



POLICY DIRECTIVE

Policy:	DOC 1.7.3 DATA QUALITY
Effective Date:	04/26/2007 Page 1 of 2
Revision Date(s):	08/26/2019; 04/24/2026
Signature/Title:	/s/ Eric Strauss, Director

I. POLICY

Department and state-owned Information Technology resources are used to provide information, both internally and externally, that is vital for operations, budgeting, and public safety. The quality of that information is the responsibility of every employee.

II. APPLICABILITY

All Department divisions, facilities, and programs.

III. DEFINITIONS (see Glossary)

IV. REQUIREMENTS

A. General Requirements

1. Staff will use the *Information Systems Change Request* maintained by Department IT to request any change to a production platform and service provided by IT.
2. Designated Department staff serve on committees related to the maintenance of data quality and related production platforms and services, including but not limited to the change management committee, consisting of administrators who set priorities regarding requested changes and approve or deny requests.
3. Individuals who enter or maintain data in the offender management system will follow *DOC 1.5.5 Offender Records Management, Access, and Release* and this policy.
4. For information not entered into the offender management system, such as medical and mental health records or administrative information, each administrator is responsible for ensuring that data quality is maintained by relevant staff through procedures, training, management tools, or any other appropriate method.
5. Administrators are responsible for maintaining public records and implementing retention schedules in accordance with *DOC 1.2.7 Inventories and Public Records Management*.
6. Staff who violate this policy may be subject to disciplinary action, up to and including termination in accordance with *DOC 1.3.2 Employee Performance and Conduct Guidelines*.

B. Data-Related Responsibilities

1. Administrators will ensure that staff are assigned roles and permissions necessary for their data-related functions, receive adequate training to perform those functions, and are held accountable for maintaining data quality.
2. Each staff member who enters, modifies, or deletes data is the data owner and is responsible and accountable for the completeness, accuracy, and timeliness of the data that they handle.

3. Data owners will:
 - a. enter information in a timely manner;
 - b. verify the accuracy of the information entered;
 - c. check for spelling and transposition errors;
 - d. check data for reasonableness (for example, offenders are unlikely to be 377 years old);
 - e. review data that was entered by others for obvious errors;
 - f. report errors they find but are unable to correct to the IT Service Desk;
 - g. verify they are not creating a duplicate record;
 - h. not violate the intent of data fields (for example, putting data in the wrong data fields);
 - i. enter data correctly into data fields (for example, applying the rules);
 - j. correct errors of which they are made aware;
 - k. restrict data entry to records pertinent to their area of responsibility;
 - l. keep their knowledge of the systems current by attending training; and
 - m. ask “how to,” “what to,” or “where to” if in doubt about any data entry issues.
4. Data stewards will monitor data entered by staff, ensure that corrective actions are prepared and executed as appropriate, and recommend or take appropriate management or disciplinary action to ensure data quality.

V. CLOSING

Questions about this policy should be directed to the Department Chief Information Officer (CIO).

VI. REFERENCES

- A. 2-15-112, MCA
- B. *DOC 1.3.2 Employee Performance and Conduct Guidelines*