services that are not practicable for use of ITS services.

4.2.2. Develop a plan for policy compliance with target dates agreed to by the dean or director.

4.2.3. 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 Unit whether hosted on-premise or as a service.

4.3. 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 Management vigilance.

4.4. 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 ITS-03, and vigilant IT Risk Management efforts. Units are required to update the reviews of their IT needs every two years.

5. Definitions

5.1. IT Risk:
Collective label for IT security risks, physical system security risks, risk to the University's reputation (ability to conduct business or research as a trusted partner), risk of University legal liability, and risks arising from natural disasters or potential infrastructure failure (broken water pipes, cooling failures, etc.).

5.2. Unique Service:
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.

5.3. Secure Facilities:
University Data Centers located on the UNK, UNL, UNMC, and UNO campuses.

5.4. 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 Units, whether provided directly by ITS or contracted for (Office 365, Canvas, Box, etc.).

5.5. Distributed IT:
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.

6. Sanctions

6.1. 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.

6.2. 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.

8. Responsible Parties

8.1. The AVP of Information Security and the CISO are responsible for monitoring and enforcing this policy.

9. Forms

9.1. Application for a Secure Computing Zone (link)

10. Related Information

10.1. NIST 800-53 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

10.2. NIST 800-171 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf

10.3. NIST CSF https://www.nist.gov/cyberframework

11. History

1. created by Rick Haugerud
2. edited by Matt Morton
3. edited by Andrea Childress
4. edited by Paul Erickson