MIDWEST RELIABILITY ORGANIZATION

380 St. Peter St, Suite 800
Saint Paul, MN 55102
www.MRO.net
651-855-1760

Policy and Procedure 5: Confidentiality Policy

1. Objective

The objective of this policy and procedure is to maintain the confidentiality of the sensitive business information of Midwest Reliability Organization (MRO), MRO Members and others subject to Reliability Standards ("registered entities" on the NERC Registry).

2. Policy

In connection with preparing and/or receiving reports and engaging in other duties regarding the delegated responsibilities of MRO, directors and members of any organizational group may gain access to Confidential Information regarding MRO, MRO Members, and registered entities, including personnel and operations information. It shall be the responsibility of every director and organizational group member to maintain the confidentiality of such information in accordance with the policy set forth herein.

3. Responsibilities

In furtherance of the above policy, directors and members of any organizational group shall keep in confidence and not copy, disclose, or distribute any information designated as "Confidential Information," except as otherwise directed by a determination of a majority of the board of directors or as required by law.

4. Obligation to Review and Agree to Confidentiality Policy

Each director, or agent of MRO, and any member and its representatives who serve on any MRO organizational group shall annually sign a statement which affirms such person:

- Has received a copy of the confidentiality policy, and
- Has read and understands the policy, and
- Has agreed to comply with the policy.

5. Provisions

"Confidential Information" includes, but is not limited to:

Proprietary or confidential information, technical data, trade secrets or know-how, including, but not limited to, research, product plans and designs, products, services, customer lists and customers, markets, software, developments, inventions, processes, formulas, technology, designs, drawings, engineering, marketing, distribution systems, finances and other business information relating to such entity's operations that is not generally available to the public.

Personnel information that identifies or could be used to identify a specific individual or that reveals personnel, financial, medical, or other personal information.

Critical energy infrastructure information (CEII), defined as specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure that (i) relates details about the

380 St. Peter St, Suite 800
Saint Paul, MN 55102
www.MRO.net
651-855-1760

production, generation, transportation, transmission, or distribution of energy; (ii) could be useful to a person in planning an attack on critical infrastructure; and (iii) does not simply give the location of the critical infrastructure. “Critical infrastructure” consists of existing and proposed systems and assets, whether physical or virtual, the incapacity or destruction of which would negatively affect security, economic security, public health or safety, or any combination of those matters. CEII shall not be distributed outside of an organizational group, nor released publicly.

Knowledge of potential violations of Reliability Standards and Organizational Standards. This includes work papers, including any records produced for an evaluation or audit, and investigative files, including any records produced or created in the course of an investigation.

Cybersecurity incident information, consisting of any information related to, describing, or which could be used to plan or cause a cybersecurity incident as defined in 18 C.F.R. § 39.1.

Confidential Information does not include (i) information already known or independently developed by a director or organizational group member; (ii) information in the public domain through no wrongful act of the director or organizational group member, or (iii) information received by a director or organizational group member from a third party who was free to disclose it.

This obligation to maintain the confidentiality of Member-related and MRO-related Confidential Information applies both during and after a director’s or organizational group member’s term of service.

6. Permitted Disclosures

- Nothing in this policy shall prohibit MRO’s disclosure of a violation of a Reliability Standard at the point when the matter is filed with an appropriate governmental authority as a notice of penalty, the “violator” admits to the violation, or the alleged violator and MRO reach a settlement regarding the violation.
- Nothing in this policy shall prohibit MRO from exchanging with NERC and other Regional Entities Confidential Information related to evaluations, audits, and investigations in furtherance of the compliance and enforcement program, on condition they continue to maintain the confidentiality of such information.

7. Remedies for Improper Disclosure

If the confidentiality provisions set forth above are violated, the person violating the confidentiality provisions and any member organization with which the individual is associated may be subject to appropriate action by MRO or NERC, including prohibiting participation in future compliance and enforcement activities.