Guiding Principles

Institutional data is a shared resource used to inform decisions that advance the university's mission. The Office of Data, Assessment, and Institutional Research (DAIR) strives to provide the right information to the right people at the right time. To achieve this goal, we will:

- Presume trust of those authorized to access data
- Seek to provide a coherent data experience that minimizes data inconsistencies and duplication of tools/systems
- Not restrict access due to concern of misinterpretation or discovery of inaccurate or incomplete data
- Impose tight restrictions only when there is clear risk of significant harm to the University

DAIR abides by K-State institutional policies and procedures, institutional data policy, federal and state laws and regulations, and the professional statement of ethical principles established by the Association of Institutional Research (AIR). This document supports DAIR's daily operations.

Procedures

I. Dashboard and Tool Access

1. Types of Dashboards and Tools
    a. Internal – Dashboards created for broad faculty and staff use. Access is granted by default to administrators (department heads, deans, and central administrators (VPs, Associate Provosts, etc.)). Access can be granted to other K-State faculty and staff with approval from an individual in this administrator group.
    b. Public – Dashboards available via the web with no restrictions. These dashboards must only contain summary aggregate data and not allow individuals to be identified. Data should only be presented at the college level, not department/plan. Sensitive data will typically be redacted when fewer than 10 cases make up a cell or if the numerator or denominator of a percentage is <5. Final decisions on whether to redact data will be made in consultation with the Chief Data Officer or designee based on additional internal DAIR guidance and consultation with appropriate data custodians and stewards.
    c. Restricted – Dashboards created for a small subset of users and for a particular purpose, or those containing personally-identifiable (PII) information. Initial creation and access must be approved by the applicable data steward(s). Further access can be approved by the initial dashboard requestor in consultation with the data steward(s). Users must have completed relevant training (such as FERPA for student data).

2. Student Access to Dashboards – Access can be granted on a limited basis to undergraduate and graduate student workers with administrator approval. A date when access is to be renewed or removed (up to a maximum of one year) must be supplied.

3. Access Audit – DAIR will automatically remove access rights of users who are no longer employed by the university. Four times a year, DAIR will request that administrators review access for their users and notify DAIR of those who should be removed due to position changes.

II. Data Requests and Release

1. Types of Data Requests
    a. Requests from K-State Faculty and Staff — A data request should be filed through DAIR's website with a clear statement regarding the purpose of data usage.
    b. K-State Student Requests — Documentation is required from a course instructor/faculty advisor to verify that the student needs the data to complete a course/research project. DAIR seeks to assist students in research projects but will determine feasibility on a case-by-case basis. IRB documentation may be required for research projects.
    c. Requests from Outside of K-State
        i. Generally, data requests coming from outside of K-State should be handled within DAIR in consultation with concerned K-State offices and data stewards
        ii. External requests from media should go through K-State's Open Records personnel within the Vice President for Communication and Marketing unit.
        iii. External requests for K-State directory information for individual scholarly research purposes should be redirected to K-State IRB and data stewards
        iv. External requests for K-State directory information for unspecified purposes and from unidentifiable person(s) should go through K-State's Open Records personnel within the Vice President for Communication and Marketing unit.
    d. Upon completion of a data request, the provided file and accompanying documentation used in the request (initial request text, data steward approval, logic/queries/files/data used to create the file, etc.) will be stored in the DAIR file storage system.

2. Assigning Data Requests
    a. For any data request filed directly by a person outside DAIR through DAIR's data request portal, the Chief Data Officer or designee will assign it to the proper staff.
    b. For requests received through email, teams, or other communication, the person who receives the communication will file a data request and then assign the request to his/herself or refer to another staff if needed.

3. General Procedures on Releasing Information
    a. In addition to abiding by Federal law and regulations (e.g., FERPA), the following policies apply when releasing information:
        i. DAIR only releases individual-level information with approval from the applicable data steward.
        ii. DAIR typically provides reports of a summary analytical nature. Operational data needed should be referred to a specific office (e.g., Registrar, Financial Aid).
    b. Confidential data sharing
        i. Data that is not generally available to the public will be shared via the university's file management system. Data should generally not be shared directly via email or email attachment except when it is already publicly available via the K-State website or when the risk is deemed very low by the CDO or designee.
    c. Information to include on all released data/reports as applicable:
        i. DAIR wordmark/title and date the report was provided
        ii. Data source and date(s) data covers
        iii. Filters/aggregations used to create the data fields and data definitions
        iv. For student data at the individual level (only after Data Steward Approval), the following note regarding FERPA regulations will be included: *K-State faculty and staff who acquire person-identity or other confidential data released by DAIR should handle the information with extra caution and be aware that FERPA regulations apply to all data users.*

III. Data Validation and Transparency

DAIR staff will use the following guidelines to ensure data integrity across reports:

1. Source of Truth Reports
    a. These reports shall be reconciled against a data query directly from the source system (KSIS, HRIS, etc.) whenever the data is updated (typically census day). Staff will ensure alignment and consistency across totals and subtotals for fields used in breakdowns, such as: gender, race/ethnicity, full-time, plan/major, department, college, and campus.
2. New Reports
    a. New reports shall be reconciled against source of truth reports, both current and historical, whenever possible. When a source of truth report is not available, staff will query a subset of data from the original data source and manually compare cases to validate the data and logic used in the report.
    b. New reports will be reviewed & approved by at least one additional DAIR staff member and any applicable data steward(s).
    c. If a new report uses data elements new to DAIR staff, DAIR will verify the correct data is used with the appropriate data steward or their designee.
3. Ongoing Reports
    a. Existing reports that apply logic to refreshed data will be checked against prior year and current year totals.
    b. Additions or changes to reports with individual-level data must be approved by the applicable data steward(s).
4. Communicating Errors/Issues
    a. Errors/Issues with the data shall be communicated to DAIR supervisory staff and then to the appropriate data user, data architect, and/or data steward as applicable.
    b. When an error is discovered in production data sources (source systems, databases that use source systems, or specific report/dashboard logic) or when the data has already been published or shared, the error and corrective steps shall be logged in the internal DAIR error tracking tool.
5. Communicating Data Assumptions
    a. When different definitions are used or change across different times/categories reports, footnotes will be provided to explain how and why the data definition is different.

IV. External Reporting and Surveys

1. External Reporting—Each year, DAIR receives numerous surveys from external agencies, publishers, and organizations. DAIR will make the best effort to respond to these external survey requests through a tiered prioritization.
    a. Tier 1 examples: IPEDs, KBOR, AAUP, CDS, USNWR, bond ratings, NIH, NSF—will respond.
    b. Tier 2 examples: Peterson's, CSRDE— generally speaking, will respond.
    c. Tier 3 examples: All other external surveys — may respond if staff time permits.
2. Internal Surveys–DAIR administers numerous surveys of K-State faculty, staff, and students.
    a. Releasing Survey Data — Upon request and on a case-by-case basis, DAIR will release original survey data to K-State internal users for research purposes with approval of the initial survey requestor and applicable data steward.
    b. Survey Confidentiality—DAIR will not release personal identity information of those who participated in K-State surveys except with approval from the applicable data steward.
3. Student Survey Research Projects – DAIR will provide certain assistance to a student's survey research project only on a case-by-case basis and if it is approved by K-State authorities (e.g., data custodian and/or steward, IRB, Graduate School, faculty PI, etc.). The survey must be sent out under the student's own name—DAIR will not distribute a student survey under any institutional title.