UNITED STATES

ENVIRONMENTAL PROTECTION AGENCY

Office of Mission Support (OMS)

Central Data Exchange (CDX) Rules of Behavior

VERSION 2.7

October 2025

Section 1. **Introduction**

Rules of behavior inform users of an information system, of the basic actions required of them to ensure that their activity supports the security processes and procedures designed to protect the system and information that it processes. Rules of behavior must also be linked with consequences for not complying with and/or intentionally violating the rules. This approach, required by federal policy, holds users responsible for their actions. In addition, users are called to act ethically, take initiative, and accept responsibility for safeguarding information resources.

This document provides requirements for rules of behavior for information users of the Environmental Protection Agency's (EPA) Central Data Exchange (CDX) as required by Appendix III to Office of Management and Budget (OMB) Circular No. A-130; and further discussed in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18 Rev 1, Guide for Developing Security Plans for Information Technology Systems.

Some CDX roles provide the ability to access CDX end user registration data in order to grant and assign access rights and roles to CDX users. One such role is Registration Maintenance Account Manager (RMAM). Each RMAM user shall be authorized and assigned RMAM privileges by specific dataflow, specific dataflow access right, and specific dataflow role for granting CDX users access privileges. RMAM users must ensure that CDX and registration data are protected from loss, misuse, unauthorized access to, or unauthorized modification of information. CDX registration data requires robust levels of protection since it includes a substantial amount of sensitive data.

Section 2. **CDX Rules of Behavior**

The rules detailed in this section govern the use of CDX information and system resources in conjunction with the CDX Terms and Conditions, which apply to all CDX account holders, and EPA's National Rules of Behavior (NROB), which apply to all EPA employees and contractors who use EPA information or systems in support of EPA operations and assets. The CDX rules of behavior apply to all personnel using CDX development, pre-production, and production information and system resources in support of the CDX program. Since CDX is an EPA information system, the CDX Rules of Behavior are considered an addendum to EPA's NROB. Thus, when agreeing to follow the CDX Rules of Behavior, CDX personnel are also agreeing to follow EPA's NROB. The NROB is available for review at https://www.epa.gov/system/files/documents/2024-04/information_security_epa_national_rules_of_behavior.pdf. The CDX Terms and Conditions are posted for review prior to CDX login at https://cdx.epa.gov/Terms.

When in doubt about whether or how a rule applies to any action you are taking or thinking about taking, please ask your manager, CDX Security, CDX Help Desk, and/or the CDX Information System Security Officer (ISSO) for clarification. Contact information for the above parties is provided in Appendix A.

AUTHORIZED USE AND ACCESS

CDX users must access EPA computer systems and information for official business only as described in EPA's NROB.

1. Only use data for which you have been granted authorization in accordance with the CDX Registration procedures.
2. If you are unsure of a requester's right to access data, contact the CDX Help Desk, CDX Security, or the CDX ISSO.
3. Abide by procedures governing the requesting/disseminating information as contained in the application data flow registration procedures. For further details, view the online CDX Frequently Asked Questions (FAQs) for additional details on your specific application data flow.
4. If you do not have access rights as described for your application data flow, then do not attempt access. If you are unsure, contact the CDX Help Desk or the CDX ISSO.
5. Follow approved procedures for acquiring/granting access rights to CDX and other non-CDX EPA systems. The granting of access is to be governed by the Principle of Least Privilege. A user is only granted the minimum necessary rights to perform their job function.
6. Use CDX access control/security software when authorizing new user access and to verify security configurations in accordance with procedures for the CDX Help Desk.
7. Always exit from the CDX application or system logon when leaving your PC for any period of time.
8. No connection of systems to CDX or the transfer of CDX data to other systems is authorized beyond that already established as authorized for CDX or through the CDX project office's authorization process.
9. Abide by the CDX Warning Notice provided at: https://cdx.epa.gov/PrivacyNotice.

ACCESS / IDENTITY PROOFING BY RMAM USERS

1. Only one Registration Maintenance account per RMAM user is allowed.
2. RMAM users shall be responsible for validating the identity of their prospective CDX users before adding or deleting access privileges to their CDX accounts.
3. RMAM users shall only be allowed to provide CDX users access to the dataflow(s) with permissions for which they have authorization.

ACCOUNTABILITY

CDX users must be accountable for their actions and responsibilities related to information resources entrusted to them.

1. Each CDX user is required to maintain unique login credentials in order to appear uniquely identifiable. All actions will be logged, and users will be held accountable for their actions.
2. Do not attempt to subvert or override internal controls or to perform access where privileges have not been authorized. For RMAM users, this includes CDX controls as well as Registration Maintenance controls.
3. Users and managers must ensure new access requirements are promptly identified, authorized, and documented.

4. Users and managers must ensure that changes to, or termination of, access requirements are promptly identified, authorized, and documented. RMAM users must follow approved procedures for granting access rights.
5. Ensure that no one person has sole access to or control over important critical or highly sensitive information resources including the CDX System Security Plan and CDX operational data and guidelines.
6. Log off CDX when not in use.

CONFIDENTIALITY

CDX users must protect confidential information from disclosure to unauthorized individuals or groups.

1. Ensure that confidentiality procedures are defined and are followed if confidential data exists within a CDX application data flow.
2. Users are subject to Section (i) (1) Criminal Penalties, under 5 U.S.C. 552a, the Privacy Act of 1974. Registration Maintenance data resources shall be used in an appropriate manner that comply with all applicable federal, state, and local statutes.
3. Store hard copy reports, containing confidential information, in a locked room or cabinet. Likewise, do not display nor allow sensitive information to remain on your screen when an unauthorized person is present.
4. Do not allow unauthorized or unescorted personnel into an area where confidential information is processed. If unsure of person's authorization, contact either CDX Security or the CDX ISSO.
5. Ensure that access to confidential information, contained in system output, fax transmissions, printouts, and removable media, is controlled in accordance with EPA CIO procedures.
6. Label and lock up storage media/hard copy containing confidential information at the end of the day, and when otherwise unattended. Except for Electronic Signature Agreements that are submitted to the CDX Data Processing Center on paper, do not print or store registration data on paper or electronic media other than user ID and user's name.
7. Erase or dispose of confidential information, if applicable, prior to reusing or disposing of media according to EPA procedures.
8. Do not disable any encryption established for Internet and Web browser communications with CDX applications.
9. When Controlled Unclassified Information (CUI), including Confidential Business Information (CBI), is transported through and/or stored on CDX, ensure proper technical controls and procedures are in place to maintain adequate security over the data.
10. Do not provide non-public information about one vendor or contractor to another vendor or contractor.
11. RMAM users shall use the following means (#12-15) to safeguard Registration Maintenance data:
12. Do not store registration data on personal computers.
13. Restrict access to computers that are logged into CDX (i.e., authenticated logins and screen savers, locked offices, etc.).
14. Only transmit registration data across the network in a secure manner (i.e., to secure web servers using data encryption with login credentials transmitted via Transport Layer Security).
15. Do not publish, post, or release any information that is considered confidential or not public on social media or public websites. If you are not sure what information is

considered confidential or not public, contact the CDX Help Desk, CDX Security, or the CDX ISSO.

INTEGRITY

CDX users must protect the integrity and quality of information.

1. Discontinue use of any computer or software that shows indications of being infected with a virus. Obtain assistance immediately. Contact the CDX Help Desk and follow CDX Incident Response procedures as soon as possible.
2. Never enter unauthorized, inaccurate, or false information that is not for authorized testing purposes and ensure all data integrity is retained.
3. Only use specifically designated and/or specially designed test data for use in system tests. Do not use Production database data. If in doubt, check with the CDX Operations Manager and the Configuration Control Board (CCB) for additional details on test data and proper backup procedures.
4. Create or modify only records or files as authorized in your assigned duties.
5. When known or suspected unauthorized changes are made, if time and conditions permit, make backups to capture the altered environment as a record for possible future reference, system recovery, and/or legal evidence.

LOGIN CREDENTIALS

CDX users must protect information through effective use of login credentials.

1. Never share your login credentials (including user ID, passwords, authentication codes from SMS or apps, security keys, PIV cards, or backup codes) with anyone.
2. CDX is not responsible for account recovery/relinking should you delete or lose access to your login credentials.
3. As an organizational user, logging in via Enterprise Identity and Access Management (EIAM) with a PIV card, you will need to contact the Enterprise IT Service Desk (EISD) for assistance.
4. If your account is configured to login via Login.gov, loss or deletion of your Login.gov account will render your associated CDX account defunct, and relinking with a new Login.gov will not be an option. Thus, it is strongly recommended that you set up more than one authentication method in your Login.gov account.
5. If a person with access to credentials for an account used for testing or running system services is terminated or transferred from CDX support duties, change the account's login credential immediately.
6. If your CDX credentials become known to anyone, change them immediately, and contact the CDX Help Desk to report a security incident.
7. If a Development, Test, or Administrator account's login credential has been compromised, contact the CDX Operations and CDX Security teams immediately, and report a security incident.

HARDWARE / SOFTWARE

CDX users must use hardware and software in a safe manner that protects both from damage and abuse.

1. Do not use hardware or software, purchased by EPA, on computers other than EPA computers or computers on the CDX contract.
2. Ensure custom designed software does not contain unknown access mechanisms through review, test, and acceptance procedures.
3. Do not install software without first having run a virus scan on it.

AWARENESS AND REPORTING

CDX users must stay abreast of security policies, requirements, and issues and report security violations and vulnerabilities to proper authorities.

1. Be alert to security issues, technical vulnerabilities, possible security incidents, and violations of EPA policy and rules of behavior.
2. If you have questions about the appropriateness of an action or activity, first discuss it with your supervisor, CDX Security, or the CDX ISSO.
3. Be alert to human factors that may indicate a security risk.
4. Challenge unauthorized personnel in the work area.
5. Be alert to clues of abuse, including but not limited to:
    a. Unauthorized computer products in the office (e.g., games, sports pools, personal business software).
    b. Possession of unauthorized equipment.
    c. Unscheduled or unknown programs running on a recurring basis.
6. It is each user's responsibility to report any form of security violation, whether it is fraud, waste, abuse, or unethical behavior.
7. When security violations occur or are suspected, or when you do not know what to do in a specific situation, promptly contact the CDX Help Desk, CDX Security, or the CDX ISSO. If unable to reach any of the above, call the Enterprise IT Service Desk. Contact information is listed in Appendix A.
8. Report any known or suspected security incidents. Examples include:
    a. Unauthorized computer products in the office (e.g., games, sports pools, personal business software).
    b. Computer viruses
    c. Phishing and social engineering attempts
    d. Lost or stolen laptops, phones, or other equipment
    e. Unexplained occurrences (e.g., unexpected account disabled, email you did not send, etc.)
    f. Sharing login credentials or user IDs
    g. Loss, modification, or unauthorized disclosure of confidential information
    h. Unauthorized access to information, systems, or applications
    i. Lack of expected controls (e.g., unlocked doors, confidential information left unprotected)
9. Take reasonable action immediately upon discovering a violation to prevent additional damage, such as logging out of a terminal or locking up property.
10. Cooperate willingly with official action plans for dealing with security violations.

PRIVILEGED USERS

CDX Privileged users must perform their duties meticulously and reliably in order to preserve information security.

Privileged users include System Administrators, RMAM, HelpDesk, and Database Administrators

1. Protect the administrator or root login credentials at highest level demanded by the sensitivity level of the system or personnel requirements per CDX operational procedures.
2. Do not use Agency or CDX equipment for unofficial government purposes. Prior to introducing programs to the Production environment, test them in an environment isolated from the Production environment.
3. Provide appropriate on-board training for users and their roles.
4. Be aware when the same personnel are responsible for several areas of a system. This scenario could be an opportunity for abuse. Ensure separation of duties.
5. Implement applicable security access procedures and mechanisms, incorporate appropriate levels of system auditing, and review audit logs.
6. Privileged users must make an effort to notice the threats to and vulnerabilities of information systems, calling these to the attention of management and working to develop effective countermeasures.
7. System developers must adhere to sound development practices in the development process. That is, software must be designed and programmed to perform accurately according to user requirements.

PUBLIC ACCESS SYSTEMS

CDX administrators must conduct only legitimate business through public access systems according to authorized procedures.

1. Use public access systems for authorized purposes only.
2. Do not transmit confidential information across public access systems, unless properly authorized and using approved encryption technology.
3. Encrypt sensitive, non-public information stored on or transmitted across public access systems.
4. Place only mission-oriented public information on an EPA public access system, including Internet Web pages, e-mail systems, and social media.
5. Never use government information resources to gather information from a public access system for personal gain.
6. Get official approvals for any Web pages placed on the Internet.
7. Ensure that information placed on a public access system is up-to-date and accurate.
8. Ensure that information placed on a public access system reflects the policies and positions of EPA.
9. Ensure information placed on public access systems cannot be changed or altered unless authorized.
10. Do not distribute, post, or receive documents via public access systems in violation of copyright laws.
11. Designate a contact person, with contact information, on each Internet page.
12. Update e-mail distribution lists as frequently as needed and at least once per year.

13. Check hypertext links routinely to ensure they are up-to-date and accurate.
14. Protect copyrighted software and information in accordance with the conditions under which it is provided.
15. Adhere to the NROB's social media guidelines.

USERS OF PERSONALLY IDENTIFIABLE INFORMATION

CDX users with access to Personally Identifiable Information must acquire and use personal information only in ways that respect an individual's privacy as described in the NROB.

1. Do not improperly alter or destroy personal information.
2. Ensure that your personal information is kept accurate, timely, complete, and relevant to its purpose.
3. Only acquire and keep personal information to support current or planned activities or required by law.
4. Provide information to those from whom personal information is collected in accordance with Privacy Act provision in the System of Records.
5. Protect confidentiality and integrity of personal information through appropriate technical and managerial controls.
6. Never use personal information in any way that is incompatible with the provider's understanding of its use.

CONSEQUENCES OF NON-COMPLIANCE

Violations of rules of behavior can, depending on the severity and type of the violation, at the discretion of management, through administrative processes and/or through the due process of law, include suspension of access privileges, reprimand, suspension, demotion, removal, or criminal and civil penalties, including prison terms and fines, if a law was violated.

Unauthorized access, use, misuse, or modification of government computer systems constitutes a violation of Title 18, United States Code, Section 1030.

Appendix A. Security Resources

The following points of contact exist for answering questions about the CDX Rules of Behavior and supporting CDX security activities:

- CDX Security: SecuritySolutions@cgifederal.com
- CDX Information System Security Officer: Sileshi Desta, 202.564.0378, desta.sileshi@epa.gov

To report security incidents or concerns:

- CDX Help Desk: 888.890.1995
- CDX Security: SecuritySolutions@cgifederal.com

If none of the above contacts are available, and the situation warrants immediate action (e.g., security violation), contact:

- Enterprise IT Service Desk: 866.411.4EPA (4372), Option 1
- EPA Office of Mission Support (OMS) Information Security Officer (ISO): Bill Sabbagh, 202.566.9859, sabbagh.bill@epa.gov

Appendix B. Abbreviations and Acronyms

The following acronyms and terms are used in this document:

Acronym / Term	Definition
CBI	Confidential Business Information
CCB	Configuration Control Board
CDX	Central Data Exchange
CUI	Controlled Unclassified Information
EIAM	Enterprise Identity and Access Management
EISD	Enterprise IT Service Desk
EPA	Environmental Protection Agency
FAQs	Frequently Asked Questions
ID(s)	Identification(s)
ISO	Information Security Officer
ISSO	Information Systems Security Officer
NIST	National Institute of Standards and Technology
NROB	National Rules of Behavior
OMB	Office of Management and Budget
OMS	Office of Mission Support
PC	Personal Computer
PII	Personally Identifiable Information
RM	Registration Maintenance
RMAM	Registration Maintenance Account Manager
ROB	Rules of Behavior
SP	Special Publication