Effective: *February 14, 2019*
Last Revised: *February 13, 2019*

Responsible University Administrators:
Executive Vice President and Provost
Vice President for Information Technology
Vice President for Business and Finance

Responsible University Office:
NU Office of Institutional Research

Policy Contact:
Chief Data Officer
data@nebraska.edu

Institutional Data Use Policy

ID-01

POLICY CONTENTS

Scope

This policy applies to all University of Nebraska (University, NU) employees whose job or contractual responsibilities include inputting, safeguarding, retrieving, or using institutional data as well as those supervising such employees. Organizationally, this policy applied to the University and all of its campuses. This policy shall apply to all University institutional data maintained in all formats, including but not limited to data in paper, electronic, audio, and visual formats.

Policy Statement

All University institutional data is the property of the Board of Regents of the University of Nebraska. Individual campuses, units, or departments may have stewardship responsibilities for portions of the data. Institutional data is crucial to fulfilling the mission of the University and the security of such data is of critical importance. NU data users shall be granted permission to use University institutional data for all legitimate business purposes without unnecessary restrictions on access, taking into account a data user's role within the University, data classification, and the granularity of data requested. Permission for data use shall be granted both across campuses within the University system and across organizational units within each campus when a legitimate business purpose for such data use exists.

The ability to use University institutional data comes with concurrent responsibilities and obligations. All NU data users shall protect the University's institutional data for inappropriate

disclosure, use, and storage at all times, keeping in mind the level of risk associated with various types of data as outlined in the University's Data Classification and Storage Policy and respecting the privacy and confidentiality of individuals whose records may be accessed. Data shall be used only for University business purposes and in a manner congruent with the mission of the University. Data users granted access to institutional data agree to comply with all applicable University policies, guidelines, and standards, as well as applicable state and federal laws and regulations including, but not limited to the Health Insurance Portability and Accountability Act (HIPPA), Family Educational Rights and Privacy Act (FERPA), the Higher Education Act (HEA), federal regulations on the use of human subjects in research, the Gramm-Leach Bliley Act (GLBA), Payment Card Industry Data Security Standards (PCI-DSS), and the European Union's General Data Protection Regulation (GDPR). Use of University data for non-business purposes, improper data disclosure, or inappropriate data storage practices shall result in termination of a data user's access to institutional data and may result in corrective action up to and including termination of employment.

Reason for Policy

The University of Nebraska strives to be a data-informed institution that commits to the furtherance of a data culture where trusted, accessible, and understandable data serves as a foundation for decision-making around issues of student success, institutional effectiveness, fiscal health, and other key metrics. As a data-informed institution, the University will:

- Improve direct access to high quality strategic data for University administrators and other data users; and,
- Realize efficiencies by fostering University-wide collaboration in establishing, maintaining, and delivering secure, valid, and accessible collections of institutional data for shared use by the University community; and,
- Maximize the value of the University's data assets by increasing understanding and use of data; and,
- Enable integrated reporting across a variety of subject matter domains; and,
- Provide a reliable and secure technical environment for data storage and management that strives to mitigate data security risks while concurrently allowing for the maximization of open and transparent data use across the University.

Definitions

Data Classifications: University institutional data is classified as high risk, medium risk, or low risk in accordance with ITS-05: Data Classification and Storage Policy.

Data Leaders: Data Leaders exercise principal administrative authority or fiduciary responsibility over University of Nebraska institutional data and its security on behalf of the University of Nebraska Board of Regents. The Data Leaders for the University of Nebraska are

the Executive Vice President and Provost, Vice President for Business and Finance, and Vice President for Information Technology.

Data Steward: Data Stewards are subject matter experts and operational managers in a campus functional area with day-to-day responsibilities for managing business processes and establishing the business rules for that area. Subject to the Policy Statement and Data Use Request Procedures and Forms directives incorporated within this policy, Data Stewards shall be responsible for first-level determinations regarding disposition of data use requests. Data Stewards shall collaborate with Security Stewards to provision access to requested data upon approval of a Data Use Request. Data Stewards for identified functional areas at each campus shall be determined in accordance with the procedure outlined below.

Data Trustee: Data Trustees are senior University of Nebraska or Nebraska State College officials (typically at the level of Vice President or Vice Chancellor) who provide high-level administrative oversight of business processes related to specific subject matter areas, information security, or legal/regulatory compliance.

Data Trustee Council: The Data Trustee Council shall be responsible for advising the Data Leaders on:

- Prioritization of necessary data governance policies and procedures in accordance with Executive Memorandum No. 32; and,
- Evaluation of data classification assignments; and,
- Nomination of functional area campus data stewards; and,
- Identification of campus representatives for ad hoc subject-specific data steward groups as necessary; and,
- Resolution of second-level data use appeal requests.

Membership of the Data Trustee Council shall be determined in accordance with the procedure outlined below.

Data User: Data Users are individuals who access institutional data to perform their assigned duties.

Institutional Data: Institutional Data is information created, collected, maintained, transmitted, or recorded by or for the University to conduct University business. It includes data used for planning, managing, operating, controlling, or auditing University functions, operations, and mission. Institutional data includes, but is not limited to information in paper, electronic, audio, and visual formats. Institutional Data does not include data used in pursuit of research.

Institutional Data Classification, Use, and Policy Committee: The Institutional Data Classification, Use, and Policy Committee is responsible for:

- Solicitation of input from and communication to data stakeholders;
- Establishment of data definitions, risk classifications, and standards;
- Articulation of proposed data management and disclosure policies;

- Review of data use procedures and forms developed by campus financial area Data Stewards;
- Development or procurement of educational materials on data security and data use;
- Determination of first-level appeals in regard to data use requests;
- Evaluation and documentation of system components, data assets, and their use; and,
- Coordination of subcommittees or task forces as needed.

Member of the Institutional Data Classification, Use, and Policy Committee shall be determined in accordance with the procedure outlined below.

Security Steward: Security Stewards shall work with Data Stewards to provision access to requested data once a Data Use Request has been approved. For the purposes of this policy, Security Seward(s) for each campus shall be appointed by the NU Vice President for Information Technology or his/her designee.

Procedures

Data Steward Designations: Members of the Data Trustee Council shall forward nominations for Data Stewards to the Chancellor of each University of Nebraska campus. The Chancellor of each campus shall, at a minimum, appoint Data Stewards for the following campus functional areas at his/her campus: (a) Faculty and Staff Data; (b) Student Data; (c) Financial and Budget Data; and (d) Alumni and Foundation Data. Data Stewards for specific subareas of the aforementioned functional domains may be appointed at the discretion of each Chancellor. The NU Chief Data Officer and NU Associate Vice President for Business and Finance shall serve as Data Stewards for the University of Nebraska Central Administration. A current list of all appointed Data Stewards, their functional areas, and their contact information shall be maintained on both campus and NU system websites.

Data Trustee Council Membership and Terms: Permanent members of the Data Trustee Council shall include the NU Vice President for Business and Finance; NU Assistant Vice President for ITS Security Services; NU Vice President and General Counsel; Nebraska State College System (NSCS) Vice Chancellor for Facilities, Planning, and Information Technology; NCSC Vice Chancellor for Academic Planning and Partnerships; NU Chief Data Officer; and the NU Chief Audit Executive (ex-officio) or their designees.

Rotating membership on the Data Trustee Council shall be appointed by the NU Executive Vice President and Provost and shall be comprised of one individual representing each of the following areas: NU campus Chief Academic Officer; NU campus Chief Research Officer; NU campus Chief Business Officer; and NU campus Chief Student Affairs Officer. Rotating membership shall be appointed such that no NU campus has more than one representative at a time and appointees shall serve staggered three-year terms to ensure continuity.

Data Use Request Process and Forms: Data Stewards from across all campuses shall be jointly responsible for the creation and documentation of a single University-wide set of written processes and Data Use Request Forms applicable to data use requests for institutional data in their functional area of expertise. The NU Chief Data Officer shall collaborate with campus functional area Data Stewards in the development of Data Use Request processes and forms when necessary. Written processes and request forms shall be reviewed by the Institutional Data Classification, Use, and Policy Committee and approved by the Data Trustee Council.

All written Data Use processes documentation shall explicitly state the decision criteria to be used in determining whether a Data Use Request will be granted. Decision criteria shall take into account the policy considerations articulated in this document. Any Data Use Request forms developed shall, at a minimum:

(a) Describe the data that is the subject of the request;
(b) Explain the intended use of the data;
(c) Identify any locations and new or existing information systems in which the data will be stored;
(d) Indicate the security classification(s) of the requested data;
(e) State why access to requested high-risk data is necessary for performance of the Data User's assigned job responsibilities, if access to high-risk data is requested;
(f) Certify that the Data User has completed all currently required data security and data use training; and,
(g) Require the approval of the Data User's supervisor.

Data Use Requests: Data Use Requests shall be submitted to the applicable functional area Data Steward at the Data User's primary campus using the approved written Data Use Request Form. Data Use Request Forms shall be made available to Data Users on both campus and NU system websites. Such requests may be submitted through designed electronic processes should these become available in the future. In the event of a cross-campus Data Use Request, Data Stewards from the relevant functional areas on each campus involved shall confer and a joint decision of the Data Stewards from each campus shall be rendered on the request. If a Data User's request is granted in whole or in part, a Campus Security Steward shall be responsible for carrying out all technical activities or operations necessary to grant access to approved data. In the event that a Data User's request for data access is denied in whole or in part, the Data Steward(s) involved in the determination of the request shall deliver a written statement of the reason(s) for denial of the Data Use Request to the Data User in a timely manner.

Data Use Requests – Appeal: In the event that a Data User's request regarding data use is denied in whole or in part, the Data User may appeal this decision to the Institutional Data Classification, Use, and Policy Committee with the permission of the Data User's supervisor. The written Data Use Request Appeal form can be emailed to the policy contact located at the top of this policy or submitted through designated electronic processes should these become available in the future. Data Use Request Appeal forms shall be accompanied by a copy of the

original written justification for denial. The Institutional Data Classification, Use, and Policy Committee shall confer with all Data Stewards involved in the original determination to deny access prior to rendering a decision, document in writing the bases for sustaining or denying the Data Use Request Appeal and deliver such documentation to the Data User in a timely manner. Appeal of decisions by the Institutional Data Classification, Use, and Policy Committee may be appealed to the Data Trustee Council, and then to the NU Executive Vice President and Provost. The decision of the Executive Vice President and Provost shall be considered final.

Institutional Data Classification, Use, and Policy Committee: Permanent members of the Institutional Data Classification, Use, and Policy Committee shall include the Director of NeBIS, Director of NeSIS, NU Chief Information Security Officer, NU Manager of Identity Access management, a representative from the NU Office of Business and Finance, a representative from the NU General Counsel's office, and the NU Chief Data Officer. Additional ad hoc representation for subcommittees and task forces may be added at the discretion of this group in response to priorities identified by Data Leaders and/or the Data Trustee Council.

Training: All users of institutional data shall be required to complete an information security training as specified in ITS-05: Data Classification and Storage Policy, and a data security training prior to a grant of authorization to use institutional data. For additional information on either training, please contact the ITS Cybersecurity Office at its-sec@nebraska.edu.

Contacts

NU Chief Data Officer: data@nebraska.edu
NeSIS Director: NeSIS@nebraska.edu
NeBIS Director: NeBIS@nebraska.edu
NU ITS Cybersecurity Office: its-sec@nebraska.edu
NU General Counsel's Office: https://nebraska.edu/administration/general-counsel-legal.html

Forms

Data Use Request Appeal Form

Related Information

ITS-05: Data Classification and Storage Policy
Nebraska Records Retention Schedules
Executive Memorandum No. 16
Executive Memorandum No. 26

History

February 13, 2019 Approved by President's Council