Proposed New ARP

Rule 15.40 –Data Governance v022620

PART 1: PURPOSE

Consistent with direction from the NMSU Board of Regents and applicable laws and regulations, this rule is adopted:

A. To modify and document the university's Data Governance Program framework;
B. To clarify the roles, responsibilities and accountability required of the Data Governance Committee, Data Trustees, Data Stewards, Data Custodians, and Data Users;
C. To authorize the adoption and use of standard operating protocols by the various Data Stewards for their particular areas of operation, consistent with policy, law and best practices.
D. To augment the university's compliance with applicable laws and regulations; and
E. To emphasize the importance of, and to require, effective Data audit capability.

PART 2: DEFINITIONS

Defined terms are capitalized to denote that the term is defined for purposes of this rule.

A. **Access**: The ability to read, write, copy, query, download, delete or transmit Institutional Data.

B. **Data Custodian**: An employee who has operational responsibility for the management of any of the systems that serve as sources of Institutional Data.

C. **Data Governance**: Regulation and protection of Institutional Data through its full life cycle, from creation or acquisition, access and use, to final disposition. A data governance program includes:

1. protection of sensitive data;
2. vulnerability assessment and risk management;
3. enforcement of legal, regulatory, contractual, and architectural compliance requirements;
4. identification of stakeholders, their roles and responsibilities;
5. access management; and
6. data inventory, classification and definition

D. **Data Governance Committee**: A university board (*RPM 2.30*) established by the chancellor consisting of the university's Data Trustees and other senior administrative officials assigned the responsibility for modifying, formalizing and implementing the university's Data Governance Program in accordance with regents policies, applicable laws and regulations and this rule, as well as with other best practies standard operating protocols the committee may approve for the NMSU system.

E. **Data Steward**: An employee, typically a supervisor, designated by the relevant Data Trustee to oversee access and management of a particular subset of Institutional Data overseen by the Data Trustee.

F. **Data Trustee**: A senior administrator with significant responsibility for a major operational area, utilizing systems and applications serving as authoritative sources of Data relied upon by the institution. (*See Appendix ARP 15.40 – A for list of major operational areas*).

G. **Data User:** NMSU employees or agents whose job duties require access to Institutional Data.

H. **Institutional Data/Data**: Institutional Data (or "Data") refers to the university's information resources and administrative records in any form, including but not limited to print, electronic, or audio-visual. Examples include:

1. Data created, acquired and/or maintained by university employees in performance of official job duties;
2. Data created or updated via use of a university computer system;
3. Data relevant to research, planning, managing, operating, or auditing ; and
4. Data included in official university administrative reports or official university records.
5. Data within the university's purview, including records that the university may not own but that are governed by laws and regulations to which the university is held accountable.
6. Data that pertains to, or supports, the administration and mission of the university.

PART 3: ROLES, RESPONSIBILITIES AND ACCOUNTABILITY FOR DATA GOVERNANCE PROGRAM

The Data Governance Committee and other data officials and s listed below are collectively and individually responsible for implementing the NMSU Data Governance Program.

A. **Data Governance Committee**: The Data Governance Committee develops and implements the Data Governance Program for the NMSU system, including the adoption and publication of data governance policies, rules and procedures or other standard operating protocols applicable primarily to the work of the Data Stewards and Data Users. The Data Governance Committee may establish subcommittees or assign tasks to university units or employees to assist with ongoing Data Governance Program work.

B. **Data Trustee**: Generally, the Data Trustees ensure access to and safeguard security, integrity and usefulness of their respective areas' Institutional Data. The responsibilities of the Data Trustees include:

1. Identify the sensitivity and criticality of the Data.
2. Ensure that appropriate business processes are in place to keep the Data secure, maximize Data accuracy, and ensure that responsible staff are trained regarding the Data Governance Program requirements.
3. Oversee planning and governance to meet the data needs of the institution and support data-driven decision making. Work closely with other members of the Data Trustee Council and other members of the senior administration to ensure that the appropriate resources (staff, technical infrastructure, etc.) are dedicated to prioritizing Data needs and setting and enforcing standard operating protocols related to Data management and use.
4. Implement the university's policies, rules and procedures as well as the standard operating protocols approved by the Data Governance Committee, for compliance with applicable laws and regulations related to data governance.
5. Serve as liaison to the chancellor or campus president, as appropriate, for issues related to data governance.
6. Designate and supervise the Data Stewards within the Data Trustee's major operational area.

C. **Data Steward**: The responsibilities of the Data Stewards include:

1. Establish standard operating procedures (SOPs) and implement data governance standards.
2. Ensure that staff who maintain Data are trained to follow standards.
3. Maintain Data quality. Work with technical and operational staff to create a process for identifying Data entry errors and correcting the Data and data entry processes to meet data governance standards. Report to the Data Trustee any issues that may require modifications or enhancements of data governance structures or standards.
4. Control access to Data. Develop appropriate standard operating protocols controlling access to Data based on job duties, and which serve the Data needs of the institution for the lifecycle of the Data.
5. Respond to inquiries about Data. The Data Steward will receive and respond to any inquiries related to Data they oversee.
6. Conduct and document regular system account access reviews to Data and systems to meet audit and requirements.

D. **Data Custodian**: The responsibilities of the Data Custodians include:
1. Provide a secure infrastructure in support of the Data. This includes, but is not limited to, physical security, network security, system security, system logging, and secure transmission of the Data.
2. Grant, modify, revoke and document authorization for, system access to Data Users based on established access policies, rules, procedures or standard operating protocols. Assist with implementation of Data access policies, rules, procedures and standard operating protocols.
3. Ensure system availability and adequate response time. Monitor system availability, backup system Data and develop disaster recovery plans; Install, configure, patch, and upgrade hardware and software used for Data management; Make sure that systems are maintained in accordance with policies and/or service level agreements.
4. Participate in setting data governance priorities. Provide details on technical, systems, and staffing requirements related to data governance initiatives.

E. **Data User**: The responsibilities of each Data User include:
1. Attend training and follow policies, rules, procedures and standard operating protocols related to Data management and protection. This includes those relating to the security, integrity, quality, consistency, handling, and dissemination of Institutional Data.
2. Identify areas of Data needs not yet served.
3. Report concerns related to Data management and protection. Convey to the appropriate NMSU administrator any observations or concerns about weaknesses in Data protection, failure to follow Data management policies, or specific issues of quality or integrity of NMSU data.

.

PART 4: NMSU DATA GOVERNANCE STANDARDS

The Data Governance Committee will work collaboratively with university officials, including the Chief Privacy Officer, Chief Information Security Officer, and Chief Information Officer to ensure the establishment of uniform university data governance rules and associated standard operating protocols, including but not limited to:

- Data Inventory
- Data Classification;
- Data Safeguards;
- Data Sharing and Usage;
- Data Dictionary and Definitions;
- Data Entry and Reporting

- Identity and Access Management;
- Data Security;
- Data Privacy and Regulatory Compliance;

PART 5: DATA GOVERNANCE TRAINING

A. NMSU employees will be trained about the NMSU system's Data Governance Program, including all policies, rules and procedures, as well as the standard operating protocols that apply withint their area's operations. Each Data Trustee must ensure that appropriate training is received by all new hires, incumbent employees, and volunteers or others granted access to Instiutional Data. After the initial training, refresher or update training will be provided on a periodic or as needed basis.

B. To ensure compliance with the data privacy regulatory training requirements, some NMSU employees will be required to participate in data privacy compliance training, which may be offered pursuant to Rule 3.19.25 - Mandatory Employee Training and Other Professional Development Opportunities. Official training logs and certificates will be kept in the institutional training system maintained by Human Resource Services, Center for Training and Professional Development.

Details
Scope: NMSU System
Source: ARP Chapter 15 | Information Management and Data Security
Rule Administrator: ***TBD***
Last Updated: ***will be date the rule is approved***
Related
Cross-References:
RPM 15.30, Information Technology Governance
RPM 15.40, Data Governance ***[note: this is concurrently pending – Q?: what edits are needed to 15.30 and 15.50 in light of new proposal for 15.40?]***
RPM 15.50, Information Data Security
ARP 14.10 - Records Integrity and Retention
ARP 15.60 – Management of Health Information – HIPAA Compliance
ARP 15.62 – Protection of Federal Information; FISMA Compliance
ARP 15.63 – Protection of Customer Information; GLBA Compliance
ARP 15.64 – Social Security Numbers, Use of
ARP 18.40 – Inspection of Public Records
Revision History:
XX/YY/2020 Adopted by Chancellor