Norman Data Governance Committee Meeting

March 9, 2020

Members present: Susannah Livingood, Jennie Clary, Chris Kennedy, Jeff Wall (for David Horton), Sandra Nettleton, Heather Hendricks, Andrea Deaton, Marcy Fleming (by phone).

Members absent: Will Wayne, Charles Wright, Karen Smith.

1. Introductions for new committee staff member – Jennie Clary

2. Draft policy update (see attached ***DGC_Policy_Draft_20200304.docx***)

    a. Per discussion, removed anything that might more appropriately be covered in a standard.

    b. Idea is to have one policy to cover both Norman and HSC that would then possibly split into more specifics for each campus. Questions would then be referred to a "committee of the whole" with representation from both campuses.

    c. Sandra Nettleton agreed to take the policy to HSC-ISRB committee at their next meeting (March 10) and provide feedback to N-DGC. Norman campus's focus has been primarily governance whereas OUHSC has been more focused on risk, so the hope is that any gaps will be filled as a result of the collaboration.

3. IT project list update

    a. Incorporated feedback from this group, first report in updated format

    b. IT Risk Assessment information will be added to the document, including a short summary of findings for the committee's information.

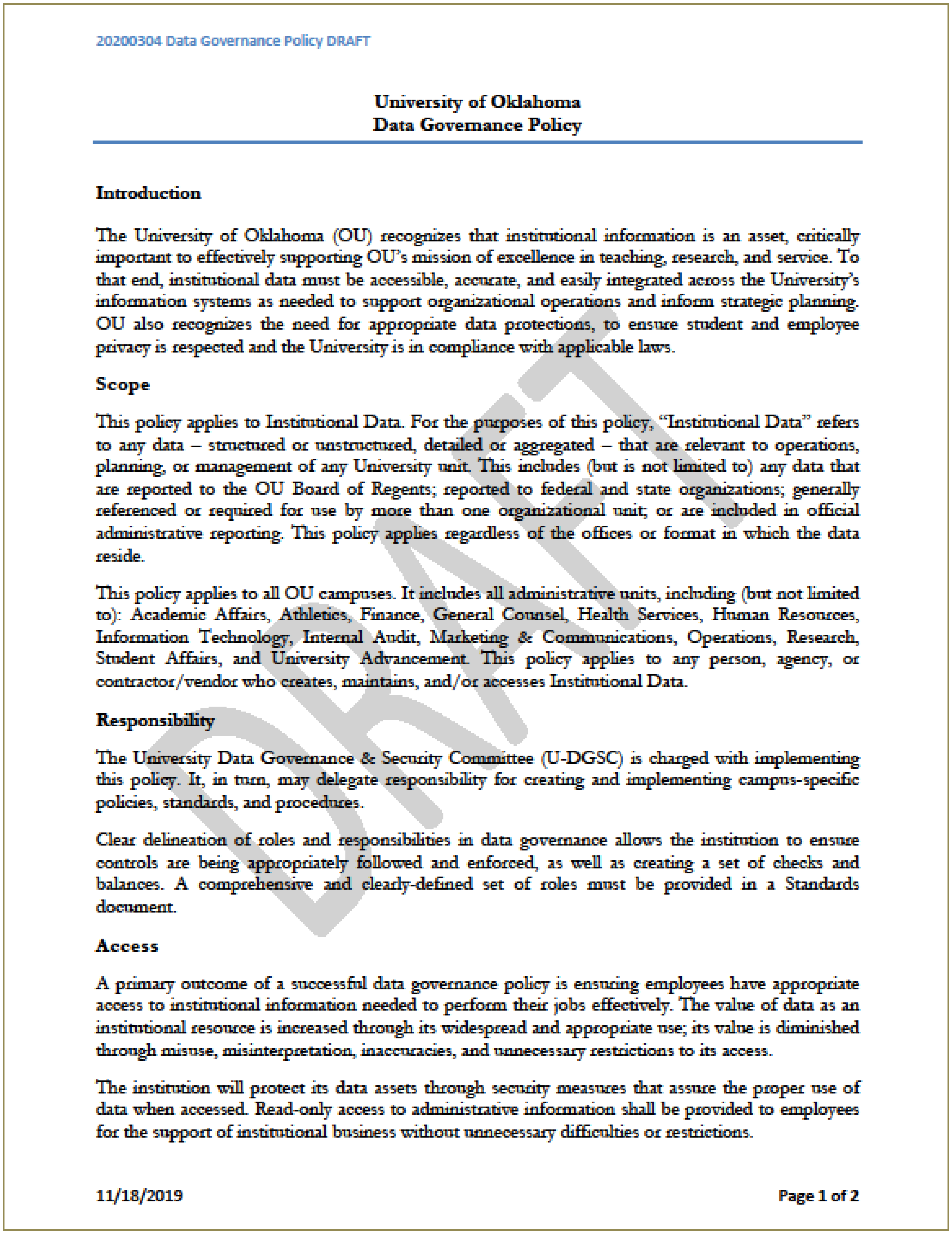
    c. There was some conversation about how the document was best presented. Its current format requires some manual entry; would a shared Excel document where all parties can contribute be a better option?

    d. Jeff Wall will consult with JP on the best practice moving forward and circle back with Susannah Livingood.

4. Law Salesforce integration

    a. Chris Kennedy and Susannah approved, with Data Steward Kellie Dyer assent – group had some questions that were addressed by Chris and Susannah about where the data originates and if an IT risk assessment had been performed

    b. There were no significant issues identified; it was stipulated that if the data was used for any purpose other than the one stated an additional IT risk assessment would need to be performed. Until such time, the committee approved the request.



University of Oklahoma
Data Governance Policy

Introduction

The University of Oklahoma (OU) recognizes that institutional information is an asset, critically important to effectively supporting OU's mission of excellence in teaching, research, and service. To that end, institutional data must be accessible, accurate, and easily integrated across the University's information systems as needed to support organizational operations and inform strategic planning. OU also recognizes the need for appropriate data protections, to ensure student and employee privacy is respected and the University is in compliance with applicable laws.

Scope

This policy applies to Institutional Data. For the purposes of this policy, "Institutional Data" refers to any data – structured or unstructured, detailed or aggregated – that are relevant to operations, planning, or management of any University unit. This includes (but is not limited to) any data that are reported to the OU Board of Regents; reported to federal and state organizations; generally referenced or required for use by more than one organizational unit; or are included in official administrative reporting. This policy applies regardless of the offices or format in which the data reside.

This policy applies to all OU campuses. It includes all administrative units, including (but not limited to): Academic Affairs, Athletics, Finance, General Counsel, Health Services, Human Resources, Information Technology, Internal Audit, Marketing & Communications, Operations, Research, Student Affairs, and University Advancement. This policy applies to any person, agency, or contractor/vendor who creates, maintains, and/or accesses Institutional Data.

Responsibility

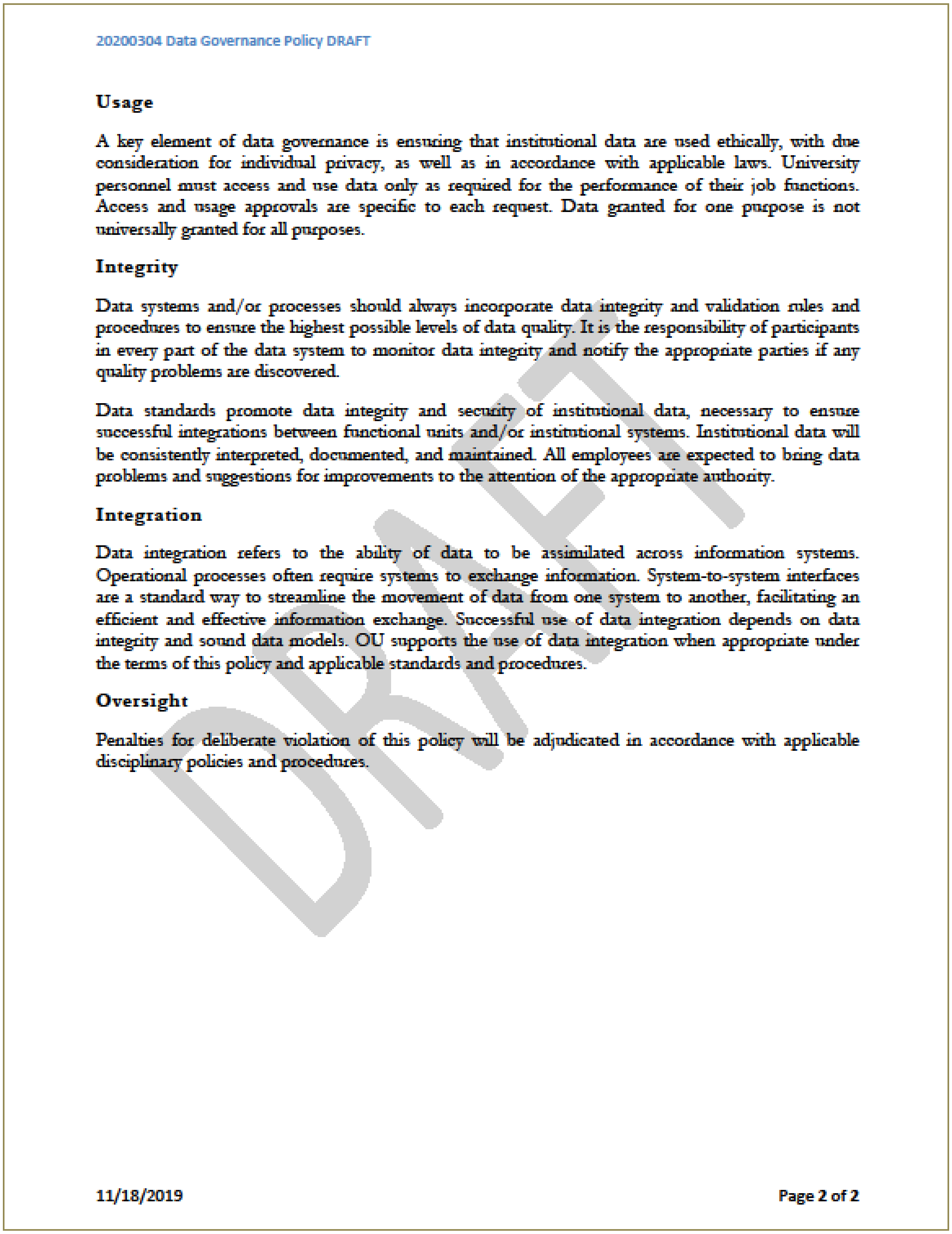
The University Data Governance & Security Committee (U-DGSC) is charged with implementing this policy. It, in turn, may delegate responsibility for creating and implementing campus-specific policies, standards, and procedures.

Clear delineation of roles and responsibilities in data governance allows the institution to ensure controls are being appropriately followed and enforced, as well as creating a set of checks and balances. A comprehensive and clearly-defined set of roles must be provided in a Standards document.

Access

A primary outcome of a successful data governance policy is ensuring employees have appropriate access to institutional information needed to perform their jobs effectively. The value of data as an institutional resource is increased through its widespread and appropriate use; its value is diminished through misuse, misinterpretation, inaccuracies, and unnecessary restrictions to its access.

The institution will protect its data assets through security measures that assure the proper use of data when accessed. Read-only access to administrative information shall be provided to employees for the support of institutional business without unnecessary difficulties or restrictions.



Usage

A key element of data governance is ensuring that institutional data are used ethically, with due consideration for individual privacy, as well as in accordance with applicable laws. University personnel must access and use data only as required for the performance of their job functions. Access and usage approvals are specific to each request. Data granted for one purpose is not universally granted for all purposes.

Integrity

Data systems and/or processes should always incorporate data integrity and validation rules and procedures to ensure the highest possible levels of data quality. It is the responsibility of participants in every part of the data system to monitor data integrity and notify the appropriate parties if any quality problems are discovered.

Data standards promote data integrity and security of institutional data, necessary to ensure successful integrations between functional units and/or institutional systems. Institutional data will be consistently interpreted, documented, and maintained. All employees are expected to bring data problems and suggestions for improvements to the attention of the appropriate authority.

Integration

Data integration refers to the ability of data to be assimilated across information systems. Operational processes often require systems to exchange information. System-to-system interfaces are a standard way to streamline the movement of data from one system to another, facilitating an efficient and effective information exchange. Successful use of data integration depends on data integrity and sound data models. OU supports the use of data integration when appropriate under the terms of this policy and applicable standards and procedures.

Oversight

Penalties for deliberate violation of this policy will be adjudicated in accordance with applicable disciplinary policies and procedures.