disclosure, use, and storage at all times, keeping in mind the level of risk associated with

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

n-

business purposes, improper data disclosure, or inappropriate data storage practices shall

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,
>
> asing 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, Senior Vice President and CFO, and Vice President for Information Technology.

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: The Chancellor of each campus shall, at a minimum, appoint Data Stewards for the following campus functional areas at his/her campus: (a) Financial and Personnel Data; and (b) Student Data. Data Stewards for specific subareas of the aforementioned functional domains may be appointed at the discretion of each Chancellor. The NU Associate Vice President and Director, NeBIS, NU Assistant Vice President and Director, NeSIS, and NU Director, Enterprise Data Solutions shall serve as Data Stewards for the University of Nebraska Office of the President. 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 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 Director, Enterprise Data Solutions 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 Governance 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
                                        -risk data is requested;
(f) Certify that the Data User has completed all currently required data security and data use training; and,
(g)