The Metropolitan Council is the regional planning organization for the seven-county Twin Cities area. The Council operates the regional bus and rail system, collects and treats wastewater, coordinates regional water resources, plans and helps fund regional parks, and administers federal funds that provide housing opportunities for low- and moderate-income individuals and families. The 17-member Council board is appointed by and serves at the pleasure of the governor.
# Table of Contents

1.0 Purpose of the Document ................................................................. 1

1.1 Overview of CROMERR Final Rule .................................................. 1

1.2 Applicability of CROMERR Final Rule ............................................. 1

1.3 EPA’s Approval of the MCES Industrial Online Reporting System ................................................................. 1

2.0 Overview of the MCES Industrial Online Reporting System Functionalities ......................................................... 2

2.1 User Account Establishment Process ................................................ 3

2.1.1 Responsible Official (RO) Account Establishment Process .................. 3

2.1.2 RO’s First Time Logging into the MCES Industrial Online Reporting System .................................................. 5

2.1.3 Consultant Account Establishment Process ....................................... 6

2.2 Electronic Submission and Revisions Processes ...................................... 8

2.2.1 Electronic Submission Process ....................................................... 8

2.2.2 Electronic Submission Revision Process .......................................... 10

2.3 User Account Management Processes .............................................. 10

2.3.1 Limit on Failed Login Attempts ..................................................... 10

2.3.2 User Forgets User Name and/or Password ...................................... 11

2.3.3 User Requests a New PIN ............................................................. 11

2.3.4 User Resets Security Questions ..................................................... 11

2.3.5 RO Account Reactivation ............................................................... 12

2.4 Account Administration Processes .................................................. 12

2.4.1 Resetting a User’s Password ......................................................... 12

2.4.2 Issue/Re-Issue a PIN to an RO ....................................................... 12

2.4.3 Inactivate a User Account ............................................................. 13

2.4.4 Change a User’s Account Permissions ............................................ 13

2.4.5 Change a User’s Account Permissions ............................................ 13

2.5 Data Backup, Disaster Recovery and Security Protection ......................... 13

2.5.1 Data Backup .............................................................................. 13

2.5.2 Disaster Recovery ........................................................................ 14

2.5.3 Security Protection ....................................................................... 15

Appendix A.Establish a Permanent Password and PIN .................................. 16

Appendix B.Example Challenge Questions and Reset Challenge Questions ......................................................... 16

Appendix C.Example of an Online Data Entry Form ...................................... 17

Appendix D.Example of Data Validation Warnings within an Online Data Entry Form ................................................. 17

Appendix E.Example of Data Review of the Form before Submission ...................... 18

Appendix F.Example of Certification Statement, PIN and Challenge Question ......................................................... 18

Appendix G.Example of Submission Confirmation Receipt Email ......................................................... 19

Appendix H.Example of Submission Receipt in the MCES Industrial Online Reporting System ................................................. 19

Appendix I.Example of List of Past Submissions .......................................... 20

Appendix J.Example of Past Submission Search Functionality ......................................................... 20

Appendix K.Example of Request to Revise a Submission ...................................... 21

Appendix L.Example of Revision Tracking .................................................. 21

Appendix M.Changing an RO’s Certification and Submission Permissions ......................................................... 22
1.0 Purpose of the Document

The U.S. Environmental Protection Agency (EPA) published the Cross-Media Electronic Reporting Rule (CROMERR): Final Rule for environmental programs that EPA has delegated, authorized, or approved to administer. The rule includes performance standards that a state, tribe, or local government should meet in order to implement EPA-authorized programs. This rule became effective January 11, 2006. Programs, “including not only those that are actually operational at the time the final rule is published, but also those that are substantially developed” must submit an application to demonstrate compliance with CROMERR standards by January 13, 2010.

A summary of the CROMERR Final Rule is presented below:

1.1 Overview of CROMERR Final Rule

- Removes all regulatory obstacles to e-reporting under EPA and EPA-authorized programs
- Sets requirements for electronic reporting to EPA
- Requires EPA approval of modifications or revisions to authorized programs that allow or wish to allow e-reporting
- Creates a special, optional process for obtaining EPA approval of program modifications or revisions related to e-reporting
- Sets mandatory standards for e-reporting systems operated by authorized programs.
- Does not set requirements for e-record-keeping
- Does not make e-reporting mandatory, but does not prohibit mandatory e-reporting under other federal, state, tribe or local law

1.2 Applicability of CROMERR Final Rule

Final Rule applies to:

- Persons who submit reports or documents to EPA to satisfy other parts of Title 40
- States, tribes and local governments that administer authorized programs under Title 40.

Final Rule does not apply to:

- Documents submitted via fax or magnetic or optical media;
- Administrative information exchanged between EPA and states, tribes or local governments as part of the implementation of authorized programs.

1.3 EPA’s Approval of the MCES Industrial Online Reporting Program:

1. MCES’s CROMERR Application Package must contain:

- Certification of sufficient legal authority to implement electronic reporting signed by the Metropolitan Council Regional Administrator;
- Listing of all electronic document receiving systems being addressed, with a description for each system that specifies how the system meets the requirements of Section 3.2000 of the rule;
- Schedule of upgrades for the systems that have a potential for affecting the program’s conformance;
- Other information needed to fully evaluate the application
2. EPA Review Process will include:

- Completeness review
- Determination is made within 75 days of application receipt
- Deficient applications may be amended, and determination of completeness is made within 30 days of amendment receipt
- Review to approve/disapprove
- Incomplete or deficient applications
- Components of a consolidated application, which can be acted on separately, for example, approving some and disapproving others
- Complete applications not acted on within 180 days are considered automatically approved
- Applications for existing systems not determined to be complete by January 13, 2010, have a 360-day review period before being considered automatically approved
- Allows consolidated applications for multiple programs

2.0 Overview of MCES Industrial Online Reporting System Functionalities

The MCES Industrial Online Reporting System is a proprietary system (the GovOnline system developed by enfoTech & Consulting, Inc.) that includes multilayered security that addresses the major facets of application security outlined in CROMERR. This includes Identity Assurance, Authentication/Authorization, Submission and Submitter Integrity, and Non-Repudiation. The MCES Industrial Online Reporting System, in conjunction with sound business practices, provides a fully CROMERR-compliant system. This document identifies the technologies, techniques, and business practices that are included in the MCES Industrial Online Reporting System implementation that provide evidence of the system’s complete compliance with the CROMERR Final Rule specifications.

Security in the MCES Industrial Online Reporting System is controlled using the following processes:

- **User Account Establishment Process:** The process in which facilities establish accounts for themselves for electronic submission by filling out an online account registration form and submitting the MCES Electronic Signature Agreement (ESA). This phase includes the following aspects:
  - Identity Proofing and Validation
  - Electronic Signature Agreement and Issuance

- **Electronic Reporting, Submission & Revision Process:** The MCES Industrial Online Reporting System provides a variety of security features during the electronic submission process. This process can be broken down into the following aspects:
  - Electronic Signature Management
  - Transmission Error Handling
  - Copy-of-Record (COR) Management

- **User Account Management Process:** The MCES Industrial Online Reporting System provides functionalities for users to protect the security of their accounts.

- **Account Administration Process:** The MCES Industrial Online Reporting System provides a security management tool for MCES staff to manage user accounts if a user’s credentials are found to be or suspected of being compromised.
• **MCES Industrial Online Reporting System Data Backup & Disaster Recovery Procedures:**
The section briefly summarizes the measures enfoTech & Consulting, Inc., has taken to back up the MCES Industrial Online Reporting System database and protect it from accidental or disastrous events. Please note that enfoTech & Consulting, Inc. is providing hosting services to MCES for the MCES Industrial Online Reporting System.

**2.1 User Account Establishment Process**

There are two types of facility user accounts in the MCES Industrial Online Reporting System:

- **Consultant:** A Consultant is a user who is able to view, create, edit or delete an unsubmitted permit renewal application or a self-monitoring report. Unless a Consultant is granted certifier privileges by a facility, a Consultant does not have the right to certify, sign, or submit any permit renewal application or self-monitoring report in the MCES Industrial Online Reporting System.

- **Responsible Official (RO):** An RO is a user who is able to view, create, edit, delete and submit an unsubmitted permit renewal application or a self-monitoring report. An RO has the right to certify, sign, and submit a permit renewal application or self-monitoring report in the MCES Industrial Online Reporting System.

The User Account Establishment Process is different for the Responsible Official (RO) and the Consultant account types. Please note that when unsubmitted permit renewal applications and self-monitoring reports are deleted, it only deletes the copy that was started. The facility is still required to submit the required submittal by the due date.

**2.1.1 Responsible Official (RO) Account Establishment Process**

The account registration process for an RO is depicted below.

**RO Creates Account in MCES Industrial Online Reporting System**

1. Facility RO fills out the self-registration form online:
   - User Info
   - Facilities Info
   - Specify User ID (system verifies uniqueness)
   - 5 Security Questions with Answers (from 20-question library)

2. Print & Sign ESA and mail it to MCES for Approval

3. MCES Staff
   - Review Registration & ESA
   - Accept or Reject?

3B. Email notification on signing privilege approval is sent to the RO’s registered email address.
   - System issues a “Temporary” Password to the RO's email

3A. Notification is sent to RO’s registered email or mailing address with rejection reason
The RO’s registration process includes the following steps:

**Step 1: RO Completes the Online Account Self-Registration Form**

The RO at the facility visits the MCES Industrial Online Report System website and clicks on the “Create a new account” link to complete an online Account Self-Registration Form, which requires the RO to provide the following info:

- User Information (first and name, title, email address, phone number, user name, etc.)
- Facility Information (Business name)
- Select Account Type (Responsible Official or Consultant)
- Associate a Facility(ies) and Submittal Types to their Account
- Select and answer five (5) security questions out of a library of 20 questions

When the RO finishes the Online Registration Form, the system will send an “Account Created Acknowledgement” email to RO’s email account with a temporary password. The RO is required to change the temporary password to a permanent password during the initial login to the MCES Industrial Online Reporting System. All passwords are stored encrypted in the database.

Please note that the registered RO cannot submit any self-monitoring reports or permit renewal applications for any facility until the RO’s “Certify & Submit” privileges have been approved and activated by MCES.

**Step 2: RO Prints, Signs and Submits the MCES Electronic Signature Agreement (ESA)**

Each person who requests to be an RO must fill out the MCES Electronic Signature Agreement (ESA). MCES has the option to require that the ESA be signed in the presence of a notary during account establishment.

**Steps 3A and 3B: MCES Approves or Denies the Account Registration**

1. The RO mails or hand-delivers the completed ESA to MCES. MCES then reviews the account information and the ESA to confirm the RO’s identity and to verify that they meet EPA’s definition of a signatory authority. Detailed processes include:

2. Verify data using MCES’ Data Management System: MCES verifies the RO’s name, mailing address, email address, and other relevant information by comparing the ESA with the information stored in MCES’ iPACS (Internet-Based POTW Administration & Compliance System) database. The iPACS database contains the name, address, and email of each facility’s signatory authority, as well as a copy of the issued permit document.

3. Verify signature using past paper submissions: Signature comparisons are performed by comparing the ESA with previously submitted documents (for example, wet-ink, signed self-monitoring reports or permit renewal applications).

4. Verify data during inspections or site visits: Inspections and/or site visits by MCES staff may be used to help verify the ESA’s authenticity. Verification can be supplemented using phone calls if authenticity questions arise.

If the RO’s account registration application is rejected, the RO will be notified via email or US Mail.

**Step 4: RO Established Permanent Password and PIN**

If the RO’s account registration application is accepted, the RO’s account will be activated in the MCES Industrial Online Reporting System. The system then emails a temporary password to the RO’s email address. The RO is required to change their temporary password to a
permanent password during the first log in to the system after account activation by MCES. During this initial login, the RO must also establish a signing PIN.

- The PIN serves as the electronic signature and is used to bind an electronic data submission to a certifier (RO). The PIN is stored encrypted in the database.
- The PIN is not visible to MCES staff and cannot be directly changed by facility users or agency staff. If a user loses their PIN, they must send a request for a new PIN to MCES staff, and a new PIN will be automatically generated and emailed to the RO’s email address by the MCES Industrial Online Reporting System.

An RO is required to submit the following two (2) forms when enrolling to use the MCES Industrial Online Reporting System:

- **MCES Industrial Online Reporting System Account Registration Form:** This form lists all facility representatives that are applying for a user account in the MCES Industrial Online Reporting System, and specifies their requested account type. Available account types are listed as follows:
  - Responsible Official (RO): A user with this account type can view, prepare, certify, sign and submit self-monitoring reports and/or permit renewal applications.
  - Consultant: A user with this account type can view and prepare self-monitoring reports and/or permit renewal applications, but cannot certify, sign or submit any electronic submissions.

- **MCES Electronic Signature Agreement (ESA):** This document identifies the Terms and Conditions of submitting data electronically for PIN holders. The ESA must be completed and signed by each prospective RO. By signing the ESA, the RO acknowledges understanding the following items outlined in the Enrollment Guide:
  - Requirements, terms and conditions of using the MCES Industrial Online Reporting System;
  - The responsibilities of MCES and participating facilities during the account registration and data submission processes;
  - The defined grounds for account suspension and termination;
  - The identification of protocol for changes in account type; and
  - The procedures for dispute resolution.

MCES has the option to require that ESAs be signed in the presence of a notary during the account registration process. While MCES does not require a notarized signature at this time, the signed ESA submitted to MCES must be the original wet-ink signature version to be submitted in person or by US Mail. Therefore, the ESA cannot be emailed or faxed.

**2.1.2. RO’s First Time Logging into the MCES Industrial Online Reporting System**

- **Establish a Permanent Password:** The first time an RO logs into the MCES Industrial Online Reporting System, the system will force the user to change their temporary password to a permanent password. This provides added security benefits by ensuring that:
  1. The RO provided a valid email address for future notifications relating to electronic reporting requirements and submissions.
  2. The RO received the temporary password at the email address provided on the ESA.
  3. The RO changes the temporary password to a permanent password, thus agreeing to the Terms and Conditions of the use of the password and PIN.
4. The permanent password is only known to the RO.

- Establish a PIN: Similarly, when the RO is establishing a permanent password, he or she must also establish a signing PIN. The PIN is also saved in the system using encryption technology. This provides the same added security benefits as indicated above. Please refer to Appendix A to see a screenshot of how to establish a permanent password and PIN.

- Answer Five (5) Security Questions: During the account registration process, the RO is required to select and answer five (5) out of 20 security questions. The 20 security questions are listed in Attachment 11 to MCES’ CROMERR application. The answers to each of the questions should be unique and will be stored in the system using encryption technology. Please refer to Appendix B for the screenshot of how to choose and answer the security questions.

2.1.3 Consultant Account Establishment Process

The account registration process for a Consultant is depicted below.

**Consultant Creates Account in MCES Industrial Online Reporting System**

1. Facility Non-Certifier fills out the online self-registration form:
   - User Info: First Name, Last Name, Title, Email, etc.

2. Facility RO “Add” non-certifier user (via email address) & assign role:
   - Preparer Role to the facility that Certifier has the certification authority

3. A Notification email is sent to the non-certifier once the association is successfully made.
Step 1: Consultant Completes the Online Account Self-Registration Form

A non-certificate (Consultant) registers for an Online Account Registration Form in the MCES Industrial Online Reporting System website by filling out an online registration form:

- User Information (first and name, title, email address, phone number, user name, etc.)
- Facility Information (Business name)
- Select Account Type (Responsible Official or Consultant)
- Select and answer five (5) security questions out of a library of 20 questions

When the applicant finishes the Online Account Registration Form, the MCES Industrial Online Reporting System will send an “Account Created Acknowledgement” email to Consultant’s email account with a temporary password. The applicant is required to change the temporary password to a permanent one during the initial login to the MCES Industrial Online Reporting System. All passwords are stored in the system using encryption technology.

Step 2: RO Associates Facilities and Permissions to Consultant

In order for the Consultant to view and prepare self-monitoring reports and/or permit renewal applications for a desired facility, the registered RO of that facility must associate the Consultant’s account to that facility. The procedures to associate a Consultant are as follows:

1. Enter the Manage “Consultants and Preparers” management screen.
2. Enter the email address of the Consultant.
3. Designate the effective and expiration dates of the Consultant’s viewing and preparing permissions.
4. Use the ”Add Authorizations” button to indicate the submittal types and facilities that the Consultant should be granted Viewer and/or Preparer permissions.

Step 3: Consultant Is Notified of Permissions

Once completed, the RO can press the ”Email Notify” button and the MCES Industrial Online Reporting System will send an email to the Consultant’s email address notifying them that their account has been activated and that they have been granted viewer and/or preparer privileges to access the facility’s submission requirements.
2.2 Electronic Submission and Revision Processes

The electronic submission process in the MCES Industrial Online Reporting System is depicted in the flowchart below:

Electronic Submission Process in MCES Industrial Online Reporting System

2.2.1 Electronic Submissions Process

The electronic submission process includes the following steps:

Step 1: RO Logs In and Enters Data for an Electronic Submission

The Consultant or RO prepares the electronic submission using online data entry forms in the MCES Industrial Online Reporting System. A server certificate is located on the MCES Industrial Online Reporting System server, which provides a Secured Socket Layer (SSL) channel of communication over port 443 to ensure that the data transmission process is secure and complete. This helps to ensure that Internet communications cannot be viewed by a third party. Please refer to Appendix C for a screenshot of an example of an online data entry form in the MCES Industrial Online Reporting System.

When the Consultant or RO is entering data into an online form, the system conducts validation checks. If the value entered by the user fails the associated validation criteria or if data in a required field is missing, the system will display an error message on the online form. Please see Appendix D for a screenshot of data validation warnings.
Step 2: RO Completes Certification and Submission Processes

During the certification and submission process, the MCES Industrial Online Reporting System displays a certification statement that the RO must read. The RO certifies that they have read the statement by clicking a checkbox next to the certification statement. Please see Appendix F for a screenshot of the certification and submission process.

Next, the RO completes the following actions:

- The RO enters their signing PIN. The MCES Industrial Online Reporting System validates the PIN by comparing the user-entered PIN with the encrypted PIN stored in the system.
- The RO answers a randomly selected security question from the five (5) questions that the RO provided answers for during the online account registration process. The MCES Industrial Online Reporting System confirms the answer by comparing the user-entered answer with the encrypted answer stored in the system.

If after three failed attempts the RO is unable to provide a valid PIN or answer the security questions correctly, the system will suspend the RO’s certification and submission permissions. In addition, the system will send an “Account Suspension” email to RO’s email address, as well as the MCES Industrial Online Reporting System Coordinator’s email address.

After the PIN and answer to security question pass the system validation checks, the RO is able to complete the electronic submission.

Step 3: System Sends RO a Submission Receipt

The MCES Industrial Online Reporting System generates a unique Submittal ID for each submission that is made using the system.

An email is sent to the RO notifying them that the submission has been successfully received by the MCES Industrial Online Reporting System. Appendix G shows an example email notification of successful submission receipt.

For each submission, a receipt is also generated. This receipt is displayed to the user immediately following submission of the report. Appendix H shows an example Submission Receipt within the MCES Industrial Online Reporting System after a successful submission. The receipt can then be printed by the RO. The receipt contains the following information:

- Unique Submittal ID
- Name, address, and contact information of submitter (RO)
- Owner Information (Facility name and address)
- Date and time of the submission
- The type of form that was submitted
- List of all attachments provided along with the submission
- The certification receipt, include a copy of the certification statement, the security question that was answered and the name of the RO
- Sender IP address from which submission was made

In addition to the list above, the following additional items are stored together with the submission data in the database:
• Date and time the PIN was captured
• Date and time the PIN was verified/approved
• A copy of certification statement language
• Indication that the RO agreed to the certification statement

The submission receipt, in conjunction with the submission data, serves as the Copy of Record (COR) for the submission.

After the submission is validated, it is stored in the MCES Industrial Online Reporting System. When the submission is stored, a Cyclic Redundancy Checksum (CRC) calculation is conducted on the submission, and the CRC value is stored in the database along with the submission. This CRC value represents a binary snapshot of the submission that is received by MCES, which can be used to detect if the original submission has ever been altered by the system or any other means.

Note Regarding the Atomic Clock Time: The MCES Industrial Online Reporting System uses atomic clock time servers to establish the critical dates and times related to electronic submission and processing. This provides additional assurance of accurate submittal times independent of potentially variant server clocks. This feature is important when using submission date/time as a basis for compliance determination of late submittals.

Step 4: User Views Past Submissions

MCES Industrial Online Reporting System users can review all past submissions made using the system. Please refer to Appendix I and Appendix J for screenshots of an example list of past submissions and of the past submission search functionality, respectively. Users can access the COR for all past submissions, including a copy of the submission itself and the related submission receipt. Each time the submission file is opened in the MCES Industrial Online Reporting System, the system performs the CRC check automatically to ensure the integrity of the submission data is being upheld.

CRC Check: The user can perform a CRC check on the submission that is currently stored in the MCES Industrial Online Reporting System. This CRC value is compared to the CRC value that was determined upon submission. If the numbers are different, this indicates that the file has been modified since it was originally submitted to MCES. This check provides additional assurance of file integrity of the submission. Each time the submission file is opened in the MCES Industrial Online Reporting System, the system performs the CRC check automatically.

2.2.2 Electronic Submission Revision Process

The MCES Industrial Online Reporting System allows users to submit corrections to previous data submissions by creating a new revision record.

To submit a correction, the RO needs to submit a revision report, which will be treated as a new COR when completed. In this scenario, the entire history of the report, including the original COR and new CORs for all corrections are maintained in the database and are retrievable. Please refer to Appendix K and Appendix L for screenshots of requests to revise a submission and an example of revision tracking, respectively.

2.3 User Account Management Processes

2.3.1 Limit on Failed Login Attempts

The MCES Industrial Online Reporting System limits the failed login attempts to ensure user credentials are not compromised.
1 The user is prompted to enter their user name and password when logging into the MCES Industrial Online Reporting System.

2 If the user name and password entered do not match with the information stored in the MCES Industrial Online Reporting System, the system will display a warning message regarding the error and potential suspension after three consecutive failed attempts.

3 After three failed attempts, a message appears advising the user that their account has been suspended.

2.3.2 User Forgets User Name and/or Password

The MCES Industrial Online Reporting System allows a user to request to retrieve their user name or request a new password if they have forgotten either credential using the following process:

1 On the Homepage, the user clicks on the “Forgot your login user name or password?” link.

2 On the “Forgot Your Password?” screen, the user enters their email address.

3 If the provided email address is found, the system asks the user to answer one (1) of the five (5) security questions they answered during online account self-registration.

4 If the security question is answered correctly, the system issues a new system-generated temporary password and sends an email to the user’s email address with their user name and temporary password.

5 The user uses their user name and temporary password to log into the MCES Industrial Online Reporting System.

6 Upon a successful login, the user must change the temporary password to a permanent password.

7 The system stores the permanent password using encryption technology.

8 The system saves a log of all password changes in the database.

2.3.3 User Requests a New PIN

The MCES Industrial Online Reporting System allows an RO to request a new signing PIN based on the following process:

1 The RO logs into the MCES Industrial Online Reporting System using their valid user name and password.

2 In the “Password Management” screen on the “My Account” tab, the user clicks on the “My PIN Information” tab.

3 In the “My PIN Information” screen, the user clicks on the “Request new PIN” button to send a request to reset their PIN.

4 Once the PIN is reset, the MCES Industrial Online Reporting System sends an “Issue PIN Notification” email to the RO’s email address with the new PIN.

5 The RO then should update the system-generated PIN to a permanent PIN.

6 The system stores the permanent PIN using encryption technology.

7 The system saves a log of all PIN changes in the database.

2.3.4 User Resets Security Questions

The MCES Industrial Online Reporting System allows the user to reset their security questions. The process is as follows:
1. The RO logs into the MCES Industrial Online Reporting System using a valid user name and password.

2. On the “Security Questions” management screen in the “My Account” tab, the user selects five (5) security questions (from a library of 20) and provides answers to each of them.

3. The user provides a reason for resetting their security questions.

4. The user clicks the “Save” button to reset the security questions.

5. Once the security questions are reset, the system will store the answers to the security questions using encryption technology.

6. The system saves a log of all security question changes in the database.

2.3.5 RO Account Reactivation Process

If the RO’s account permissions are suspended for any reason, the RO must follow the process below to have their account reactivated:

1. The RO requests that their certification permissions for a facility be restored to the MCES Industrial Reporting System by resubmitting the MCES Electronic Signature Agreement (ESA).

2. Once the ESA is received, MCES reviews the request and confirms the signatory authority of the RO.

3. If MCES approves the RO’s request, MCES will re-activate the RO’s certification permissions for the facility. This is completed by changing the signing status of the RO for the facility from “Pending” or “Inactive” to “Active”. In addition, the re-submitted ESA will be stored in the MCES Industrial Online Reporting System. Please see Appendix M for a screenshot on how to complete this process.

4. The RO logs into the MCES Industrial Online Reporting System using a valid user name and password. The RO is then able to prepare, certify, sign and submit data electronically for the facility.

2.4 Account Administration Processes

The MCES Industrial Online Reporting System Coordinator is able to perform the following functions to manage user accounts.

2.4.1 Resetting a User’s Password

1. The Coordinator searches for the user’s account in the Agency Portal of the MCES Industrial Online Reporting System.

2. The Coordinator clicks on the “Reset Password” button.

3. The MCES Industrial Online Reporting System sends an email notification to the user with the new system-generated temporary password.

4. The system logs each time the Coordinator resets a user’s password in the system.

5. Upon first login, the user must change the temporary password to a permanent password.

6. The system saves the permanent password in the system using encryption technology.

2.4.2 Issue/re-issue PIN to RO

1. The Coordinator searches for the RO’s account in the Agency Portal of the MCES Industrial Online Reporting System.

2. The Coordinator clicks on the “Issue/Reset PIN” button.
The MCES Industrial Online Reporting System sends an email notification to the RO with the new system-generated temporary PIN.

The system logs each time the Coordinator reset an RO’s PIN in the system.

Upon first log in, the RO must change the temporary PIN to a permanent PIN.

The system saves the permanent PIN in system using encryption technology.

2.4.3 Inactivate a User Account

1. The Coordinator searches for the user’s account in the Agency Portal of the MCES Industrial Online Reporting System.

2. The Coordinator clicks on the “Account Status” button to change the status from “Active” to “Inactive”.

3. The system logs each time the Coordinator changes a user’s account status in the system.

4. The system sends an email to the user to notify them that their account has been inactivated.

5. At the next attempted log in, the user will not be able log into the system.

2.4.4 Activate a User Account

1. The Coordinator searches for the user’s account in the Agency Portal of the MCES Industrial Online Reporting System.

2. The Coordinator clicks on the “Account Status” button to change the status from “Inactive” to “Active”.

3. The system logs each time the Coordinator changes a user’s account status in the system.

4. The system sends an email to the user to notify them that their account has been inactivated.

5. At the next attempted log in, the user will be able to log into the system using a valid user name and password.

2.4.5 Change a User’s Account Permissions

1. The Coordinator searches for the user’s account in the Agency Portal of the MCES Industrial Online Reporting System.

2. In the “Manage Account Type” tab, the Coordinator changes the user’s role accordingly to one of the following:
   a. Consultant
   b. Responsible Official

3. The system sends an email to the user to notify them that their account permissions have been changed.

4. The system logs each time the Coordinator changes a user’s account permissions in the system.

2.5 Data Backup, Disaster Recovery & Security Protection

2.5.1 Data Backup

MCES has two (2) ways of retaining copies of electronic submissions. The first way is at the database level and the second way is at the Cloud Hosting level by using the environment backup process.

Database Level:
For each electronic submission by a facility, the XML instance files (identified as the Copy of Record) are maintained in the MCES Industrial Online Reporting System database. These files are never deleted from the system.

Per organizational policy, the MCES Industrial Online Reporting System will store a minimum of five (5) years of electronic submissions before archiving the data.

Cloud Hosting Level:

The system will maintain the COR in the database. This database system is an SQL production database environment, which is highly redundant. The data is backed up using two- (2) different backup methods:

- The first method is a full database backup which is completed weekly with an incremental backup done daily.
- The second method is a full database backup which is archived to a tape backup. These backup tapes are created weekly and are stored offsite in a secure facility.

Data storage is provided as a directly attached storage array (Host Bus Adapter – HBA, connected Data Vault), which is part of the overall database cluster. The database server backup is configured to take frequent production SQL Server backups of database server image (from Active Database Server) with a complete database backup from the Data Vault (Weekly “Full” and Daily “Incremental”), plus a near real-time transaction log (~5-15 minutes interval) for the purpose of quickly recovering the faulted database to prevent or minimize any potential data loss.

The primary hosting site is at the enfoTech Data Center (http://www.enfoTech.com/). There is a minute-by-minute backup service of the systems and databases from the primary hosting site to the secondary hosting site. If the primary hosting site is not functional, the secondary hosting site will automatically be brought into service within hours.

The tertiary hosting site is located several miles away from the primary and secondary hosting sites. There is a minute-by-minute backup service of the systems and databases from the enfoTech headquarters server farm to the tertiary hosting site to guarantee 100% no-loss discovery recovery.

The server team maintains a mirror copy of current production system environment on the secondary hosting site in a remote location.

2.5.2 Disaster Recovery

A disaster recovery plan is in place for the MCES Industrial Online Reporting System:

- A full database backup is completed weekly. An incremental backup is completed daily.
- A mirror copy of the current production system environment is kept on the secondary hosting site in a remote location.

The applications and database servers are failed over from the primary hosting site to the secondary hosting site automatically by pre-configuration, but it requires hosting center staff to manually complete the entire process of disaster recovery. Once the action of failover succeeds, the secondary hosting site will serve as the main hosting site so users can continue to use the MCES Industrial Online Reporting System. As soon as the primary hosting site is back up, the reverse replication actions will be scheduled and completed. The primary hosting site will be failed over from the secondary hosting site. The primary hosting site will then resume operations as the main hosting site.
• In the case of catastrophic failures, such as server crashes, fire, etc., the latest tape backup for the MCES Industrial Online Reporting System can be quickly recovered to resume services within hours.

2.5.3 Security Protection

Hosting services from enfoTech provide strong security protection using the following processes:

1. **Next-Gen Network Firewall Protection with Unified Threat Management.**
   - Built on the top-ranking Unified Threat Management platform (FortiNET).
   - Provides Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, and Application Intelligence and Control for intelligent, real-time network security protection against the latest blended threats.
   - Monitors for anomalous data, generating alerts if unauthorized data packets are found.

2. **Secure Remote Access**
   - Access is limited to only authorized IT staff using their user name and password.
   - Provides network authentication, grants access and maintains security privileges for remote connections.

3. **Penetration Testing results and mitigation**
   - Uses third-party penetration testing services from Trustwave ([www.trustwave.com](http://www.trustwave.com))
   - Provides a scanning report monthly or on demand by Trustwave.

4. **Server Security Protections:**
   - Requires keypad and assigned access codes to access the server rooms.
   - Access to individual databases on those servers is limited to only authorized IT staff using their user name and passwords.
   - Access to the application with SSL ([RSA 2048 bit encryption](http://www.trustwave.com)) security protection.
   - Balance traffic load with Network Load Balancer (f5) connecting Web servers (extendable up-to 32 Web servers), which receives requests from the external Clients through SSL ([RSA 2048 bit encryption](http://www.trustwave.com)) protected communication channel.
   - Access to hosting servers is allowed to only a few administrators or managers including the infrastructure manager, maintenance manager, release manager, and the database administrator.

5. **Managed Anti-virus:**
   - Uses Firewall native anti-virus protection as hardware protection mechanism.
   - Uses AVG as software anti-virus protection mechanisms.
Appendix A. Establish a Permanent Password and PIN

**Change Password**

Password must have at least one uppercase letter, one lowercase letter and one digit number.

- **Now Password:**
- **Confirm Now Password:**

**Change Pin**

- **Now Pin:**
- **Confirm New Pin:**

**Save**

Appendix B. Example Challenge Questions and Reset Challenge Questions

**Create Account**

For public user to create user account. (*) Denotes a required field.

**Security Questions**

One of the following security questions will be referenced during the application submission process. Please answer all five questions below with unique responses.

1. **Question 1:** What is your least favorite movie?
   - **Answer:**
2. **Question 2:** What is your favorite book?
   - **Answer:**
3. **Question 3:** Who is your favorite all-time entertainer?
   - **Answer:**
4. **Question 4:** What is your favorite song?
   - **Answer:**
5. **Question 5:** Who is your favorite author?
   - **Answer:**

**Note:** The above security questions will be used in the MCES Industrial Online Reporting System.
Appendix C. Example of an Online Data Entry Form

Appendix D. Example of Data Validation Warnings within an Online Data Entry Form
Appendix E. Example of Data Review of the Form before Submission

Appendix F. Example Certification Statement, PIN and Challenge Question
Appendix G. Example of Submission Confirmation Receipt Email

Dear Robert Johnson,

Thank you for your electronic data submission.
Application ID: 1699
Application Name: Industrial Waste Discharge Report - Reporting Period Information
Application Status: Complete Submittal
Submitted Date: 9/15/2015 1:14:06 PM

Thank you for using the MCES Industrial Online Reporting System!

Regrets,
MCES Industrial Online Reporting System

Appendix H. Example of Submission Receipt in the MCES Industrial Online Reporting System

Submit ID: 1699 (Please remember the Report ID for any future references.)

Submitted By:
Robert Johnson
Metropolitan Area Solutions
1000 N 5th St
St Paul MN 55101
651-555-5555
robertjohnson@metro-solutions.com

Submitted on: 9/18/2015 1:14:06 PM

Form Detail

- Standard SMR

Attachment Detail

EPA Categorical Compliance Form (Optional) –

Supporting Documents (Optional) –

Certification Receipt

Certification Statement: I certify under penalty of law that this document and all attachments were prepared under my direction or supervision in accordance with a system designed to ensure that qualified personnel properly gather and evaluate the information submitted. Based on my inquiry of the person or persons who manage the system, or those persons directly responsible for gathering the information, the information submitted is, to the best of my knowledge and belief, true, accurate, and complete. I am aware that there are significant penalties for submitting false information, including the possibility of fines and imprisonment for knowing violations.

Certification Question: What is your favorite book?

Certification Question Answer: ********

PIN Number: **************

Responsible Officer: Robert Johnson

Sender IP: 172.168.168.254
Appendix I. Example of List of Past Submissions

![Submit List](image)

Appendix J. Example of Past Submissions Search Functionality

![Search Functionality](image)
Appendix K. Example of Request to Revise a Submission

Users may request to revise a submission made using the MCES Industrial Online Reporting System. The request is sent to their MCES Permit Engineer.

- **Review Status:** Complete Submittal

**Application Form(s) Detail**

**Application Revision**

- **Reason for Revision:** Data entry incomplete

**Request for Revision**

The MCES Permit Engineer reviews and decides to approve or deny the revision request on the Agency Portal of the MCES Industrial Online Reporting System.

**Revision Request**

- Reason for Revision: Data entry incomplete
- Comments:

**Appendix L. Example of Revision Tracking**

**Unfinished Submittals**

<table>
<thead>
<tr>
<th>State</th>
<th>Submittal Information</th>
<th>Facility Name</th>
<th>Form Type</th>
<th>Report Frequency</th>
<th>Monitoring Period</th>
<th>Due Date</th>
<th>Last Updated Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td>MS - Industrial Waste Discharge Report - Reporting Period Information</td>
<td>Metropolitan Areas Solutions</td>
<td>STD</td>
<td>01/01/2014 ~ 06/30/2014</td>
<td>11/10/2015 09:05 AM</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>State</th>
<th>Submit Date</th>
<th>Last Updated Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td></td>
<td>11/10/2015 09:05 AM</td>
</tr>
</tbody>
</table>
## Appendix M. Changing an RO’s “Certify & Sign” Permissions

### Public User Management

This page allows you to manage Public accounts.

<table>
<thead>
<tr>
<th>General Information</th>
<th>Manage Account Type</th>
<th>Manage Account Association</th>
<th>Attachment</th>
</tr>
</thead>
</table>

- **Account group:** Consultant, Responsible Official
- **Account type:** Responsible Official
  
  **Save Account Type**

### Associated Facility List

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Address</th>
<th>Submittal Type</th>
<th>Status</th>
<th>Updated By</th>
<th>Updated Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>107911</td>
<td>Metropolitan Area Solutions</td>
<td>1000 N 5th Street, ST PAUL, Minnesota 55201</td>
<td>Industrial Waste Discharge Report - Sampling Results</td>
<td>Active</td>
<td>admin</td>
<td>9/18/2015 12:43:41 PM</td>
</tr>
<tr>
<td>107911</td>
<td>Metropolitan Area Solutions</td>
<td>1000 N 5th Street, ST PAUL, Minnesota 55401</td>
<td>Industrial Waste Discharge Report - Reporting Period Information</td>
<td>Active</td>
<td>admin</td>
<td>9/18/2015 12:43:45 PM</td>
</tr>
<tr>
<td>107911</td>
<td>Metropolitan Area Solutions</td>
<td>1000 N 5th Street, ST PAUL, Minnesota 55401</td>
<td>Permit Renewal Application - Standard Discharges</td>
<td>Pending</td>
<td>admin</td>
<td>9/18/2015 2:18:15 PM</td>
</tr>
</tbody>
</table>

If you are registered as an RO, you are required to sign and mail a hard-copy Subscriber Agreement to EPO.

### Review Associated Facility

**ID:** 107911

**Name:** Metropolitan Area Solutions

**Address:** 1000 N 5th Street

**Submittal Type:** Permit Renewal Application - Standard Discharges

**Status:** Pending

**Comment:**

<table>
<thead>
<tr>
<th>Save</th>
<th>Cancel</th>
</tr>
</thead>
</table>