Data Governance

Data Stewards and Custodians Meeting

January 28, 2020

AGENDA

I. Data Systems Access: 5/30 Rule Implementation

II. Data Cookbook

III. Tier 2 Requirements and Deadlines

IV. Looking Ahead to Tier 3

V. Tier 1 Outstanding Items

VI. Guidance and Support from Data Governance Team

System Access Controls: 5/30 Rule

BOR BPM 12.4.3: Data trustee or designee will ensure that a business process exists to update information system access no more than **five** business days after terminations and no more than **30** days after other personnel status changes.

Campus Broadcast
January 15, 2020

Changes to the Deactivation Process for Former Employee CampusID Accounts

To comply with University System of Georgia policy, beginning **Friday, Jan. 31** Instructional Innovation and Technology will update the automated process used to deactivate CampusID account access for former faculty, staff and student employees. Faculty, staff and student employee CampusID access will be automatically deactivated **five business days** after the last date of university employment. *(Prior to this change, employee CampusID access has remained active for 180 days after the last date of employment.)*

Deactivation of CampusID will enable compliance with the 5-day rule for data systems using Single Sign-On

5/30 Rule: Transfers (all data systems) and Systems not on SSO

- **All data stewards are responsible for ensuring data access is adjusted appropriately for data users who have transferred to other positions within thirty days of the transfer.**
- Data stewards of systems not utilizing SSO will be responsible for having business procedures to ensure compliance with the 5-day access termination requirement for terminated users in addition to the 30-day requirement for transfers.
- A list of transfers and terminations will be circulated weekly by the Data Coordinator (Erik Lauffer) to the stewards.

data cookbook

idata
Data Management for Higher Education

- Procurement process underway
  - Working with iData to determine which features will require assistance and input from IIT to implement.
  - Will follow-up with IIT in February.
- Anticipated implementation schedule (goals):
  - Purchase and setup by April 30, 2020
  - Training for Data Stewards May – June 2020
  - System fully implemented and active July 1, 2020
- Will facilitate compliance with upcoming USG requirements regarding data definitions and classification

Tier 2 Requirements

6/30/2020

Section	Current Status
Data Governance Structure	Complete
Data Availability	Partially complete for some systems
Training	Information gathering and planning

Tier 2 Requirements 6/30/2020

12.3.4 Data Availability

Assets of the USG should be available commensurate with their operational importance. For all data domains and their respective data systems, the organization should document and socialize to data users the expectations and processes around the availability of each data resource including, but not limited to:

- The periods of time data is available;
- Expectations for “uptime” (percent of time data is available) if appropriate;
- Modes of access (types of devices, etc.) that are provided for;
- Communications plan around both planned and unplanned system downtime; and,
- Method for users to report an unexpected lack of availability of data or data systems.

Tier 2 Requirements 6/30/2020
12.3.4 Data Availability

Current State

- Several of the mission critical systems already meet this requirement
- Data Governance Team will work IIT to determine enterprise network availability and other assumptions regarding service levels
- We will circulate guidance for data stewards to assist in documenting the specifics of data availability for each system

Tier 2 Requirements 6/30/2020

12.5.2 Training

USG Institutions must:

- Provide role specific training to all individuals within the data governance structure, including data users and all those subject to data governance policies;
- Ensure individuals understand their roles and the larger governance structure, responsibilities, and applicable policies and procedures;
- Provide training to individuals as they enter these roles, when there are substantive changes to training and at regular intervals over time to ensure up-to-date understanding;
- Update training materials as changes to policy and procedure require;
- Document participation in training and audit training participation at regular intervals;
- Provide training materials in a permanent form (such as on a website) for individuals to reference as needed;
- Specifically address in training materials for all individuals how data classified as public or protected is managed throughout its lifecycle; and,
- Provide clear information about how an individual should proceed if he or she believes data policies or standards are not followed, or there has been a breach of data security.

Tier 2 Requirements 6/30/2020

12.5.2 Training

- We will develop a basic training module for all data stewards and users
- We will work with HR and Legal Affairs to ensure new hires are receiving adequate data governance training
- We will circulate a draft of the training module to the stewards for feedback before finalizing
- Stewards may supplement the basic University training with system-specific training

Looking ahead to Tier 3: 12/31/2020

12.3.2 Data Elements and Data Definition Documentation

For all data systems, there must be a mechanism to access documentation of the system's table structure and data elements. In addition, for systems that are part of routine data collection and reporting, data element dictionaries should be maintained that include:

- Data definitions;
- Metadata including data sources and security classifications;
- Business practices where applicable;
- Any validations or quality checks applied against the elements;
- Change history; and,
- Valid values.

Looking ahead to Tier 3: 12/31/2020

12.3.3 Data Quality Control

USG organizations must ensure that information is of the highest possible quality to facilitate effective decision-making. Data quality refers to the accuracy, timeliness, comparability, usability, completeness and relevance of data.

Data quality requires USG organizations to appropriately collect, store, process and manage data, whether electronic or physical. As part of data governance, USG organizations must communicate, prioritize and practice data quality. Just as institutions maximize their financial resources and facility assets, USG organizations should invest in the quality of their data holdings.

For all data essential to operation and reporting, each USG organization should:

- **Document and promulgate data standards and definitions** to ensure accurate data entry or data creation;
- **Assess collected data** to ensure accuracy, completeness, and adherence to standards at a minimum on an annual basis; and,
- Regularly consult data users or stakeholders to ensure data usability and relevance.

Tier 1 Status
12.3.1: Mission Critical Systems

- All systems "partially" meet requirements given the pending work on disaster recovery and business continuity, must complete by 12.31.20
- A few systems lack updated user procedures or technical guidelines
- Interviews will commence with remaining Enterprise systems to determine if others need to be added to this list
- Over the next six months, Branden will be reaching out regarding development / enhancement of business continuity plans and any follow-up needed on business continuity plans of third-party vendors

Communication	Office 365 WordPress Multi-site Dept Storage
FERPA	Banner Accounts Receivable Banner Document Management Banner Financial Aid Banner Self-service (GoSOLAR) Banner Student Bill+Payment CommVault Parchment Slate Student Accommodation Manager (SAM) Terradotta
Instruction	iCollege
Payments	OneUSG PeopleSoft Financials Raisers Edge (added in January)
Safety & Security	Axiom GLUU SSO Manager NetIQ Sunapsis

Tier 1 Status: 12.4 Cybersecurity (must complete by 12.31.20)

Section	What needs to be done and how are stewards impacted?
Safeguards	Mission critical systems will receive a risk assessment by Cybersecurity and a monitoring program will be developed
Classification	Implementation of the Data Cookbook will assist in identifying and classifying all PII and ensure procedures and processed are in place for proper classification
Access Procedures	• Implementation of the 5/30 rule • Steward analysis and definition of user roles • Steward compliance with six-month access review rule: *"Access to an information system must be reviewed regularly. Data stewards must review user access to the information system every six months and document findings."* Compliance already in place for many systems; method of compliance can be different across systems but all stewards must document their process
Separation of Duties	Development of general guidelines by data governance team to guide users in conducting an evaluation of separation of duties

Guidance / Support from Data Governance Team

- Legal guidance distributed in December
- Tier 1 checklist for data stewards forthcoming
- Let us know how we can assist you in formalizing your processes and procedures and areas where you might need help