U.S. Environmental Protection Agency
Office of Mission Support (OMS)

Rules of Behavior - Shared CROMMER Services (SCS) and Partner Help Desk

Shared CROMERR Services (SCS) credentials allow Exchange Network Partners to develop and test applications integrating CROMERR services for environmental information exchange.

Partner help desk dataflows and roles in SCS provide Account Manager Users the ability to access SCS end user registration data in order to grant and assign access rights and roles to SCS users**.** Each Account Manager user shall be authorized and assigned particular privileges within their partner help desk dataflow, allowing them to grant access privileges to SCS users by specific partner, specific dataflow, and specific dataflow role.

All Account Manager Users and Exchange Network Partners shall ensure that SCS, partner help desk dataflows, and registration data are protected from loss, misuse, or unauthorized access to or modification of, the information in the SCS system. SCS credentials contain sensitive administrative privileges that come with use restrictions and require precautions to protect their usage. SCS registration data requires a robust level of protection as it includes an individual user's name, self-assigned user name and security question, work address, work contact information (e.g., phone and fax numbers, E-mail address), and other personal contact information. Depending upon the specific SCS dataflow(s) to which an end user has access privileges, registration data may also additionally include such items from an individual as date of birth, mother's maiden name, high school graduation date, and similar personal identifiers.

Given the nature of this access and the sensitive data that it relates to, all Account Manager Users and Exchange Network Partners must comply with the following Rules of Behavior. Violations may result in suspension of access privilege, reprimand, demotion, suspension or removal depending on the severity of the violations. In addition, for the unauthorized disclosure of information, including information protected by the Privacy Act of 1974 (5 U.S.C. § 552a), there may be criminal and civil penalties, including fines or prison terms.

Account Manager Users and/or Exchange Network Partners with questions regarding these Rules of Behavior or who wish to report security violations may contact:

- SCS Help Desk – 888.890.1995 or sharedcromerrservices@epacdx.net
- CDX Security – securitysolutions@cgifederal.com

For rules that are applicable to both, Account Manager Users and Exchange Network Partners are hereinafter referred to as “Users and Partners”.

Development/Test Credential Limits

1. Privileged use of Development and Test credentials shall be limited to Development and Testing purposes only.
2. Credentials for CROMERR development and testing shall not be used for Production regulatory use.

Authorized Use / Official Business

1. Users and Partners shall use EPA/SCS computer systems information and/or credentials for official business only.
2. Deliberate access or use of SCS data for other than authorized Agency purposes is strictly prohibited.
3. Users and Partners must abide by the SCS Warning provided at: https://encromerr.epa.gov/Scs/PrivacyNotice

Access / Identity Proofing

1. Users and Partners shall access and use only information strictly for which they have official authorization.
2. Only one partner help desk account per Account Manager User is allowed.
3. Account Manager Users shall be responsible for identity proofing their prospective SCS users before adding or deleting access privileges to their SCS accounts.
4. Account Manager Users shall only be allowed to provide SCS users access to the dataflow(s) that correspond with the dataflow(s) roles and permissions for which each particular Account Manager user has authorization.
5. Note that SCS credentials may leverage per use, fee-based LexisNexis® services for identity proofing. For detailed procedures and applications for these services, users should contact the SCS Help Desk.

Accountability

1. Users and Partners shall be accountable for their own actions and responsibilities related to information and information resources entrusted to them.
2. Users and Partners shall not attempt to perform accesses for privileges not authorized to the User and/or Partner.
3. Users and Partners shall not attempt to subvert or override internal SCS or Registration Maintenance controls.
4. Account Manager Users shall follow approved procedures for acquiring / granting access rights to SCS users.
5. Users and Partners shall log off SCS when not in use.

Confidentiality

1. Users and Partners shall protect SCS confidential or privacy act information from disclosure to unauthorized individuals or groups.
2. Do not allow partner help desk information to remain on your screen when an unauthorized person is present.
3. It is the responsibility of each Account Manager user to use partner help desk data resources in an appropriate manner and to comply with all applicable federal, state, and local statutes.

Additionally, it is the responsibility of each Account Manager user with access to sensitive data resources to safeguard these resources.

Methods of safeguarding partner help desk and registration data include:

- Registration data shall not be stored on personal computers or devices.
- Access to computers that are logged into SCS should be restricted (i.e., authenticated logins and screen savers, locked offices, etc.)
- Access to registration data stored on SCS should be restricted to those individuals with an official need to access the data (i.e., Account Manager Users).
- Registration data should be transmitted across the network in a secure manner (i.e., to secure web servers using data encryption with passwords transmitted via secure socket layer, etc.)
- Any accidental disclosure or suspected misuse of registration data should be reported immediately to the SCS Help Desk and/or CDX Security.

4. Other than user ID and user name, do not print or store registration data on paper or electronic media.
5. Any PC used to access partner help desk information must have a Windows password setting, such that a user must log back in after a 10-minute period of inactivity.

Integrity

1. Account Manager Users shall protect the integrity and quality of the partner help desk dataflow and registration data.
2. Maliciously changing registration data via the partner help desk is prohibited.
3. Never enter unauthorized, inaccurate, or false information.

Passwords and User IDs

1. Users and Partners must accept the SCS Terms and Conditions identified at https://encromerr.epa.gov/Scs/TermsAndConditions
2. Users and Partners shall protect information securely through effective use of their SCS user IDs and passwords.
3. Sharing of SCS user IDs or partner help desk privileges is strictly prohibited.
4. Protect and never share your SCS password.

Awareness

1. Users and Partners shall maintain awareness of and abide by all security policies and requirements.
2. EPA Users and Partners shall perform Agency annual security awareness training.

Reporting

1. Users and Partners must report all security incidents by contacting either the SCS Help Desk or CDX Security. Types of incidents to report include but are not limited to the following:

- Computer viruses
- Social engineering attempts
- "Phishing", lost or stolen laptops/PDAs or other equipment
- Unexplained occurrences (e.g., unexpected locked password, email you did not send, etc.)
- Sharing passwords or user identification (IDs)
- Loss or unauthorized disclosure of confidential information
- Unauthorized access to information, systems, or applications
- Verbal threats related to computer resources
- Lack of expected controls (e.g., unlocked doors, confidential information left unprotected)

2. Prior to or immediately following changes in role/responsibility, transfer, or termination, all Users and Partners shall notify the SCS Help Desk to disable or modify access for your account.