University of Nebraska
LINCOLN | OMAHA | KEARNEY | MEDICAL CENTER

Effective: *October 2, 2017*
Last Revised: *October 2, 2017*

Responsible University Administrator:
Vice President of Information Technology

Responsible University Office:
Information Technology Services

Policy Contact:
Chief Information Security Officer

Establishing Information Security Policies
IT-01

POLICY CONTENTS

I. Scope

This policy applies to any Information Security policy to be adopted at the University of Nebraska (University).

II. Policy Statement

The University formally approves information security policies through an established process, publishes those policies in a consistent format, and maintains official University policies in a central, readily accessible policy website. That website is available at https://nebraska.edu/bylaws-and-policies. Responsible administrators (as defined below) and their offices must comply with the procedures in this policy for drafting, approving, revising, distributing, maintaining, and withdrawal of information security policies.

III. Reason for Policy

The University establishes information security policies to protect information technology resources, research data, and the information of vendors, customers, alumni, faculty, staff and students; promote consistency, efficiency, and effectiveness; and mitigate or manage significant institutional risk.

University information security policies must be thoroughly reviewed, maintained, and made available to the campus community to promote compliance and accountability. The present policy provides for a consistent, transparent, and inclusive development process; an identified authority for approving policies; a mechanism for regular review of policy needs, compliance, and effectiveness; a consistent policy format; and an accessible electronic policy library.

IV. Procedures

A. DEVELOPMENT & APPROVAL PROCESS

1. Identification of Need and Development of Draft Policy

University information security policies should be based on a determination that policy requirements are necessary to protect University information technology resources and data; promote consistency, efficiency, and effectiveness; mitigate or manage significant institutional risk; or assure compliance with federal or state laws, rules, or regulations. A

responsible unit that identifies the need for an information security policy must draft the policy using the standard template. The University aligns its IT security program to the NIST 800-53 security framework. Questions or requests on policies can be sent to the University Executive Information Security Council (UEISC) via email at infosecuritycouncil@nebraska.edu.

2. Review & Comment Period

The UEISC will review all draft policies and provide suggestions concerning language, level of detail, readability, and potential impacts on other information security policies or practices (within 14 days of receipt of the draft). The responsible office, with guidance from the UEISC, consults stakeholders, University leadership, and others as needed to seek feedback. After receiving input and feedback, the responsible unit will update the policy draft as needed. Unless circumstances necessitate an expedited process (see below), the policy draft must be posted on the information security policy website for a minimum of 30 days to provide a review and comment period. Any comments received will be forwarded to the responsible office.

3. Final Approval

Following the review and feedback period, the legal representative on the UEISC will facilitate review by the Office of the Vice President and General Counsel (OVPGC). The OVPGC shall review the draft within 30 days of receipt. After any revisions are addressed, and the draft is approved by the OVPGC the Chair of the UEISC will forward to the President for final approval. Once approved, the policy will be posted on the University Information Security Policy website as "approved".

4. Distribution & Maintenance

The Responsible Administrator shall communicate and distribute the approved policy broadly to the University community and key stakeholders. The Responsible Office should monitor compliance, measure effectiveness of policy, and evaluate feedback. Policies should be reviewed by the responsible office no less often than every three years from the effective date or the last update or review, to ensure that the information in the policy remains accurate and that the policy is still necessary and effective in its current form. Revisions that affect the substance or scope of the policy should follow the policy development and approval process; however, minor non-substantive revisions and changes in contacts, forms, or related information may be made by the responsible office and posted without review. Notification to the University community and key stakeholders about minor non-substantive revisions should still be made. If a policy needs to be withdrawn, that information should follow the policy development and approval process along with any replacement policy. Review, revision, and withdrawal actions should be noted in the history section of the policy. Versions of policies that are revised or withdrawn will be archived.

B. INTERIM/EXPEDITED POLICIES

Responsible offices may forego the review period and approve an interim information security policy via an expedited process when necessary. Special situations where this is likely may include a change in federal or state law, a significant and immediate financial opportunity, or a major institutional risk. Interim information security policies must utilize the standard template, require the approval of a unit director, and will remain in force for up to one year from the date of issuance. Interim information security policies will be communicated and distributed to the University community and key stakeholders using the same process identified in number 3 above. The removal of the interim designation will occur after the policy completes the Development and Approval Process.

C. RELATIONSHIP OF UNIVERSITY INFORMATION SECURITY POLICIES TO SYSTEM-WIDE POLICIES OR BYLAWS

University information security policies must be compliant with any University Board of Regents policy, Board of Regents Bylaw, Executive Memoranda, or any other University system-wide policy. In the event of a conflict between a University Information Security Policy and a University system-wide policy, the system-wide policy will prevail.

D. COMPLIANCE

University faculty, staff and students are responsible for knowing, understanding, and complying with information security policies that relate to their position, employment or enrollment at the University.

V. Definitions

University Information Security Policy – A guiding or governing set of rules or principles, formally approved, to protect University information technology resources and institutional data.

Unit Director – The term Unit Director refers to the senior most leaders in the University's administrative offices. Those offices are identified as Academic Affairs, Business and Finance, Diversity and Equity, General Counsel, Information Technology Services and University Affairs.

University Executive Information Security Council (UEISC) – The UEISC is a standing committee of representatives from the University of Nebraska at Kearney, the University of Nebraska-Lincoln, the University of Nebraska Medical Center, the University of Nebraska at Omaha, and the University of Nebraska Central Administration. For the purposes of this policy, the Executive Council will serve as a resource to consult with University offices on proposed and draft information security policies to consider whether they are necessary and aligned with University mission, goals, and priorities; that information security policies are concise, consistent in format and scope, and easy to understand; to identify constituencies and other policies that may be affected; and to make recommendations to the responsible offices.

Responsible Administrator – The responsible administrator is the highest ranking staff member in a unit who has oversight responsibility for University information security policies in their areas of responsibility. The responsible administrator is accountable for the substance of the University Information Security Policy and compliance with University policies under their jurisdiction; and delegating to others and overseeing the performance within the responsible office. Depending on the scope of the subject matter, an information security policy may have more than one responsible administrator and in such cases, the responsible administrators must communicate and agree regarding policy decisions. In the event of a disagreement between two or more responsible administrators, the more senior ranking responsible administrator will make the decision. If there is a disagreement between two or more responsible administrators with an equivalent rank, the Unit Director will make the decision. At the Unit Director's discretion, the Unit Director may seek input from the UEISC before making the policy decision.

Responsible Office –The responsible office is assigned by the responsible administrator and is tasked with the operational administration of information security policy and its related procedures, processes, instructions, and forms. Depending on the subject matter, an information security policy may have more than one responsible office.

Forms

Standard University Information Security Policy Template

Related Information

University of Nebraska Board of Regents Bylaws and Other Policies

History

Approved by the President on 10/2/2017.