CROMERR System Checklist	
Item	**North Dakota Department of Health Environmental Health Section Electronic Reporting Information System (ERIS)**
Registration (e-signature cases only)	
1. Identity-proofing of registrant	
	Business Practices: Does not Apply for this electronic reporting information system
	System Functions:
	Supporting Documentation (list attachments):
1a. (priority reports only) Identity-proofing *before* accepting e-signatures	
	Business Practices: Does not Apply for this electronic reporting information system
	System Functions:
	Supporting Documentation (list attachments):
1b. (priority reports only) Identity-proofing method (See 1bi, 1bii, and 1b-alt)	
1bi. (priority reports only) Verification by attestation of disinterested individuals	
	Business Practices: Does not Apply for this electronic reporting information system
	System Functions:
	Supporting Documentation (list attachments):

CROMERR System Checklist	
1bii. (priority reports only) Information or objects of independent origin	
	Business Practices: **Does not Apply for this electronic reporting information system**
	System Functions:
	Supporting Documentation (list attachments):
1b-alt. (priority reports only) Subscriber agreement alternative	
	Business Practices: **Does not Apply for this electronic reporting information system**
	System Functions:
	Supporting Documentation (list attachments):
2. Determination of registrant's signing authority	
	Business Practices: **Does not Apply for this electronic reporting information system**
	System Functions:
	Supporting Documentation (list attachments):

CROMERR System Checklist	
3. Issuance (or registration) of a signing credential in a way that protects it from compromise	
	Business Practices: **Does not Apply for this electronic reporting information system**
	System Functions:
	Supporting Documentation (list attachments):
4. Electronic signature agreement	
	Business Practices: **Does not Apply for this electronic reporting information system**
	System Functions:
	Supporting Documentation (list attachments):

CROMERR System Checklist	
Signature Process (e-signature cases only)	
5. Binding of signatures to document content	
	Business Practices: **Does not Apply for this electronic reporting information system**
	System Functions:
	Supporting Documentation (list attachments):

6. Opportunity to review document content	
	Business Practices: **Does not Apply for this electronic reporting information system**
	System Functions:
	Supporting Documentation (list attachments):
7. Opportunity to review certification statements and warnings	
	Business Practices: **Does not Apply for this electronic reporting information system**
	System Functions:
	Supporting Documentation (list attachments):
CROMERR System Checklist	
Submission Process	
8. Transmission error checking and documentation	
	Business Practices: Transmission error checking and documentation will be implemented through SSL (Version 3). Also, a checksum value is computed before the file is uploaded and again after it is saved on the server. If the checksums do not match it will reject the uploaded file.
	System Functions: The SSL protocol makes a secure connection, so it is impossible to tamper with transmitted data. If the data was changed, the encryption/decryption process would fail. The system will also perform a checksum of the file using the SHA-256 algorithm before it is uploaded and will store this checksum in the database with information for the copy of record. It will then perform the same checksum when it is saved to the server and will check to ensure the checksums match. If the checksums do not match it will reject the uploaded file. The system will store the uploaded file and associated metadata that makes up the copy of record. The only updates to the database will be done by the application so users of the system will not be able to make any changes to the data. Also the database will be configured so that an audit log will track anyone who logs into the database without using the front end application. So if a checksum value indicates that a change was made, the logs will indicate who logged into the database where the change would have had to be made and will show the changes made to a record.

	Supporting Documentation (list attachments): See Design Document; -Use Case 001 Login, Page 16 under System Function for description of SSL use. -Additional Design Considerations; page 71 – Specifies SSL use for application. -Use Case 004 Upload Report, under Steps items 5-7, Page 30-31. Describes how checksum is used to validate the uploaded file. Also under System Function on page 32, it describes the Checksum and how a report record is written for each file upload. -Use Case 005 Submit Report Pages 41-43 show the submit process and describes the data stored for the copy of record.

9. Opportunity to review copy of record (See 9a through 9c)

9a. Notification that copy of record is available

	Business Practices: When a file is uploaded, the system will check the file format to verify that it meets the fixed file format definition (for future XML flows it will check it against an XSD). If the file verification is successful, then it must be submitted by a person with submit security level. If the person uploading the file has submit level security, they can view the file, submit the file or notify users with submit authority that a file is ready to be submitted. Users that do not have submit authority will be able to view the uploaded file or notify users with submit authority that a file is ready to be submitted. Notification is done by sending an email to the registered email address of users with submit authority for that facility and data flow type. When a file is submitted it will automatically send an email to the registered email address of the user submitting the file. The user submitting the file will also be able to add additional email addresses to which a notification will be sent indicating that the file has been submitted and a copy of record is available to view.
	System Functions: After a file has been successfully uploaded and verified that it is the right format for that dataflow, The Environmental Health System Electronic Reporting Information System (ERIS) displays a screen where the user can press a button that will send an email to users who have submit authority for that facility and data flow, notifying them that a file is uploaded and ready to be submitted. The email will be sent to the registered email address of the appropriate users. After a file has been successfully submitted, the ERIS will automatically send an email to the registered email address of the user submitting the file. During the submit process the user will also have the option to select multiple email addresses, and when the file is submitted the system will also send an email to these additional addresses notifying them that a file was submitted and they can review the copy of record.
	Supporting Documentation (list attachments): See Design Document; -Use Case 004 Upload Report, Page 30-37 under Steps Item 9 (Page 31) – Notification to all Submit Users -Use Case 005 Submit Report, Pages 41-43, Notification of a report being submitted is sent to the current submit user.

9b. Creation of copy of record in a human-readable format

	Business Practices: The copy of record consists of an exact copy of the uploaded data file in the same file format as the original; the date and time the record was uploaded and submitted; and other circumstances of receipt including the user who uploaded and submitted the data file, the file name, the reportID, the status of the file and the checksum of the uploaded file as well as the facility and dataflow type for which the file was submitted.

	System Functions: The ERIS allows users with appropriate permission to upload an exact copy of a data file. The system will have code which enables it to display the file in a human readable format along with the metadata associated with that file that makes up the copy of record. The metadata recorded includes ReportID, User, Facility, Dataflow Type, Report Name, Date/Time, and Status. This will be able to be viewed or printed as a web page or as a PDF document. The PDF document will be formatted as a text document displaying the same information that is displayed on the web page with all of the meta data labeled and with the uploaded data file displayed and labeled. The PDF document of the copy of record will also be able to be downloaded.
	Supporting Documentation (list attachments): See Design Document; -Use Case 004 Upload Report, Page 30-37 under System Functions (Page 31-32), it describes how the information that makes up the copy of record is recorded and saved by the system. -Use Case 005 Submit Report, Pages 41-43, It explains how the submit information which is part of the copy of record is recorded and saved by the system. -Use Case 006 Copy of Record, Page 52-53. Describes the copy of record.

CROMERR System Checklist	
9c. Providing the copy of record	
	Business Practices: The system generates a copy of record when a file is uploaded and submitted. After a file is uploaded or submitted anyone that has appropriate security in the system for a facility and dataflow type, can find the record and view, print or download a copy of the file submitted in a human readable format and the associated metadata. This provides near instant access to the copy of record. The copy of record is retained on the server for the length of time not less than the record retention requirements specified in the Safe Drinking Water Act. After this record retention time has been met, the data file can be archived.
	System Functions: When a file has been uploaded and submitted, the ERIS will store the file and the metadata for the file (such as facility, dataflow type, user, date and time of submission, checksum, etc., …). Users will have the option to go to a web page where they can see a list of all of the reports uploaded or submitted for a facility and dataflow type. They can select the report they want to view and either view or print the report from the web page, or press a button that will convert the file to PDF and will allow them to view, print, or save the file in PDF format. The file will display the copy of record for the data upload as shown on the screen shot for "UC006 Copy of Record" of the attached design document. When the file is converted to PDF it will take this same information displayed as a text file and convert it to PDF format. It will display all of the meta data related to the record including ReportID, User, Facility, Dataflow Type, Report Name, Date/Time, and Status; and then display the data submitted in a human readable format with appropriate labels to explain the data.
	Supporting Documentation (list attachments): See Design Document; -Use Case 006 Copy of Record, Page 52-53. Describes the copy of record and how it can be viewed or downloaded.
10. Procedures to address submitter/signatory repudiation of a copy of record	
	Business Practices: Users that have submit authority can select a file from the list of submitted files, then specify that they want to retract that file. They will be asked to confirm that they wish to retract the file. If they confirm that they wish to retract it, the file status will be changed to "retracted" and the user as well as the department dataflow type administrator will be sent an email indicating the specific file was retracted. When the file is retracted, the copy of the file on the LAN will be deleted, but the copy of

	the data file saved on the database will be kept.
	System Functions: The ERIS has a retract button as an option on the page where each submitted file is displayed. When the retract button is pressed, it asks the user to confirm that the file is to be retracted. If the user confirms this, it changes the status of the file to "retracted" and automatically sends an email to the registered email account for the user and for anyone listed as a dataflow type administrator for that dataflow type. The system also generates a history record to record that this data file was retracted. The digital file will not be removed from the database, but will only be marked with a status of "retracted." The copy of the file on the LAN will be deleted.
	Supporting Documentation (list attachments): See Design Document; -Use Case 005B Retract Report, Page 49-51. Describes how a submit user can retract a previously submitted repot.
11. Procedures to flag accidental submissions	
	Business Practices: The System is designed to be very user friendly to prevent accidental submissions. First, the user must have adequate security to get into the system. The system has security that is assigned by facility and data flow type. Therefore, users can access data only for the facilities and dataflow types for which permissions have been assigned. They have no access to data for facilities and dataflow types for which they have no permissions. The user must select the facility and dataflow type before they can upload or submit a file. Users will only be able to see data for one facility at a time. Next, when uploading a file they must select the dataflow type, followed by the file they wish to upload. The system performs verification on the file being uploaded to ensure it is a valid file type for the specified data flow type. After the upload is complete it will display an upload message indicating that the uploaded was completed successfully. When submitting a file, the users are taken to a distinct web page used for submitting files. The page displays the facility, dataflow and file they are proposing to submit. They must enter their Personal Identification Number (PIN) and press the submit button. Then a new form comes up where the user is asked to confirm that they are the specified user and that the information is true and they are intending to submit this data. They must press "Yes" for the record to be saved. If they press the "Yes" button, a confirmation email is automatically sent out to the registered email address for that user notifying them that the report was submitted by their user ID. At that time a copy of the submitted file will be copied to the LAN where appropriate Drinking water program staff will have read only access to the file. While the PIN has some components that are similar to an electronic signature, the North Dakota Department of Health Drinking Water rules do not require a signature when submitting drinking water lab data, so this is not being treated as an electronic signature.
	System Functions: The system security only allows a user to access facility information for those facilities for which they are registered and only for dataflow types for which they are assigned permission. When a file is uploaded, a validation check is done to ensure it is the correct file type for the dataflow type specified. The user is given confirmation on the web form that the upload is successful, and a history record is generated indicating a file was uploaded. To submit a file, the user must go to a specific and distinct web page used for submitting a file where it displays the facility, dataflow type and file to be submitted. They must enter the correct PIN to submit the file and are also asked to confirm that they are the listed user and are intending to submit this file. A confirmation is then automatically sent to the registered email address of the user and to any other email addresses the user specified. At that time an exact copy of the file in the same file format is saved to the LAN where appropriate drinking water program staff have read only access to the data file. A history record is also generated indicating that the file was submitted. All of these steps are intended to ensure the user is knowingly submitting the file and to prevent accidental submission. At anytime, a user can go into the system and mark a submitted file as "retracted" or mark a file that has been uploaded, but not yet submitted as "deleted."

	Supporting Documentation (list attachments): See Design Document; - Use Case 005 Submit Report, Pages 41-47, It explains how the user can submit information and is asked to verify they intend to submit this information (page 45). -Use Case 001 Login, Page 15-17. Describes how a user can login to the system and users roles will be by assigned facility and dataflow. -Use Case 010 Roles, Page 61-63. Describes how a user is assigned roles
CROMERR System Checklist	
12. (e-signature cases only) Automatic acknowledgment of submission	
	Business Practices: **Does not apply for this electronic reporting information system**
	System Functions:
	Supporting Documentation (list attachments):

CROMERR System Checklist	
Signature Validation (e-signature cases only)	
13. Credential validation (See 13a through 13c)	
13a. Determination that credential is authentic	
	Business Practices: **Does not apply for this electronic reporting information system**
	System Functions:
	Supporting Documentation (list attachments):
13b. Determination of credential ownership	
	Business Practices: **Does not apply for this electronic reporting information system**
	System Functions:
	Supporting Documentation (list attachments):
CROMERR System Checklist	
13c. Determination that credential is not compromised	
	Business Practices: **Does not Apply for this electronic reporting information system**
	System Functions:
	Supporting Documentation (list attachments):

14. Signatory authorization	
	Business Practices: **Does not apply for this electronic reporting information system**
	System Functions:
	Supporting Documentation (list attachments):
15. Procedures to flag spurious credential use	
	Business Practices: **Does not apply for this electronic reporting information system**
	System Functions:
	Supporting Documentation (list attachments):
CROMERR System Checklist	
16. Procedures to revoke/reject compromised credentials	
	Business Practices: **Does not apply for this electronic reporting information system**
	System Functions:
	Supporting Documentation (list attachments):
17. Confirmation of signature binding to document content	
	Business Practices: **Does not apply for this electronic reporting information system**

	System Functions:
	Supporting Documentation (list attachments):

CROMERR System Checklist

Copy of Record

18. Creation of copy of record (See 18a through 18e)

18a. True and correct copy of document received

	Business Practices: The user that is uploading a file, i.e. transmitting a file from a local machine to the ERIS system using a secure SSL connection (UC004 Upload Report on page 30 of design document), has the ability to review it anytime after upload because the file is saved in the database upon completion of the procedure. A user also has the ability to review a submitted file, i.e. an uploaded file that has been submitted in the ERIS system (use case UC005 Submit Report on page 41 of the design document). The user who uploaded a file can open the human readable copy of record and compare the data uploaded with the original file to ensure it is accurate. Also during upload, the system performs a checksum on the original file before upload and again after it is saved on the server, and if they do not match it rejects the file for upload. A user can do a checksum separately using the SHA-256 algorithm at any time on the file saved in the ERIS system and compare it to the checksum calculated by the system as a way to ensure the file was not changed. A file that has been uploaded but not submitted can be marked as "deleted" from the system by any user with at least add security level permission for that record, if it is determined to be in error. Also a file that has been submitted can be marked as "retracted" by a user with at least submit security level permission for that record, if it is determined to be inaccurate. Once a file is uploaded or submitted it cannot be changed. Also, the checksum value is stored for the record and if there is any question if the record has been changed, the checksum can be checked to verify that the file was not changed. This allows for many checks to ensure the copy of record is not changed.

	System Functions: When a file is uploaded to the system, a checksum is done on the file using the SHA-256 algorithm before it is uploaded. The file is then uploaded using a secure SSL connection and stored in the database. After upload, the checksum is performed again and compared with the original checksum calculated before upload. If the checksums are not the same, the file is rejected. If the checksums are the same, the checksum is stored in the database along with the other metadata for that file which then becomes the copy of record. This checksum can be recomputed at any time using the SHA-256 algorithm and compared to the checksum value stored in the database with the file and its metadata. If the checksums do not match the file has been corrupted or altered. The database where the data for each uploaded file is stored will have an audit log that tracks all users who access the database. If the checksum for a record no longer matches the checksum of the file stored it could have either been corrupted or changed by someone directly accessing the database tables. The audit log will show if anyone accessed the database where the data file and checksum are stored. If there is no change to the record where the checksum is stored, we can be assured that the checksum was not altered. The audit log is a component of SQLServer. It will only be accessible by a SQLServer database administrator who works at the state Information Technology Department and will not be accessible by any ERIS users or ERIS administrators. Users with appropriate security can view an uploaded or submitted file through the ERIS. The ERIS uses the file definition provided for the drinking water data flow type to display the file data on a webpage in a human readable format. This file can be viewed or printed from the web page, and it can also be generated as PDF document in a human readable format where it again can be viewed, printed or downloaded. This allows users to view and compare the data with the original data submitted. The system also has screens that allow users with appropriate permission to mark a file as "deleted" if it has been uploaded but not submitted. Uploaded records are stored in the database as an exact copy of the uploaded file in the same file format as the original. Files that are deleted will be marked as "deleted," but the digital copy of the data file stored in the database and all of the records used to log the file will remain in the database. For retracted records, the copy of the submitted file on the LAN will be deleted, but the digital copy of the submitted file and all of the records used to log the file will also be kept in the database and will not be deleted. The ERIS system will have no functionality to delete records or data from the database. The copy of the data stored on the LAN will only be deleted by the system if a file is retracted, but within the database a "delete" or 'retract" only consists of changing the status of the record for that data to "deleted" or "retracted" as appropriate. So the system will always have a complete record of the data that was uploaded or submitted even if it has been marked as "deleted" or "retracted."
	Supporting Documentation (list attachments): See Design Document; -Use Case 004 Upload Report, Page 30-37 under Steps (Page 31) and under System Functions (Page 32) it describes the checksum. Under User Interface (Page 33), it indicates the user can view a copy of the uploaded report. -Use Case 005 Submit Report, Pages 41-48, It explains how the submit information, which is part of the copy of record, is recorded and saved by the system. -Use Case 006 Copy of Record, Page 52-53. Describes the copy of record. -Use Case 004B Delete Report, Page 38-41. Describes how to delete an uploaded report. -Use Case 005B Retract Report, Page 49-51. Describes how to retract a submitted report.
18b. Inclusion of electronic signatures	
	Business Practices: **Does not apply for this electronic reporting information system**

	System Functions:
	Supporting Documentation (list attachments):
18c. Inclusion of date and time of receipt	
	Business Practices: The ERIS keeps a history record which includes the date and time of all actions related to a file submission. This includes the actions of "upload" and "submit" as well as "delete" and "retract," so the date and time of upload, submit, delete and retract will be available for all files. Other information included in the history log for each file includes: user, facility, dataflow type, status, date, time and checksum.
	System Functions: The system database has a log table which records the history of each file that has been uploaded or submitted. It tracks the date and time of any and all actions done on a file including upload, submit, delete and retract. This is available for users to review on the Data Flow List page, which displays the list of file uploads and submissions for a facility. This table is updated automatically by the system so the information in this history table, including the date and time, cannot be altered by the users.
	Supporting Documentation (list attachments): See Design Document; -Use Case 004 Upload Report, Page 30-37 under System Function (Page 32) it describes the date and time of transaction will be recorded. -Use Case 005 Submit Report, Pages 41-48, under User Interface (page 43) it lists the data that will be recorded for the submit transaction including date and time. -Use Case 006 Copy of Record, Page 52-53. Describes the copy of record. -Use Case 007 Data Flow List, Page 54-56. Describes each record that has been loaded into the system, and includes a history record which shows the history of all activity associated with that record.

CROMERR System Checklist	
18d. Inclusion of other information necessary to record meaning of document	
	Business Practices: The ERIS stores the data file in the database as well as metadata about the data file. This metadata includes facility, data flow type, record ID, user, record status, date and time of activity, and checksum. This information is presented with the copy of record and the metadata is presented with the Data Flow List.
	System Functions: The ERIS stores the data file in a record in the database that tracks all data flows, and this record has a unique ID number. The database also has a history table with a 1-to-many relationship with the dataflow table, which associates multiple history records to each data flow record. This allows the ERIS to track the following data for each file uploaded, submitted, deleted or retracted in the system: facility, data flow type, record ID, user, record status, date and time of activity, and checksum. This information is displayed with the copy of record and the metadata is included with the Data Flow List.
	Supporting Documentation (list attachments): See Design Document; -Use Case 004 Upload Report, Page 30-37 under System Function (Page 32) it describes the data recorded with the upload transaction.

	-Use Case 005 Submit Report, Pages 41-48, under User Interface (page 43) it lists the data that will be recorded for the submit transaction. -Use Case 006 Copy of Record, Page 52-53. Describes the copy of record. -Use Case 007 Data Flow List, Page 54-56. Describes each record that has been loaded into the system, and includes a history record which shows the history of all activity associated with that record. -Entity Relationship Diagram, Page 74
18e. Ability to be viewed in human-readable format	
	Business Practices: Users with at least read access security can get into the system to view, print or download a copy of the "Copy of Record" in human readable format anytime after a file is uploaded for records of facilities and data flow types for which they are assigned permission.
	System Functions: The ERIS has a tool to allow users to display the Copy of Record for a record that they have appropriate security to view. It does this by first taking the uploaded data file and annotating it with labels so the data in that file can be displayed in a human readable format with data properly labeled. Then it displays this human readable data file on a page along with the metadata associated with that data file that allows the file to be fully qualified. The system also has the ability to display this same information (metadata and data file in human readable format) in a PDF file as a text file that users can view, print or download as a PDF file.
	Supporting Documentation (list attachments): See Design Document; -Use Case 006 Copy of Record, Page 52-53. Describes the copy of record.
19. Timely availability of copy of record as needed	
	Business Practices: The system allows the copy of record to be viewed anytime after the report is successfully uploaded. After a report is uploaded, an email can be sent to all users with submit authority for that facility and data flow type, so they can immediately log into the system to view the copy of record. After a report is submitted, the system will automatically send an email to the user submitting the report, and it can also be sent to any other email addresses the user specifies. Users with appropriate permission can, at that time, log in and view the copy of record for that data record. Also when a file is submitted, an exact copy of the uploaded data file is placed on a LAN. Appropriate Drinking Water program staff will have read only access to the LAN where the data file is stored. They will be able to read the file as soon as it has been submitted, but will not be able to modify or delete the file.
	System Functions: When a file has been successfully uploaded into the ERIS system, the copy of record for that file can be immediately viewed by any user with adequate permissions for that facility and dataflow type. When a file has been submitted, the system will put a copy of the submitted file onto the LAN, where appropriate Drinking Water Program staff will have read only access to the file. So drinking water program staff will have near instant access to a data file. The system provides an automated tool that can be used to send emails to all users with submit authority for a facility and data flow type, once a file has been uploaded into the system. After a file has been submitted, the ERIS will automatically send an email notification to the user's registered email address who submitted the file. If the user lists other email addresses during the submit process, the system will send emails to those users as well. Any user with adequate security permissions will have the ability to immediately access the copy of record.

	Supporting Documentation (list attachments): See Design Document; -Use Case 004 Upload Report, Page 30-37 under User Interface (Page 33) it describes that the copy of record will be available as soon as an upload is successful. -Use Case 005 Submit Report, Pages 41-48, under System Function (page 42) it indicated that a copy of the data file will be put on the LAN. -Use Case 006 Copy of Record, Page 52-53. Describes the copy of record.
CROMERR System Checklist	
20. Maintenance of copy of record	
	Business Practices: The system will maintain the copy of record which includes an exact copy of the data uploaded and submitted for a length of time that meets the record retention requirements specified in the Safe Drinking Water Act. The documents may be maintained within the system longer, depending on the frequency of archiving records. In no case will the document of record be removed in a time that is less than that specified by the record retention schedule specified in the Safe Drinking Water Act. When documents are archived, a system administrator will be given a request signed by the dataflow type administrator and by the appropriate and responsible North Dakota Department of Health, Environmental Health Section program manager. The system administrator will archive the records specified by copying them to electronic media, where they will be stored, then remove those records from the ERIS database and the LAN as appropriate. System administrators will not delete any data from the system on their own. The databases where the records are stored are all on the North Dakota Information Technology Department (ITD) servers. These servers are in a server cluster that uses Redundant Array of Independent disks (RAID), so no data will be lost if a server should fail. The data is backed up on a nightly basis to a tape backup system, and the backups are stored in a secure location. The ITD servers are all located in a secure server room that is environmentally controlled and that has security, so only authorized personnel have access to the room. SQLServer database administrators are disinterested parties who work for the North Dakota Information Technology Department and have authority to setup and backup the database. SQLServer database administrators will not delete or update any data within this database or on the LAN.
	System Functions: The system is designed with limited access so only a system administrator with proper authority can remove records from the database used for ERIS and from the LAN. The system allows a person with Submit authority for a data flow type to mark a record as “deleted” or “retracted” for the records for which they have permission. However, this does not delete the data file in the database. Also, when a file is uploaded and submitted, the checksum of that data is stored with the copy of record so it can always be verified that it is the same data that was uploaded and submitted. The system stores information on each activity performed on a record of data (upload, submit, delete, retract) and these are the only actions that can be performed on a record. Therefore, a history of all activity associated with data uploaded to the system is maintained within the system. The database has the audit logging and transaction logging feature activated, so if anyone logs into the database, the user and time of access will be recorded. Also, if anyone changes data within the database itself, bypassing the front end of the application, it will be recorded. Both the transaction logs and audit logs are backed up nightly to secure tape storage by a SQLServer database administrator as per the North Dakota Information Technology Department server backup protocol.

	Supporting Documentation (list attachments): See Design Document; -Additional Considerations, (Page 71) item 7 indicates that the system will not delete any records. Attachment#03 System Administrator Request to Delete and Archive records from ERIS Reporting System. This form will be used by the dataflow type administrator to remove records from the system and archive them, provided the records have exceed their retention time as specified by the Safe Drinking Water Act. The archiving process is performed by a system administrator. This form must be signed by a user who is a dataflow type administrator and by the program manager for that Environmental Health Section program area.