

SERC Compliance Monitoring and Enforcement Program

Implementation Procedure 9.0 Data Management and Confidentiality



SERC CMEP Implementation Procedure 9.0: Data Management and Confidentiality

Revision History

Revision	Date	Originator	Comments
0	May 31, 2007	T. Galloway	Document Origination.
1	October 2, 2008	A. Koch	Updated document retention to 7 years for SERC. Added information regarding confidential information and critical energy infrastructure information. Provided examples of specific Compliance Activities
2	May 13, 2009	T. Galloway	Rewritten to better describe the Data Management and Confidentiality processes.
3	October 8, 2009	N. Fallon	Changes made regarding redaction of CEII materials. Inserted "some" in NOTE in Section 5.4.1.1 and inserted "shall require" in Section 5.4.1.2.

Cross Reference Table

The procedures listed in the table below refer to this procedure, Compliance Implementation Procedure 9.0 Data Management and Confidentiality. As revisions are made to Procedure 9.0, the Originator should review the procedures listed to determine if corresponding changes to these procedures are warranted.

Procedure Number	Procedure Title
5.0	Consolidated Compliance Enforcement Tracking

Responsible SERC Group(s)

SERC Board Compliance Committee (BCC)

Review and Re-Approval Requirements

This document will be reviewed every two years or as appropriate for possible revision. The existing or revised document will be re-approved by the SERC Board Compliance Committee (BCC), distributed by the Compliance Director to all applicable SERC staff, and posted on the website for Registered Entity and SERC Member reference.

List of Appendices

None

Table of Contents

1.0	Purpose	4
2.0	Responsibilities	4
3.0	References	4
4.0	Definitions	4
5.0	Procedure Steps	6
5.1	Retention of Electronic Records and Data	6
5.2	Disposal of Electronic Records and Data	6
5.3	Management of Confidential Compliance Information – General requirements.....	6
5.4	Protection of Confidential Information	7
5.5	Handling of Confidential Information.....	9
5.6	Requests for Confidential Information (Reference ROP Section 1503)	11
5.7	Provision of Information to FERC / Other Regulatory Authorities (Ref ROP 1505).....	12
5.8	Transmission of confidential compliance information.....	13
5.9	Data Loss or Theft of Confidential Information.....	14
5.10	Miscellaneous Topics.....	14

SERC CMEP Implementation Procedure 9.0: Data Management and Confidentiality

1.0 Purpose

The purpose of this procedure is to outline how SERC Compliance will manage confidential information, including critical energy infrastructure and physical / cyber security information, related to Compliance Program activities. Such information includes but is not limited to requested data and work papers related to processing of Compliance Audits, Self-Certifications, Spot Checking, Compliance Violation Investigations, Self-Reporting, Periodic Data Submittals, Exception Reporting, Complaints, Compliance Inquiries, and Hearings. This procedure implements and augments Section 1500 of the NERC Rules of Procedure (ROP) and Section 9.0 of the SERC / NERC Compliance Monitoring and Enforcement Program (CMEP) document.

2.0 Responsibilities

- SERC Compliance Director is responsible for implementation of this procedure.
- SERC compliance staff, contractors, consultants (collectively SERC compliance personnel), and authorized industry subject matter experts are responsible for compliance with the NERC Rules of Procedure (ROP) section 1500 and this procedure as it relates to information and/or data obtained in connection with SERC compliance activities.
- Audit, Spot-Check, and Compliance Violation Investigation (CVI) Team Leaders are responsible for ensuring compliance to this procedure by the team members, particularly during field activities.
- Submitting entities (typically SERC Registered Entities but could include entities seeking registration) are responsible for proper identification of confidential information in accordance with section 1500 of the NERC ROP and as further described in this procedure. Submitting entities are also responsible for promptly notifying SERC regarding any change in classification of confidential information.

3.0 References

- NERC Rules of Procedure, Section 1500 - Confidential Information
- SERC / NERC CMEP Section 9.0
- NERC BOT Approved Reliability Standards
- SERC Member Confidentiality Agreement
- SERC Non-Member Entity Confidentiality Agreement
- SERC Non-Member Individual Confidentiality Agreement
- SERC Data Retention Policy
- Compliance Staff Guide – Data Management and Confidentiality

4.0 Definitions

There are two general classes of information related to the compliance program, public

SERC CMEP Implementation Procedure 9.0: Data Management and Confidentiality

and non-public / confidential.

4.1 Public information does not contain any data or material meeting one or more definitions of confidential information. Public information also includes information that has been made ready for public disclosure based on factors such as related violations achieving confirmed status, proper redaction of confidential content, or a determination requiring confidential information be made public by a properly authorized regulatory agency. Examples of public information include generic (non entity specific) compliance statistics, documents describing certain processes and staff expectations, etc.

4.2 Non-public / confidential information meets one or more of the confidential information definitions from the NERC Rules of Procedure, Section 1501. These are restated directly as sections 4.2.1 to 4.2.4 below. Sections 4.2.5 and 4.2.6 further clarify selected compliance staff generated confidential information. All non-public / confidential information is considered sensitive and will be controlled, as appropriate, based on this designation. The definitions are as follows:

4.2.1 **Confidential information** means (i) confidential business and market information; (ii) critical energy infrastructure information; (iii) personnel information that identifies or could be used to identify a specific individual, or reveals personnel, financial, medical, or other personal information; (iv) work papers, including any records, produced for or created in the course of an evaluation or audit; (v) investigative files, including any records produced for or created in the course of an investigation; or (vi) cybersecurity incident information; provided, that public information developed or acquired by an entity shall be excluded from this definition.

4.2.2 **Confidential business and market information** means any information that pertains to the interests of any entity, that was developed or acquired by that entity, and that is proprietary or competitively sensitive.

4.2.3 **Critical Energy Infrastructure Information, or CEII** is defined as specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure that: (1) relates details about the production, generation, transportation, transmission, or distribution of energy; (2) could be useful to a person in planning an attack on critical infrastructure; (3) does not simply give the general location of the critical infrastructure.”

4.2.4 **Cybersecurity incident information** means any information related to, describing, or which could be used to plan or cause a cybersecurity incident as defined in 18 C.F.R. [Code of Federal Regulations] 39.1.

4.2.5 **Compliance information associated with in-process compliance actions** (See Sections 4.2.1 (iv) and (v) above). This information will be treated as

SERC CMEP Implementation Procedure 9.0: Data Management and Confidentiality

confidential until it is appropriate for public disclosure by virtue of proper completion of the activity such as confirmation of associated alleged violations. Public disclosure of confirmed violations is made via a Notice of Penalty properly filed with FERC. Relevant “record” information can include notices, settlements, penalty amounts, mitigation plans, entity completion certification, etc. Any subparts of the record associated with a Notice of Penalty pertaining to sections 4.2.1 (i), (ii), (iii), or (vi) will be addressed through proper redaction or authorization for public release consistent with those sections. Public disclosure of audit reports will be after any associated possible alleged violations are dispositioned and, the report has been properly redacted and marked.

4.2.6 Compliance internal reports and other documents used in performance of compliance activities that contain confidential information such as alleged (as yet unconfirmed) violation related information specific to one or more than one entity. Examples include Tracking All, Mitigation Plan Status reports, etc.

4.2.7 Confidential personnel information (Section 4.2.1 (iii) above) for SERC personnel is controlled by SERC Human Resources and is not otherwise addressed within this procedure.

5.0 Procedure Steps

5.1 Retention of Electronic Records and Data

This section has been superseded by the SERC Corporate Document Retention and Procedure Document.

5.2 Disposal of Electronic Records and Data

This section has been superseded by the SERC Corporate Document Retention and Procedure Document

5.3 Management of Confidential Compliance Information – General requirements

SERC Compliance handles considerable information, both electronic and hardcopy, and some of the information is classified as non-public / confidential. This procedure outlines the steps necessary for proper conduct related to non-public / confidential information including requirements for identification, protection marking, receipt, storage, transmittal, meetings, and disclosure.

5.3.1 Only personnel under current confidentiality / non disclosure agreements are authorized to access any confidential compliance information. SERC compliance staff, consultants, and contractors complete a confidentiality / non

SERC CMEP Implementation Procedure 9.0: Data Management and Confidentiality

disclosure agreement upon hire.

- 5.3.2 Personnel are provided access only to that information for which they are authorized and have a legitimate need. For example, industry subject matter experts are provided access to confidential information only after being authorized by completion of a confidentiality / non-disclosure agreement. Access to confidential information is restricted to that associated with the specific activity they are supporting, such as a specific compliance audit. Discussion of or access to non-related confidential information is prohibited.
- 5.3.3 Confidentiality requirements are periodically reinforced to compliance personnel and are reviewed prior to conduct of certain meetings with entity personnel such as Board Compliance Committee meetings, Compliance Advisory Group meetings, Compliance Seminars, and other related forums.
- 5.3.4 Unescorted access to the Compliance Department is prohibited by anyone other than SERC employees and SERC contractors under current confidentiality / non disclosure agreements.
- 5.3.5 Requests for confidential information by FERC or other regulators or, from third parties (representatives from outside the ERO) shall be promptly brought to the attention of the Compliance Director.
- 5.3.6 Compliance staff is not authorized to speak directly with any members of the media. Contact with, or requests for information from, any media personnel are to be promptly reported to the SERC President and Compliance Director.
- 5.3.7 Personnel are to immediately raise questions or concerns, including any potential instances of improper access to (including actual or suspected instances of cyber intrusion or hacking) or inadequate management or control of confidential information to the attention of the Compliance Director.

5.4 Protection of Confidential Information

NOTE: Certain details regarding processes for marking and control of confidential information may itself be confidential to compliance personnel. Such details are controlled via internal staff processes.

5.4.1 Identification of Confidential Information

5.4.1.1 Entity submittals

- Per NERC ROP Section 1500 users, owner, and operators and other “submitting entities” are required to mark information as confidential

SERC CMEP Implementation Procedure 9.0: Data Management and Confidentiality

that reasonably conforms to one or more of the definitions of confidential described in ROP 1502 and restated in steps 4.2.1 to 4.2.4 above. Submitting entities for compliance related confidential information will typically be SERC registered entities but, could include others including unregistered entities seeking registration. Elsewhere in this procedure submitting entities will be referred to as entities.

- Entities shall mark all information provided to SERC as confidential that meets one or more of the above definitions. In these submittals the entity should indicate all categories of confidentiality that apply per steps 4.2.1 to 4.2.4 above and reference the relevant sections within the information provided.
- Entities shall use file names of any electronic files submitted to SERC, and document headers in any electronic or hard copy files submitted to SERC, that clearly state whether the information provided contains any Critical Energy Infrastructure Information (CEII) of Cyber Security Incident information.

NOTE: Clear understanding of which aspects of the information represent CEII information allows for proper redaction of that content in the event that documents containing some CEII information are required to be filed as part of the record of a confirmed violation.

- Entities are to contact compliance staff with any questions or concerns regarding proper marking of the documents and required method of transmission given the content.
- Entities shall make known to compliance staff, in writing, any prohibition against public disclosure including the associated basis.
- Entities shall promptly make known to staff any information previously marked as confidential that no longer qualifies for that designation.
- Entities shall contact SERC compliance staff to coordinate appropriate transmission of the confidential information based on the confidential categories identified.
- NOTE: SERC compliance takes no responsibility for disclosure of entity information that has not been appropriately marked as confidential (including omissions, wrong classification, and over-classification).
- SERC compliance will preserve entity confidentiality markings unless

SERC CMEP Implementation Procedure 9.0: Data Management and Confidentiality

a needed modification is identified and is properly coordinated with the entity.

5.4.1.2 SERC Compliance personnel developed confidential information

- The majority of information handled by compliance personnel relates to possible alleged violations associated with one or more entities (Sections 4.2.5 and 4.2.6 above) and is therefore treated as confidential information until such time as it is filed with FERC.
- Compliance developed confidential information shall be marked as in accordance with applicable internal staff guidance. Amplifying suffixes may be included as appropriate. As example:
 - Confidential – Internal SERC Use Only
 - Confidential – For Settlement Discussions
 - Confidential – Until filed with FERC

Note: Some information needed to support Notice of Penalty (NOP) filings is treated as confidential but, may require omission of confidential marking at the time of filing with FERC to eliminate a contradiction while properly publicly disclosed.

- Compliance personnel will coordinate proper treatment of any information identified by an entity as confidential per sections 4.2.2 to 4.2.4 above that is required to support the record for a confirmed violation (refer to NERC CMEP for definition of confirmed violation and related process steps). This treatment shall require redaction of specific sections containing CEII or Cyber Security related information.

5.5 Handling of Confidential Information

5.5.1 General requirements

- 5.5.1.1 Compliance personnel and other authorized personnel are required to employ all reasonable caution to protect against unintended or improper disclosure of confidential information. These precautions include but are not limited to ensuring personnel with access are under current confidentiality agreements, taking possessions of only those materials necessary to execute compliance responsibilities, properly securing / storing confidential information both at rest and in transit, and disclosing / distributing confidential information only as authorized. Personnel that improperly disclose confidential information are subject to sanctions

SERC CMEP Implementation Procedure 9.0: Data Management and Confidentiality

including temporary or permanent loss of access to such information.

5.5.2 Transfer, transport, and storage of electronic confidential information

- 5.5.2.1 Any entity confidential information meeting section 4.2.2 to 4.2.4 definitions determined as not required for the record of a compliance action (compliance audit evidence, possible alleged violation, etc.) should not be taken into SERC possession. Any such information in SERC possession that is subsequently deemed not required will be returned to the appropriate entity or destroyed.
- 5.5.2.2 The preferred and typical method to store confidential entity information that meets one or more of the section 4.2.2 to 4.2.4 definitions is to load all such information onto encrypted / password protected media and then physically secure it within the SERC offices. Storage of such information on the secure S-drive or a properly secured committee site, as determined necessary by the staff single point of contact (SPOC) or Audit Team Leader (ATL), is acceptable to promote efficient transfer and review of the information.
- 5.5.2.3 Confidential entity information used as evidence for a CIP compliance activity is afforded specific treatment. SERC compliance personnel will typically review such evidence at an entity site and using only entity equipment. Such confidential information will not be loaded onto the computers or jump drives of any SERC compliance personnel and authorized subject matter experts. At the conclusion of the activity, the entity will load relevant evidence onto an encrypted jump drive or other media. This media will be stored in a secure location.
- 5.5.2.4 Confidential electronic information as defined by sections 4.2.5 and 4.2.6, such as related to a compliance audit or enforcement action, and not covered above is typically maintained within the appropriate folders on the secure compliance S-drive that constitutes the formal “record” for that activity. The applicable compliance personnel (SPOC or ATL) can allow for temporary storage of confidential information on a secured committee site to facilitate secure information transfer provided that site access is limited to properly authorized individuals with need and, the committee site naming convention does not improperly disclose the nature of any confidential action.
- 5.5.2.5 Compliance personnel transporting confidential electronic information will do so by loading this information on a SERC laptop, jump drive, or other media with appropriately configured encryption / password protection.

SERC CMEP Implementation Procedure 9.0: Data Management and Confidentiality

- 5.5.2.6 Redundant copies of confidential compliance information stored on laptops, jump drives, and other media / locations are to be properly controlled and promptly eliminated once the information is properly stored with the location of the final “record”.
- 5.5.3 Transfer, transport, and storage of hardcopy confidential compliance information
 - 5.5.3.1 Hardcopy confidential information shall be marked with the applicable confidentiality designations per the applicable internal staff guidance.
 - 5.5.3.2 Compliance personnel shall minimize the amount of hardcopy information taken outside the secure compliance work area. This information should typically consist only of that information essential to execute a particular task (i.e. compliance audit).
 - 5.5.3.3 Compliance personnel shall not leave hardcopy confidential compliance information unattended outside of secure compliance work areas.
 - 5.5.3.4 Compliance personnel must secure all confidential hardcopy information at the end of each work day.
 - 5.5.3.5 Compliance personnel shall destroy hardcopy confidential information once it is no longer needed and, an electronic copy of that information necessary to satisfy documentation retention requirements has been properly created and stored.
- 5.6 Requests for Confidential Information (Reference ROP Section 1503)
 - NOTE: NERC and the regional entities are authorized to exchange confidential compliance information such as evaluations, audits, and investigations in the furtherance of the compliance and enforcement activities; on the condition they continue to maintain the confidentiality of that information. Typical exchanges of information with NERC and others regions are considered permitted disclosures and are not construed as “requests for information” by either party as described below.
 - 5.6.1.1 Any requests for confidential information shall be directed to the Compliance Director.
 - 5.6.1.2 Confidential information will only be made available to a requester with a demonstrated need and following the below protocol:
 - 5.6.1.2.1 Request is in writing and clearly marked “request for confidential

SERC CMEP Implementation Procedure 9.0: Data Management and Confidentiality

information”.

5.6.1.2.2 The request provides the bases and qualifications for the request and the intended use.

5.6.1.2.3 The requester specifies whether it seeks public disclosure or not. If not, the requester must execute a properly composed confidentiality agreement.

5.6.1.2.4 The Compliance Director, or designee, will promptly notify the SERC President of the request for confidential information.

5.6.1.2.5 The “submitting entity” (that entity which initially provided the confidential information to SERC) will be notified of the request for confidential information and provided an opportunity for comment.

5.6.1.2.6 Based on the merits of the request and the submitting entity response the SERC President (or delegate declared in writing) will determine whether to release the information.

5.6.1.2.7 If the decision is made to release the information, the submitting entity is afforded 21 days written notice to seek alternative action.

5.6.1.2.8 If the decision is to not release, the requesting entity can appeal the decision to NERC within 30 days of the decision.

5.6.1.2.9 Determinations on requests for confidential information are posted to the SERC website.

5.7 Provision of Information to FERC / Other Regulatory Authorities (Ref ROP 1505)

5.7.1 Compliance staff will promptly notify the Compliance Director of any requests for confidential compliance / reliability related information by a regulatory authority.

5.7.2 The Compliance Director will notify the SERC President of the request.

5.7.3 The Compliance Director, or designee, will contact the regulatory authority to understand the scope, bases, and desired delivery schedule for the requested information.

5.7.4 Unless directed otherwise by the requesting regulatory authority, the SERC Compliance Director, or designee, will provide contemporaneous notice of the

SERC CMEP Implementation Procedure 9.0: Data Management and Confidentiality

request to the entity that submitted the confidential information.

5.7.5 All confidential markings on such documents will be preserved and the requesting regulatory authority will be made aware of the confidential status of the requested information.

5.7.6 The Compliance Director, or designee, will provide the requested data in a form, format, and delivery method suitable to the request and the nature of information being provided.

5.8 Transmission of confidential compliance information

5.8.1 Exchange of compliance information, including confidential information, between SERC, NERC, and other regions is necessary to the implementation of the compliance monitoring and enforcement program. These are considered permitted disclosures (Reference ROP 1506 (2)), provided confidential information is maintained as such. Confidential information defined by step 4.2.5 constitutes the majority of the information meeting this case. Transmission of such confidential information is authorized provided there is a recognized need and the associated authorized recipient(s), including contact information, is known to SERC staff transmitting the information.

5.8.2 Routine transmission of confidential information to NERC will be made to satisfy reporting requirements described under CMEP section 8.0. Transmission of such information will be in the form dictated by NERC.

5.8.3 The Audit Program Manager is authorized to distribute draft and final non-public audit and spot-check reports to team participants, subject entities, and NERC. Such reports are to contain markings per applicable internal staff guidance.

5.8.4 Transmittal of information marked by entities as confidential per sections 4.2.2, 4.2.3, or 4.2.4 outside of compliance staff must be authorized by the Compliance Director, Audit Program Manager, or Compliance Enforcement Manager. The authorizing manager will determine the proper scope, formatting, and transmission method for the subject information per applicable internal staff guidance. All entity marks of confidentiality will be preserved unless required changes are reconciled with the applicable entity.

5.8.5 Compliance personnel will coordinate with the submitting entity and NERC in cases where information marked as confidential by the entity must be filed with NERC and FERC as part of the public record for a confirmed violation. In such cases, the entity must clearly identify any sections of the information

SERC CMEP Implementation Procedure 9.0: Data Management and Confidentiality

that meet the definitions of section 4.2.2, 4.2.3, 4.2.4, and 4.2.7 such that it can be appropriately redacted prior to filing.

NOTE: It is improper to mark entire documents as confidential or CEII without specificity as a means to preclude filing.

5.8.6 Transmittal of confidential information meeting the definition in section 4.2.6 will not be made outside of SERC compliance without Compliance Director authorization, except as otherwise addressed in this section.

5.9 Data Loss or Theft of Confidential Information

SERC compliance personnel and authorized industry subject matter experts will make every reasonable effort to secure and protect written and electronic compliance activity information while it is being used in the performance of those activities. In the event that a computer or other electronic device containing confidential data is lost / stolen or a confidential document is lost / stolen, the employee must notify the Compliance Director and Manager of IT immediately.

5.10 Miscellaneous Topics

5.10.1 Registration and Certification Confidentiality

To maintain the integrity of the NERC Organization Registration and Certification Program, SERC staff, certification audit team members, and committee members shall maintain the confidentiality of information provided by entities in order to become registered or certified as reference Section 500 of the NERC Rules of Procedure. SERC staff shall have appropriate codes of conduct and confidentiality agreements for staff and other certification audit participants. Individuals not bound by ERO or approved SERC codes of conduct and who serve on certification-related committees or audit teams shall sign an ERO confidentiality agreement prior to participating on the committee or team. SERC staff, committee, and audit team members shall maintain the confidentiality of any certification-related discussions or documents that are designated as Confidential. SERC staff, committee, and audit team members shall treat as confidential the individual comments expressed during audits and report-drafting sessions.

Copies of notes, draft reports, and other interim documents developed or used during a certification audit shall be destroyed after the public posting of a final, uncontested report, or as directed by Certification or Audit Team Leads.

Information deemed by an entity, SERC, or NERC as confidential or critical

SERC CMEP Implementation Procedure 9.0: Data Management and Confidentiality

energy infrastructure information shall not be distributed outside of a committee or team, or released publicly.

5.10.2 Confidentiality of Complainants

SERC compliance personnel shall not disclose the identity of any person or entity reporting a complaint to SERC. SERC compliance personnel will maintain the identity of any known complainant as confidential whether anonymity is requested or not. (Also reference procedure 3.8)

5.10.3 Maintaining Confidentiality during Meetings

SERC staff, contractors, industry subject matter experts and others participating in Compliance Program activities will be reminded prior to the start of applicable meetings, conference calls or discussions involving confidential information which consists of SERC compliance personnel and more than one other party, of confidentiality requirements. SERC compliance personnel will ensure that all individuals involved in confidential discussions are bound by a Non-Disclosure agreement or are covered by a current signed confidentiality agreement.