Financial Data Stewardship Implementation Guide

Reason for Implementation Guide

University Policy 4.12, Data Stewardship and Custodianship informs users, data stewards and custodians of the university's administrative data of their responsibilities for using that data consistent with the university's standards of security and confidentiality. This document provides additional guidance for implementing policy 4.12 with respect to financial data and information. The goal is to meet the business needs of the university while also protecting the university's data assets and to provide open and easily available access to financial information.

(Reference: https://www.dfa.cornell.edu/policy/policies/data-stewardship-and-custodianship)

Contents

Entities Affected by this Implementation Guide

All units of the university, excluding the Weill Cornell Medicine)

Who Should Read this Implementation Guide

- All members of the Cornell University community using or having access to financial data
- Anyone extracting, translating or presenting Cornell University financial data for others

Related Documents

University Documents	Other Documents
University Policy 4.12, Data Stewardship and Custodianship	Annual PCI Requirements Annual Certification Dashboard
University Policy 5.10, Information Security University Policy 5.8, Authentication to Information Technology Resources University Policy 4.7, Retention of University Records	Financial Data Access Dashboard

(Reference: https://www.dfa.cornell.edu/policy)
(Reference: https://www.dfa.cornell.edu/treasurer/cash-management/proccreditcards)
(Reference: https://obieeprod.cit.cornell.edu/)

Contacts

Subject	Contact	Telephone/Email/Web Address
Financial Data Steward	Associate Vice President and University Controller	(607) 254-8975
Guideline Clarification	Director of Financial System Administration and Information Delivery	(607) 254-8633
Kuali Financial System Support		https://www.dfa.cornell.edu/fsaid/gethelp
Financial Information Delivery and Reporting Support		kfs-idr@cornell.edu

Definitions

Data: A set of qualitative or quantitative values that are the result of measurement and represented in a well-defined structure.

Information: Communication of accurate and timely data that has been given meaning and relevance by context and organization.

University Administrative Data: Administrative functional area data, in any form, including that stored centrally as well as in colleges and departments.

Financial Data: At Cornell, financial information is most commonly derived from the data stored in the Kuali Financial System (KFS) and the Kuali Data Warehouse (KDW) or extracted from those sources. Additional data and backup documentation exists in central offices and individual units.

Stewardship: University Policy 4.12, Data Stewardship and Custodianship identifies stewards for financial data to be the Associate Vice President and University Controller. Data stewards are responsible for establishing definitions of the available administrative data sets and developing access procedures for those data sets, as appropriate. The financial data steward is responsible for centrally delivered financial reports that are produced from data in financial systems. Stewardship responsibility is delegated to the senior financial officer in the local unit for local financial information, data extracts from central systems, and reports generated locally.

Custodianship: Anyone who possesses or has access to university administrative data, either electronic or otherwise, is a custodian of this data. Custodianship and its associated responsibilities apply to individuals who dispense or receive data.

Responsible Use of Financial Data

The Division of Financial Affairs (DFA) follows rigorous guidelines for developing, testing, and securing centrally managed financial systems. DFA is responsible to ensure that the financial data it maintains and the information it produces is complete, accurate, authorized, and consistent. Once financial data is disseminated to local units, any additional manipulation of the data or creation of value-added systems becomes the responsibility of the unit. Those responsibilities include design, comprehensive testing, adequate documentation, and funding for ongoing operations and maintenance.

At the university, financial data is presented for different audiences and levels of expertise in numerous formats including the following:

1. Kuali Financial System queries/lookups[1]
2. Centrally provided reports[1]
3. Locally developed ad-hoc queries[2]
4. KFS and KDW data extracts; local unit/college reports[2]
5. Applications developed by local units[2]

[1] centrally validated for accurate presentation

[2] responsibility of the local unit/end users to ensure accuracy of information

Central electronic financial systems such as KFS and KDW store data in complex structures with a large number of attributes that must be correctly used to return accurate results. Current-generation reporting tools provide users flexibility and functionality to use that data to produce useful information and knowledge. It is critical that report creators and application developers fully understand the data they use, so that the resulting information is accurate and reflects the intended meaning to end users. Reports should be validated against the KFS application or centrally supported dashboards to ensure data integrity and accuracy.

Custodian Roles and Responsibilities

Custodian responsibilities with financial data include:

- Acquire necessary training on data definitions and usage. Request clarification to ensure understanding.
- Sign an Access to University Data Agreement in accordance with University Policy 4.12, Data Stewardship and Custodianship.
- If data is being extracted into another system (including Excel), ensure data integrity between the source system (KFS or KDW) and local system.
- Ensure accurate information presentation by validating to official university records (e.g., financial dashboards or KFS system).

- When creating new reports and representations of information, document transformations and filtering performed to source system data.
- When publishing information or sharing with others, include a note indicating the responsible office for the presentation of the data and a contact for questions.
- When creating new electronic applications that include financial data, implement access controls for local systems and tools, provide customer support and develop remediation procedures for when central systems are upgraded.
- Adhere data access to central university-defined controls. Ensure that any deviations are approved by financial data stewards. See the authorization chart below for the processes for obtaining approvals.
- Secure storage and transmission of data in accordance with University Policy 5.10, Information Security.
- Respond to University Audit inquiries or reviews of locally transformed and presented information.

Central Office Role and Responsibilities (DFA/CIT)

The Division of Financial Affairs (DFA) and Cornell Information Technologies (CIT) support the tools and representation of data in the central financial application (KFS) and data warehouse (KDW). DFA and CIT are jointly responsible to support data custodians in the following ways:

- Provide training and consulting support on data, tools, and services.
- Provide guidance to local financial data stewards and delegates.
- Provide tool and processes for financial data stewards and authorizers to request financial data and access.
- Modify central systems and data sources using defined change-management processes; fully test to assure quality is retained.
- Communicate to all data custodians changes that impact use of data.
- Provide access to development and test system instances during upgrades to allow for testing of data integrations prior to release to production.
- Monitor system performance and reliability; work to resolve any issues in a timely manner.

Roles and Responsibilities Summary

	End User	Provider	DFA	CIT
Data Knowledge				
Acquire training	✓	✓		
Ensure understanding	✓	✓		
Provide user support			✓	

Respond to audit inquiries		✓	✓	✓
Information Accuracy				
Ensure integrity	✓	✓	✓	
Validate results	✓	✓	✓	
Document transformations	✓	✓	✓	
Identify contact in responsible office	✓	✓	✓	
Data Access				
Appropriate access controls		✓		✓
Secure transmission and storage		✓		
System Support				
Provide and support enterprise tools		✓	✓	✓
System access (dev/test/prod)				✓
Change management process		✓	✓	✓
Communicate changes		✓	✓	
Remediation of downstream systems		✓		
Monitor system performance		✓	✓	✓

Confidential and Sensitive Financial Data

University Policy 5.10, Information Security categorizes institutional information into three levels: 1) Confidential, 2) Restricted and 3) Public. Level 1 confidential data includes:

- Social Security number
- Credit card number
- Driver's license number
- Bank account number
- Protected health information , as defined in the Health Insurance Portability and Accountability Act (HIPAA)

Financial systems can include level 1 confidential data, and access to such data is restricted and not made available through general purpose reporting tools. Staff members who receive such data in the course of performing their job duties must follow university policy in its management.

Restricted (level 2) information is defined as "all information used in the conduct of university business, unless categorized as public (level 3) or confidential (level 1)." By this definition, most financial data is restricted. Within this level, certain data are considered sensitive. Sensitive data includes individual salary data (or data that might allow a person to determine salary) and detailed purchasing information.

Contractual agreements may include non-disclosure agreements on certain pricing discounts or other arrangements.

Where sensitive KFS or KDW data is needed to perform business activities, access will be restricted and data limited to a minimal subset needed to perform those activities (e.g., by org or business function).

(Reference: https://www.dfa.cornell.edu/policy/policies/information-security)

Storage and Transmission of Financial Data

Because of its nature of being restricted or confidential, all financial data should always be stored in limited-access locations, transmitted via secure methods, and only shared with persons with a business need to have the information. Data that is restricted but not sensitive or confidential can be shared via email or university-approved collaboration spaces. Sensitive or confidential data should not be shared by email or collaborative tools. Cornell Dropbox (https://dropbox.cornell.edu) is the approved method for transmitting sensitive data. Confidential data handling must strictly adhere to university policy and best practice.

(Reference: https://www.dfa.cornell.edu/policy/policies/information-security)

Data Access

Provisioning and Deprovisioning

As faculty, staff members, and students join the university, change positions, shift job responsibilities or leave the university, it is critical that their access to financial data be granted, modified, or removed to avoid risk of data exposure or misalignment with business responsibilities. Supervisors are responsible for working with financial data authorizers to immediately initiate changes. When jobs change to another unit, the old unit is responsible to de-provision current access, and the new unit is responsible to request appropriate access. The Financial Data Access dashboard in OBIEE provides a means to monitor access on a regular basis.

(Reference: https://obieeprod.cit.cornell.edu/analytics/saw.dll?dashboard&PortalPath=%2Fshared%2FFinancials%2F_portal%2FFinancial%20Data%20Access)

Authorization

Approval for access to financial data is controlled and explicitly defined. The following table identifies the authorization method for financial data sets and access method.

Financial Information/Data Sets	Tool Access	Access Granted	Authorizers/Delegated Authorizers	Comments/References
KFS	*KFS application*	*Role Based*	*FTC/BSC Director or Delegate*	*Via Kuali Security Request tool https://confluence.cornell.edu/x/yo-sC*
KFS	*KFS database*	*CIT developers, tightly integrated systems, web services*	*CIT resource managers*	
KFS Near Real Time	*Direct Connect Accounts*	*All tables, all rows. No row level access roles available.*	*Controller/SFG Rep/Unit Functional and Technical Custodians*	*https://confluence.cornell.edu/x/eoPeD*
KDW	*Direct Connect Accounts*	*Role based via Cynergy (PIAM, KDW Staff Accounting, KDW Staff Labor) Table level access by database role.*	*Controller/SFG Rep/Unit Functional and Technical Custodians*	*https://confluence.cornell.edu/x/eoPeD*
Standard Financial and Web Fin 2 Dashboards	*OBIEE Dashboards*	*Role based via Cynergy (PIAM, KDW Staff Accounting, KDW Staff Labor)*	*FTC/BSC Director or Delegate*	*Via Kuali Security Request tool https://confluence.cornell.edu/x/yo-sC*
Special Financial Dashboards	*OBIEE Dashboards*	*OBIEE group (e.g.Financial Statements, KFS Metrics)*	*FSAID staff members*	*Via security loader file https://www.it.cornell.edu/services/obiee/developers/index.cfm*
OBIEE subject areas	*OBIEE Answers*	*OBIEE Answers group defines subject areas available plus KDW Staff Accounting/Labor roles via Cynergy.*	*FSAID staff members Budget subject area - UBO*	*Access request via kfs-idr@cornell.edu. With setup by CIT ODAA. OBIEE Answers training required.*
OBIEE "Act As" role	*OBIEE Dashboards*	*Delegate acquires permissions of target users the person is "acting as"*	*FTC/BSC Director or Delegate*	*Via proxy loader file https://www.it.cornell.edu/services/obiee/developers/index.cfm*
KDW Local Security	*OBIEE Dashboards, OBIEE Answers*	*Access limited to Orgs identified in Local Security system*	*FTC/BSC Director or Delegate*	*https://confluence.cornell.edu/x/XwTPCw*

KFS = Kuali Financial System, KDW – Kuali Data Warehouse, OBIEE – Oracle Business Intelligence Enterprise Edition

(Reference: *https://www.dfa.cornell.edu/fsaid/getaccess*)

Review and Certification

At least annually, data access for individual users will be reviewed and certified. The financial transaction center/business service center (FTC/BSC) director is responsible to oversee the review, request removal or modification of access, and certify that the process has been completed for each unit. The Annual Certification dashboards provide the tools to perform the review.

Local Security

In the Kuali Data Warehouse (KDW), access granted through the staff accounting role provides access to non-sensitive data across all accounts in all units. Access for individual users can be restricted to align with

business responsibilities to a smaller set of orgs through the Local Security process. Limiting access can be beneficial by limiting the amount of data that will be returned to only that which is of interest to the user, making use of dashboards simpler.

(Reference: https://confluence.cornell.edu/display/KFSIMPL/KDW+Local+Security)

Direct Connect Agreements

Direct Connect agreements define the business purpose, access methods, terms and conditions, governing policies, and tables needed for expanded data access beyond the standard that is provided to regular users. Agreements are signed by functional, technical, and security representatives from the unit, the college business officer, and the financial data steward. If the need or purpose of a Direct Connect agreement changes, a new agreement needs to be defined and approved.

There are two types of Direct Connect agreements for financial data:

1. For an individual NetID, to meet specialized job responsibilities for individual staff members using alternative reporting tools (e.g., Hyperion Interactive Reporting Studio).
2. For a generic user id (non-NetID), when data will be extracted or accessed by another system or through an automated integration.

DFA's goal is to reduce the need for and use of non-central financial systems and data by providing financial information in a centrally controlled environment. However, resource constraints and unique requirements across campus do not always allow unit needs to be met in a timeframe required by the units. Prior to creating external value-added systems, a dialog is encouraged between local units and DFA on any system and data requirements. When practical, DFA will consider modifications and enhancements to central systems to meet other unit needs as efficiently and effectively as possible.

(Reference: https://confluence.cornell.edu/display/kfsidr/KDW+Database+Direct+Connect+Accounts)

Data Access Control for Downstream Systems

To ensure that data access is consistent between central and local data sources, downstream systems that provide access to financial data via batch data extracts or dynamic queries should reference central data access tables to control what data can be accessed by users. If this is technically not possible to accomplish, an exception must be approved describing how the data access subsystem will be kept in sync with central data access, and how certification will be accomplished at least annually. Data access controls must also be approved by the IT Security Office.

Data Access for Application Developers and Project Team Members

When systems are being developed or updated that have close integration with financial systems, it is often necessary that technical staff members and other project team members be granted access to perform their tasks. Ongoing operation of these systems requires technical staff member access for problem resolution and system maintenance. Technical and project staff members may be in CIT, DFA, other central offices or academic units. Because these activities are usually limited in time periods or specific job assignments, the following additional access controls and guidelines are specific to these types of staff members.

- Access should be requested by role rather than for individual people, so that as responsibilities migrate between staff members, the access needs stay with the role rather than follow the person.
- Access will be removed immediately upon leaving a project, a position, or the university.
- Data access reviews will be done quarterly by the supervising unit of the application developers and project team members.
- Access to sensitive or confidential data will be restricted to a subset whenever possible.
- Project managers are responsible for timely provisioning and de-provisioning access for team members during the life of the project.

Following these guidelines will allow a streamlined request process for quick turnaround, so that project staff members can be efficiently on-boarded and system support is not compromised.

Support

System Availability

DFA and CIT have defined a level of service for financial systems. Our goal will be to meet this service level consistently and respond to any problems that result in a reduced level of service in a timely manner. Unplanned outages will be resolved as quickly as possible and reported on the IT Service Alerts page (http://www.it.cornell.edu/services/status.cfm). Communication to campus will occur through the controller-l and kfs-dashboard-l mailing lists.

Kuali Financial System

- KFS will be available during normal business hours (8:00 a.m.-5:00 p.m.), Monday - Friday.
- KFS will be available from 8:00 a.m.-9:00 p.m. on the last day of the month, including Saturday or Sunday IF the last day of the month falls on one of these days.
    - Outages during normal business hours and on the last day of the month will be addressed immediately.
- KFS will generally be available outside of normal business hours with the exception of the daily batch processing window, and, if necessary, during the scheduled maintenance windows.
    - Daily Batch Processing Window: 9:00 p.m.-1:00 a.m. daily, KFS will be down during this time
    - Please see KFS Standard Maintenance Windows for details.

- If KFS will be down during a maintenance window, advance notice will be sent the controller's e-list.
- Outages outside of normal business hours will be addressed, so that KFS is available the next business day.

Kuali Data Warehouse/Oracle Business Intelligence Enterprise Edition

The KDW load schedule is Monday through Friday except holidays. The load is started after the KFS Daily Batch Processing is complete. The load is normally complete prior to start of business the following morning. Weekend loads will be executed when the last day of the month falls on a Saturday or Sunday. The KDW test system will normally be loaded with production data following the regular schedule, but will be used as needed for special testing scenarios. Direct connect userid holders will be notified of changes to the KDW test load schedule.

- The data warehouse and OBIEE dashboards are available during the overnight load window.
- Normal scheduled maintenance on the test and production databases will be communicated in advance.
- Data may sometimes not load due to business needs or technical complications.
- The date of the last load can be found on any financial dashboard in OBIEE.
- Changes in load schedule will be communicated in advance or as soon as determined.

Training and Consulting

Training opportunities for use of financial dashboards and ad-hoc reporting via OBIEE Answers are regularly provided. Support is offered during normal business hours. One-on-one consulting can be arranged by appointment. See http://www.culearn.cornell.edu/ for offerings. Subscribe to the email list controllers-l@cornell.edu to receive notices about system changes that may impact data and other information. To subscribe, send a blank e-mail to CONTROLLERS-L-request@cornell.edu with this word in the subject: join (or contact owner-CONTROLLERS-L@cornell.edu).

Contact

To report problems and for assistance with using financial data or questions contact or kfs-idr@cornell.edu (KDW). KFS system support help requests can be submitted at https://www.dfa.cornell.edu/fsaid/gethelp.