NOCCCD Data Management Handbook

Spring 2024

Prepared by NOCCCD Educational Services and Technology

Contents

1. Introduction

Institutional data are valuable resources and are the basis for local, state, and federal programmatic and funding decisions. Having accurate data is essential to decision-making and institutional effectiveness. As a District, one of our goals is to increase the use of data in decision making. That goal cannot be achieved without attention to and work on improving data accuracy and integrity. This handbook describes district-wide practices for the collection, storage, reporting, and use of institutional data in order to achieve the following:

- Improve the security of NOCCCD data, including confidentiality and protection from loss
- Improve the integrity of NOCCCD data, resulting in greater accuracy, timeliness, and quality of information for decision-making
- Improve the understanding of NOCCCD data to ensure users have enough information about the data to record and interpret them correctly and consistently

This handbook is a compliment to *AP 3722 District Data Security Standards for End Users*, which establishes district-wide principles and standards related to data access and security; data integrity; and data use.

1.1. Expectation of Shared Ownership

Shared ownership recognizes the importance of every individual and organizational unit to both positively and negatively impact data integrity, access, and usage across the system. Given the importance of institutional data, all individuals and organizational units must act as caretakers of information on behalf of the District. All NOCCCD employees are responsible for properly handling data within information systems. Sensitive data must always be protected and secured. Knowing how different types of data are classified and following proper information security practices helps ensure the protection and security of sensitive information used by NOCCCD employees and students as well as external partners.

Different employees across the District have duties that provide them with an intricate understanding of the data in their area. Therefore, all employees are expected to bring data problems and suggestions for improvements to the attention of the appropriate data stewards who can then communicate them to a broader group so that system-wide changes can be made. Because of the expertise of employees within their functional areas, individuals and organizational units support correct data access and usage by providing appropriate documentation and training to support data users and are integral to establishing procedures for data management, including data entry and reporting.

1.2. Scope

This handbook applies to all users of NOCCCD data, including, but not limited to:

- All employees at all campuses and locations whose job responsibilities include safeguarding, entering or inputting, retrieving, reporting and/or analyzing institutional data.
- All institutional data contained in any NOCCCD-owned information system. This includes data reported to federal (i.e., U.S. Department of Education) and state organizations (i.e., the California Community College Chancellor's Office). This does not apply to instructor notes, materials, data generated from sponsored research, or personal property of individuals.

2. Data Security Standards

2.2 Information Security Basics (PII, FERPA)

Personally Identifiable Information (PII) is information that either alone or combined could directly identify an individual or make the individual's identity easily traceable[1]. PII includes information that is unique to an individual (Direct Identifier) or can be combined with other information to identify a specific individual (Indirect Identifier) [2]. For purposes of this handbook, PII means an individual's first name or first initial and last name in combination with any one Direct Identifier or any combination of Direct/Indirect Identifiers that permits a person's identity to be reasonably inferred by someone who does not have personal knowledge of the relevant circumstances.

- **Direct Identifiers**: Information that relates specifically to an individual, such as: name, social security number, student or employee id, driver's license number, address, telephone number, username or e-mail address, account number, credit card number, and biometric record (e.g., fingerprints).
- **Indirect Identifiers**: Information that is not unique to an individual but that can be combined with other information to identify specific individuals, such as date of birth, place of birth, mother's maiden name, gender, race/ethnicity, geographic indicator, verification data (pet's name, etc.), and passwords.

The Family Educational Rights and Privacy Act (FERPA) is a Federal law that sets forth requirements to protect the privacy of student education records[3]. FERPA governs: (1) release of these records (known as education records) maintained by an educational institution and (2) access to these records. This law applies to K-12 as well as postsecondary education institutions and any student "in attendance" (regardless of age) as well as former students. Under this law, students have the right to inspect and review their education records maintained by the school; and students have the right to request that a school correct records that they believe to be inaccurate or misleading. Generally, schools must have written permission from the student in order to release any information from a student's education record. However, FERPA allows schools to disclose those records without consent to certain officials with a legitimate educational interest or for compliance reasons. Schools may disclose, without consent, "directory" information, which includes the student's name, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, the most recent previous public or private school attended by the student, and any other information authorized in writing by the student. (NOCCCD BP 5040)[4].

---

[1] OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information (2007). Retrieved from https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2007/m07-16.pdf

[2] Seastrom, M. (2010). Basic Concepts and Definitions for Privacy and Confidentiality in Student Education. Retrieved from https://nces.ed.gov/pubs2011/2011601.pdf

[3] Family Educational Rights and Privacy Act Regulations (2009). Retrieved from https://www2.ed.gov/policy/gen/guid/fpco/pdf/ferparegs.pdf

[4] North Orange County Community College District (2009). BP 5040 Student Records, Directory Information, and Privacy. Retrieved from https://nocccd.edu/files/5040bpfinalrevisedbot-2017-11-28_59859.pdf

2.3 Data Classification System

The District identifies three classification levels based on information's value, legal requirements, sensitivity, and availability to the public. Aggregate information is classified based upon the most secure classification level. That is, when information of mixed classifications exists in the same file, document, or other written form, then the entire file, document, etc. shall be classified at the most secure classification level. For example, a document with both Level 1 – Confidential and Level 2 – General information would be classified as Level 1- Confidential.

- **Level 1 Confidential**: Information used by NOCCCD operations that may contain SSN's, PII, financial, health, or other sensitive data such as passwords that may harm or damage NOCCCD or users if exposed to the public or to unauthorized subjects. Confidential data is intended solely for use within NOCCCD and limited to those with a "business need-to-know". These data must be secured and protected at all times and only authorized personnel may access such data.
  - **Examples of Level 1 Confidential Information**:
    - Social Security Number
    - Driver's license or California identification card number
    - Account number, credit, or debit card number, in combination with the required security code or password
    - Medical information (medical history, conditions, etc.)
    - Biometric information (e.g., fingerprints)
    - Private key (digital certificate)
    - Personal health insurance information (individual policy number, claims, etc.)
    - Personal financial information (tax exemptions, deductions, etc.)
    - Protected health information
    - Law enforcement records (e.g., criminal background check results)
    - Legal information (investigations, attorney/client communication, etc.)
    - Contract information (e.g., sealed bids)
- **Level 2 General**: Other information not specifically protected, but may result in financial loss, legal action, damage to NOCCCD's reputation, or violate an individual's privacy rights if released. General information is vital to NOCCCD operations and not intended for public knowledge or consumption. General classification includes information only for internal use within NOCCCD that must be protected due to proprietary, ethical, or privacy considerations. Examples include Banner ID, alumni information, job applicant information, and student or employee information.
  - **Examples of Level 2 General Information:**
    - Banner ID
    - Student information (address, gender, date of birth, etc.)
    - Employee information (home address, personal telephone numbers, race/ethnicity, employment history, etc.)
    - Alumni information (same as student and employee information)
    - Job applicant information (same as employee information)
    - Donor/patron information (same as employee information)
    - NOCCCD Research (intellectual property)
    - Student directory information - release must comply with AP 5040 and FERPA regulations (student's name, major field of study, participation in officially recognized activities and

sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, the most recent previous public or private school attended by the student)
    - Student educational records - release must comply with AP 5040 and FERPA regulations (grades, GPA, test scores, etc.)
- **Level 3 Public**: Information prepared and approved for the public knowledge and consumption, which is either explicitly defined as public information or intended to be available to individuals both on and off campus.
    - Examples of Level 3 Public Information:
        - Employee information (title; work email address, location, and telephone number; position classification; gross salary)
        - Marketing materials
        - Materials created for public release.

2.4 Standards for Data Ownership

- All District employees are considered data stewards and are responsible for properly handling District data within information systems.
- Managers are responsible for ensuring the information collected in their areas is being stored, used, shared, and retained in accordance with this procedure.

2.5 Standards for Data Collection

- Information collection should only be made where such collections are essential to meet the authorized business purpose and mission of the District. Examples of information collection include web forms, surveys, account creation, payment transactions, etc.
- All District employees should regularly review their data collection procedures and purpose to determine whether it is still relevant and necessary for the District's business. Regular review should take place each semester at a minimum.

2.6 Standards for Data Storage

- All District employees should use an NOCCCD-managed secure storage system as their primary data storage location. The Information Technology department at each campus shall define and manage the primary secure storage system for their site.
- Data from the Level 1-Confidential category should always be stored in an NOCCCD-managed secure storage system. Level 1-Confidential information should never be stored outside of the NOCCCD-managed secure storage system, such as on a personal hard drive, removable media (USB Drive), personal cloud storage, etc.
- Data from the Level-2 General categories may only be stored on removable media (e.g., USB Drive, personal cloud storage, external hard drive, etc.) for specific business purposes and need to be encrypted.

2.7 Standards for Data Use and Transmission

- All District employees should perform day-to-day work using the minimum appropriate level of information. For example, if work only requires Level-2 General information, do not include Level 1-Confidential information in the task.
- All District employees should use a secure connection to access institutional information systems (e.g., Banner, Argos).

- All District employees should use an NOCCCD-managed secure storage system to transmit and share Level 1-Confidential and Level-2 General data with other authorized users. Level 1-Confidential and Level-2 General information may also be shared using other electronic transmission (e.g., email) so long as the file is encrypted and/or anonymized (PII removed from the file).

2.8 Standards for Data Retention

- All District employees should regularly review their holdings of previously collected Level 1-Confidential and Level-2 General information to determine whether it is still relevant and necessary for the District's business purpose. Regular review should take place at a minimum of once per semester.
- All District employees should delete and/or anonymize (remove PII from the file for long-term storage) any electronic records no longer necessary for the District's business purpose.
- Federal, state, or other programs, including various student aid or grant programs, may require longer retention periods and such program requirements shall take precedence over the requirements contained herein.

2.9 Standards for Data Sharing and Data Agreements

- Third parties who will access Level 1-Confidential or Level 2-General NOCCCD information to perform a service will sign the NOCCCD Confidentiality and Nondisclosure Agreement and return to the Vice Chancellor of Educational Services and Technology before gaining access to such information.
- Third parties interested in requesting NOCCCD data for research and educational program improvement purposes should enter into a data-sharing agreement specifying the data need, data purpose, method of secure information transfer (e.g., secure ftp server), and plan for reliable and secure data storage and destruction.
- All shared information shall remain the property of NOCCCD and shall not be disclosed to any outside institution or individual not specifically mentioned in the NOCCCD Confidentiality and Nondisclosure Agreement and/or Data-Sharing Agreement.

4. MIS Data Management

4.1 Overview of MIS System

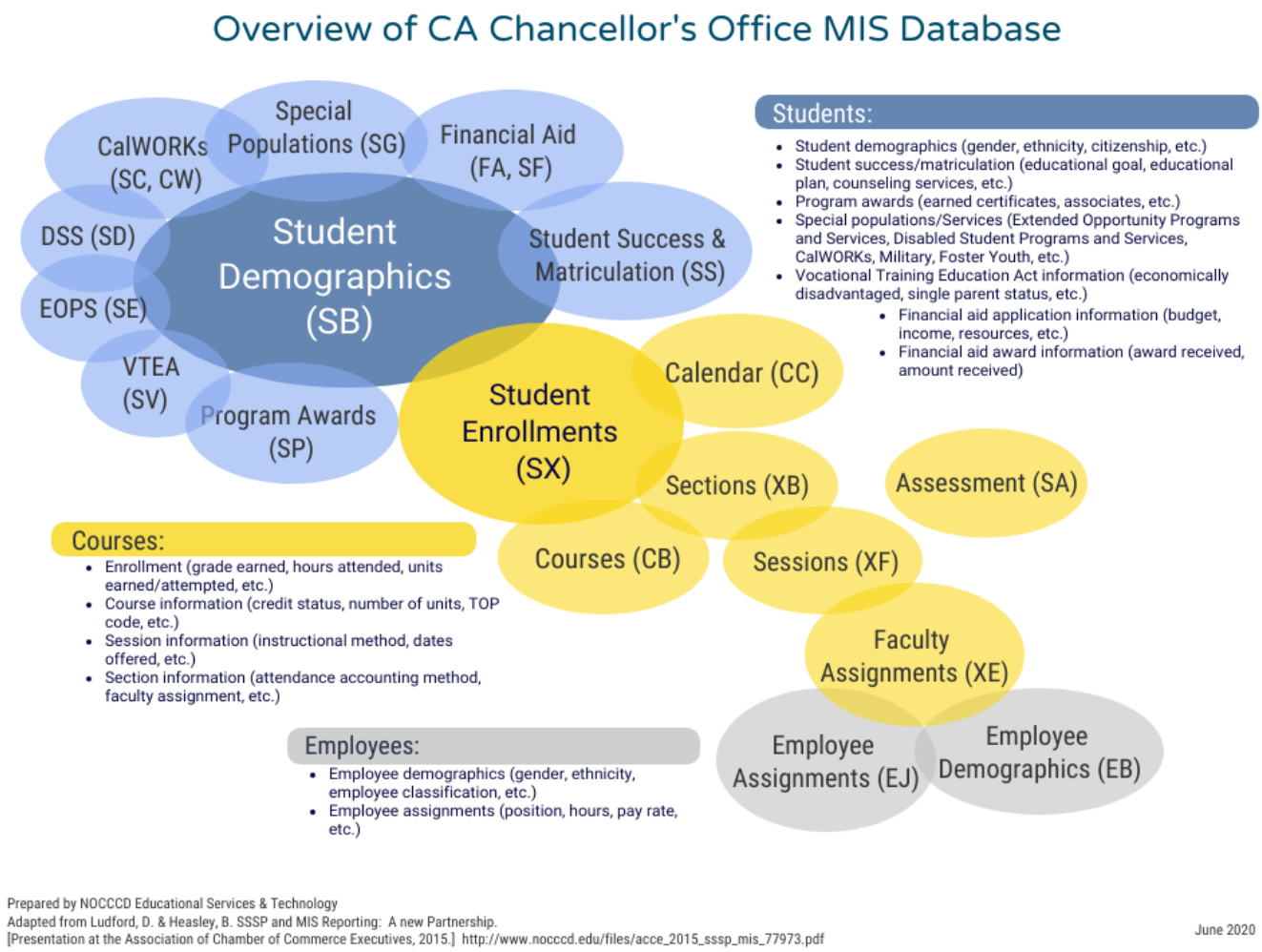
The Chancellor's Office Management Information System (MIS) is a data system designed to collect and report on information about California's community colleges. Each college is responsible for submitting information about students, courses, programs, and employees on a semester and/or annual basis. According to the California Community Colleges Chancellor's Office (CCCCO), the MIS system is designed to provide 1) accountability, 2) data integration, 3) data quality, 4) longitudinal tracking, and 5) flexibility.[5] MIS data are used to monitor and fund a variety of state initiatives, including the California Adult Education Program (CAEP), Strong Workforce Program (SWP), the Student Success and Support Program (SSSP), the Student Equity and Achievement Program (SEA), and the Student-Centered Funding Formula (SCFF). Because of these and other direct uses of MIS data, it is essential that the data reported to the Chancellor's Office are accurate and complete.

The MIS system houses a collection of inter-related databases encompassing the following areas:[6]

- **Students Demographics and Outcomes**:
  - Student demographics (gender, ethnicity, citizenship, etc.)
  - Student success/matriculation (educational goal, educational plan, counseling services, etc.)
  - Enrollment (grade earned, hours attended, units earned/attempted, etc.)
  - Program awards (earned certificates, associates, etc.)
  - Special populations/Services (Extended Opportunity Programs and Services, Disabled Student Programs and Services, CalWORKs, Military, Foster Youth, etc.)
  - Vocational Training Education Act information (economically disadvantaged, single parent status, etc.)
- **Financial Aid**:
  - Financial aid application information (budget, income, resources, etc.)
  - Financial aid award information (award received, amount received)
- **Courses:**
  - Course information (credit status, number of units, TOP code, etc.)
  - Session information (instructional method, dates offered, etc.)
  - Section information (attendance accounting method, faculty assignment, etc.)
- **Employees:**
  - Employee demographics (gender, ethnicity, employee classification, etc.)
  - Employee assignments (position, hours, pay rate, etc.)

[5] California Community Colleges Chancellor's Office. (2000, October 1). *MIS database design overview*. Retrieved from https://www.cccco.edu/-/media/CCCCO-Website/Files/DII/x_Chart.pdf?la=en&hash=0DEF29FA51817111DE0EB79DBBE2C54BF10B2A04

[6] California Community Colleges Chancellor's Office. (2019). *Data element dictionary*. Retrieved from https://webdata.cccco.edu/ded/ded.htm



4.2 MIS and CCFS-320 in the Student-Centered Funding Formula

The Student Centered Funding Formula is designed to fund California community colleges, at least in part, on how well their students are achieving the goals of the system. The SCFF attempts to link districts' financial planning more explicitly with student success by allocating a percentage of funding to attainment of specific metrics, rather than basing budgets entirely on full-time equivalent student (FTES) enrollment. The SCFF calculates funds for California community college districts based on three major categories of data:

1) Base Allocation: FTES enrollment;
2) Supplemental Allocation: Low-income student enrollment (California College Promise Grant, Pell grant, and AB 540 students); and
3) Student Success Allocation: Number of students successfully completing certain achievement outcomes (e.g., awards, transfer-level courses, etc.), plus additional funds for each low-income student achieving these outcomes.

Beginning with the 2018-19 academic year, all California Community Colleges will either be paid according to the new funding formula, or at their 2017-18 FTES funding level, plus COLA, whichever

value is higher. As of 2021-22, all CCCs will only be paid according to the SCFF formula. This is referred to as the "hold harmless period."

Having accurate data has always been important. However, now SCFF funding requires accurate reporting within an additional 27 categories of information, generating over $2 billion dollars in revenue.[7] Once the hold harmless period is over, about 30 percent of the funding allocation to CA community college districts (approximately $60 million dollars for NOCCCD)[8] will be coming from the supplemental and student success areas of the SCFF. **MIS data are used to calculate most metrics included in these allocations.** Appendix A describes the SCFF metrics and related data elements in detail.

4.3 Role of MIS Workgroup

The MIS Workgroup is comprised of the Chancellor, Vice Chancellor of Educational Services and Technology, Vice Chancellor of Finance, CEOs, Directors of Institutional Research and Planning, and the District Director of Fiscal Affairs. The primary responsibilities of the workgroup include the following:

- Develop and oversee the implementation of data management policies and procedures
- Solicit input and review from data stewards on data management policies and procedures
- Make recommendations regarding changes to procedures, processes, and systems to improve the collection and application of data
- Establish regular communication with data stewards and leadership positions across and between all NOCCCD institutions regarding MIS and 320 data collection, reporting, and use
- Facilitate initiatives to improve the quality of institutional data
- Help identify and resolve data quality issues and other recurring errors
- Streamline and automate data systems for collection and reporting
- Provide necessary data-related training for data entry, collection, and reporting of institutional data

4.4 MIS Workflow

4.4.1 Data Set-up & Collection

At the start of every term or academic year (depending on the cycle of data), the Responsible and Accountable parties within each functional area review the relevant local NOCCCD data codes compared to the corresponding MIS data elements. If discrepancies are noted, code updates are made in the student information system (or appropriate data system), relevant data entry documentation is adjusted, and changes are communicated to the IS Data Quality Analyst to adjust reporting queries and/or modify information system processes.

When the CCCCO initiates major changes to data elements, the District Director of Enterprise IT Applications Support and Development and IS Data Quality Analyst communicate the changes to the relevant functional areas and develop a plan for modifying the information system and reporting

[7] California Community Colleges Chancellor's Office (2020, February 25). *Fiscal & policy update: A bi-monthly webinar series by the College Finance and Facilities Planning Division*. https://www.cccco.edu/About-Us/Chancellors-Office/Divisions/College-Finance-and-Facilities-Planning/Fiscal-and-Policy-Updates

[8] California Community Colleges Chancellor's Office (2020, February 20). *California Community Colleges 2018-19 recalculation apportionment*. https://www.cccco.edu/-/media/CCCCO-Website/College-Finance-and-Facilities/Apportionments-2020/fy2018-19recalculationapportionmentexhibitc-a11y.pdf

processes accordingly. Depending on the magnitude of the change, processes might take six months to a year to implement. Once implemented, documentation is modified accordingly.

Throughout the year, data are collected via internal processes on a regular basis (mostly as part of the "everyday" work of the functional area).

4.4.2 Data Integration

The majority of institutional data reported to state and federal agencies are collected and stored in the Banner Student Information System. However, some data are collected and stored in supplemental information systems due to differences in data collection processes (e.g., paper applications, manual attendance tracking for noncredit courses, etc.). Processes are in place to import the data from these external systems into Banner so that they can be queried for institutional reporting. On a term-by-term basis, the IS Data Quality Analyst receives and processes files from supplemental systems and uploads them into appropriate Banner tables. The District Director of Enterprise IT Applications Support and Development and his team are responsible for maintaining and upgrading these systems as needed.

4.4.3 Report Generation

The District Information Services department, specifically the IS Data Quality Analyst, is responsible for generating and submitting MIS files to the Chancellor's Office. The IS Data Quality Analyst runs extract file processes from Banner to populate the files needed. He then prepares the files for submission by running checks on issues relating to formatting, special characters, etc. and then submits the file to the CCCCO submission system.

4.4.4 Error Review/Validation

Each CCCCO file submission results in an error log, which has record-level details about any errors in the file. Errors fall into the following categories:

- **Field Check:** The value submitted is invalid for the field. For example, a student's birthdate may not be less than zero or greater than 115.
- **Referential Error**: Related values are compared against one another. For example, a section coded as positive attendance (XB01) must have attendance hours (XB11) coded as "8888."
- **Integrity Check**: Values are evaluated for logical consistency. For example, a student may not have an unknown educational goal (SS01) if they have developed an Educational Plan (SS09).
- **Data Quality Check**: An overall evaluation of the file to ensure that minimum data standards are met and large amounts of unknown data are not submitted. For example, if more than 70% of Student Educational Goals (SB14) are unknown, the entire Student Basic file will be rejected.

The Business Analyst-EST distributes the error files to responsible positions at each campus (MIS Analysts, Program Directors, etc.) who then review the error logs and correct all errors possible. Once reviewed, the responsible parties clean up the data in Banner and notify the Business Analyst-EST of corrections made and/or request that some records be removed in order to resubmit MIS files to the Chancellor's Office. This is an iterative process between Educational Services and Technology, District Information Services and campus data stewards that repeats until all files can be submitted to the Chancellor's Office without any errors.

4.4.5 Data Submission

Once all errors have been reviewed and corrected, the Business Analyst-EST submits cleaned and reviewed files to the CCCCO production system. For term-end files, the initial submission must be completed within one month after the end of each term. (Although the Fall term due date is the first Monday in February.) The last day to resubmit for (i) categorical and SSSP allocation purposes is the first Monday in August, and (ii) financial aid data for Vocational and Technical Education Act (VTEA) allocation purposes is the second Friday in February. Annual files have different submission dates, but are generally due in the fall following the relevant academic year.

5. Data Integrity

5.1 Issue Resolution Process

Issues are brought to the attention of the MIS Campus Analysts first and are resolved locally, when possible. If any issues arise that require help to resolve outside the local context, District IS (Banner processes) and Educational Services and Technology (data management procedures) provide support.

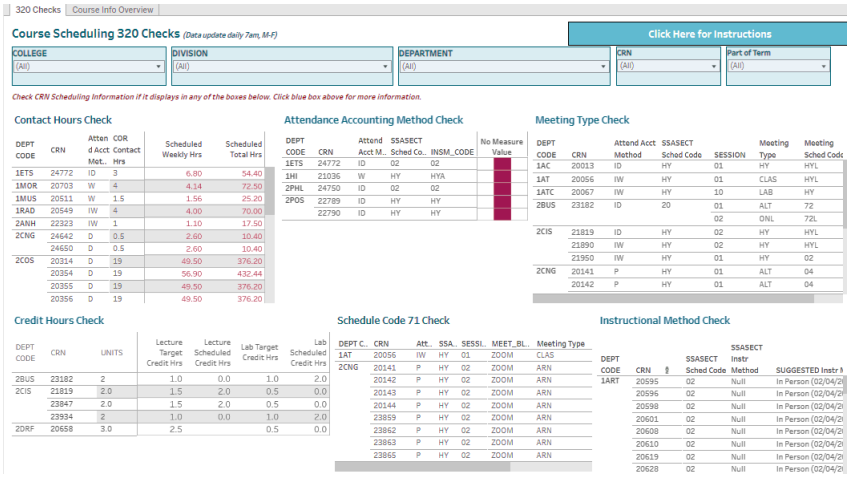
5.2 Post-submission Review Process

After each MIS submission, the District Director of Research, Planning, and Data Management convenes the MIS Campus Analysts, the IS Data Quality Analyst, and the Business Analyst-EST to discuss the process and any associated errors. When there are errors that relate to a Banner process/code or a data management issue, the group discusses and plans to resolve before the next submission.

6. Ongoing Monitoring of Data Quality

6.1 Process

For course schedule-related data, the District Director of Research, Planning, and Data Management publishes a Tableau dashboard every semester highlighting course sections with potential code mismatches or errors for MIS and 320 reporting. An example dashboard is presented below. Schedule inputters and deans review the dashboard data and make corrections at certain points throughout the year – before the schedule is published, before students register for classes, and before the 320 reports are submitted.



Appendix A: Policies and Procedures for Data Standards and Security

1. AP 3722 District Data Security Standards for End Users: 3722apnewadopteddcc-2022-05-23_27874.pdf (nocccd.edu)
2. BP 5040 Student Records, Directory Information, and Privacy: https://nocccd.edu/files/5040bpfinalrevisedbot-2017-11-28_59859.pdf
3. AP 5040 Student Records, Directory Information, and Privacy: https://nocccd.edu/files/5040apfinalreviseddcc-2019-04-22_63988.pdf
4. BP 5800 Prevention of Identity Theft in Student Financial Transactions: https://nocccd.edu/files/5800bpfinalbot02-08-11_88000.pdf
5. AP 5800 Prevention of Identity Theft in Student Financial Transactions: https://nocccd.edu/files/5800apfinalc-cabinet8-22-11_88004.pdf
6. BP 3310 Records Retention and Destruction: https://nocccd.edu/files/3310bpfinalrevisedbot-2019-11-26_33051.pdf
7. AP 3310 Records Retention and Destruction: https://nocccd.edu/files/3310apfinalreviseddcc-2019-10-28_62704.pdf
8. NOCCCD Information Services Training Procedures and Materials: http://nocccd.edu/training-and-training-materials
9. NOCCCD Information Services Presentations and Guidelines: https://www.nocccd.edu/presentations-and-guidelines
10. Cloud Solution Security Measure Guidelines: https://www.nocccd.edu/files/cloud-solution-security-measure-guidelines-tcc-approved-10-17-17_57777.pdf
11. Mobile Computing Device Guidelines: https://www.nocccd.edu/files/mobile-computing-guidelines-dcc-approved-01-22-18_29027.pdf
12. SSSP and MIS Reporting: A new Partnership: http://www.nocccd.edu/files/acce_2015_sssp_mis_77973.pdf