NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

NERC Employee Code of Conduct

Standards of Performance

In connection with their adherence to the other provisions of this Code of Conduct and the Company's policies, NERC employees have three recognized duties to the organization: the duties of care, loyalty, and adherence to objectives.

Duty of Care

The duty of care concerns the competence of the employee in performing his or her duties and generally requires the employee to use the care that an ordinarily prudent person would exercise in a like position and under similar circumstances in respect to the management and administration of the affairs of the organization. This duty of care is generally thought to have two components: the time and attention devoted to the organization's affairs and the skill and judgment reflected in decisions that affect the organization.

Duty of Loyalty

The duty of loyalty requires the employee's faithful pursuit of the interests of NERC rather than his or her own financial or other interests or the interests of another person or organization. The duty of loyalty includes compliance with NERC's conflict of interest guidelines and policies.

Duty of Adherence to Objectives

The duty of adherence to objectives requires that the employee devote himself or herself to assuring that the organization operates to further its stated objectives in conformance with the policies and structures of the organization set by senior management, consistent with legal, moral, and ethical requirements.

Collegiality and Demeanor

Key to NERC's success and effectiveness are good working relationships among NERC employees. NERC employees also serve a broad and diverse stakeholder community that looks to NERC for leadership and support on a wide variety of matters. Each employee has a responsibility to be open, honest, and respectful in communications with others and to be fair and impartial in all aspects of his or her deliberations and decision-making.

Confidential Information means (i) Confidential Business and Market Information, as defined below; (ii) Critical Energy Infrastructure Information, as defined below; (iii) personnel information that identifies or could be used to identify a specific individual, or reveals personnel, financial, medical, or other personal information (Personnel Information); (iv) work papers and investigative files, including any records produced for or created in the course of an evaluation, audit, investigation, enforcement action, or other activity conducted pursuant to the Compliance Monitoring and Enforcement Program; (v) confidential or classified information obtained from governmental entities; or (vi) Cyber Security Incident Information, as defined below. Confidential Information does not include information that (i) becomes generally available to the public other than as a result of improper disclosure; (ii) was legally available on a non-confidential basis prior to being made available; or (ii) becomes legally available on a non-confidential basis.

Confidential Business and Market Information means any information that pertains to the interests of any entity – including NERC, a Regional Entity, a NERC member, or any other third party – that was developed or acquired by that entity, and that is proprietary or competitively sensitive, including trade secrets (as defined by applicable law). This includes information that NERC considers private or non-public, that is not common knowledge outside the corporation or required by law or contract to be maintained as confidential, which might be of use to third parties or harmful to NERC.

Critical Energy Infrastructure Information means specific engineering, vulnerability, or detailed design information about proposed or existing Critical Infrastructure that (i) relates details about the 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 means 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.

Cyber Security Incident Information means any information related to, describing, or which could be used to plan or cause a data breach or Cyber Security Incident, as defined in Appendix 2 to the NERC Rules of Procedure.

To the extent permitted by law, each employee shall maintain the confidentiality of: (1) any Confidential Information of NERC or the Electricity Information Sharing and Analysis Center (E-ISAC) , of members of NERC or the E-ISAC, or of market participants to which the employee has access by virtue of his or her position with NERC or the E-ISAC (such information may include enforcement actions, cyber threats or incidents, data breach information, confidential or classified information obtained from governmental entities, or trade secrets (as defined by applicable law)); and (3) any Confidential Information of other third parties that has been provided to NERC or the E-ISAC under the terms of a confidentiality agreement. Confidential Information gained as a result of employment with NERC may not be shared with any individual, firm, or other organization during your employment with NERC or after your employment with NERC has ended, except in accordance with NERC rules or policies, or with the express consent of NERC management. In addition, with respect to any trade secrets (as defined by applicable law), the related policy protections contained herein survive for so long as the underlying information is deemed a trade secret by applicable law.

NERC personnel operating on behalf of the E-ISAC shall further protect any Confidential Information gained in such capacity and not share any E-ISAC Confidential Information with any non-E-ISAC personnel, except as provided for in the E-ISAC Code of Conduct or other applicable NERC or E-ISAC policies. No employee may copy, reveal, give or make known to anyone outside of NERC E-ISACE-ISAC any Confidential Information (or for E-ISAC Confidential Information, outside of the E-ISAC), without appropriate safeguards and authorization by management including, without limitation, limiting access to the least amount of Confidential Information to allow any third party to meet their obligations to NERC and making all third parties aware of the confidential nature of such information and all requirements related to its protection.

Safeguarding NERC Assets / Accuracy of Books and Records

NERC maintains internal controls to provide direction on protecting NERC assets and financial accountability. The controls are based upon the following principles.

Do not:

- Make personal use of NERC assets that creates any additional costs to NERC, interferes with work duties, or violates or is otherwise inconsistent with the intent of any NERC policies;
- Knowingly or negligently allow NERC property to be used to help carry out illegal, unethical, or improper acts; or
- Falsify financial information, accounts, records, or reports for any reason.
- Do not open or reply to messages purporting to be from popular social web sites, online payment processors, or IT administrators requiring personal or company information if you are not 100% sure of the requesting entity. Be extremely vigilant for spam and phishing attempts when opening and reading email. Contact NERC IT immediately if you are a victim of or suspect a phishing attempt.

Do:

- Prepare project contract, financial, and budget material with accurate information;
- Maintain books, accounts, and records in accordance with all applicable legal requirements and general accepted accounting principles, using enough detail to reflect accurately and fairly all transactions and key accounting assumptions; and
- Record transactions, including expenses, in a timely manner, so that no misleading financial information is created.

Use of Computer Resources

NERC invests in and uses computer resources (computer hardware, software, supporting infrastructure, network connections, and telecommunications equipment) to advance its business strategy and objectives. NERC permits employees to use NERC's computer resources for educational and personal use during lunch times and other non-business hours, so long as that use does not cause NERC additional expense, adversely affect those resources or the resources of others, or interfere with the employee performing his or her job duties.

Unless prohibited by law, the use of this technology, including but not limited to electronic mail and the Internet, is subject to monitoring by NERC. Employees have no expectation or right to privacy in any electronic information received, produced, or placed on the company's computer systems. Electronic information may be accessed and reviewed by NERC personnel responsible for oversight of the company's computer systems and enforcement of corporate policies, notwithstanding the use of passwords.

Computer software (computer programs, databases, and related documentation), whether purchased or licensed from a supplier or developed by NERC, is protected by copyright and may also be protected by patent or as a trade secret. Employees must comply with the terms and conditions of the license agreements, including provisions

not to copy or distribute materials covered by these agreements. Employees must comply with NERC security and virus protection policies.

Use of the Internet, intranet, and electronic mail should be in support of and to advance NERC's business and overall success. Any personal use of these technologies must not create additional costs for NERC, interfere with work duties, or violate any NERC policies, including policies related to the prohibition of defamatory, offensive, or threatening messages. Electronic mail messages should never be created, received, or transmitted that include obscene statements or that contain derogatory comments regarding co-workers or others. Similarly, electronic mail messages should never contain any improper or offensive materials relating to such topics as race, sex, age, religion, national origin, sexual orientation, or disability. NERC's policy prohibiting discrimination or harassment encompasses the electronic mail system, and any violation of that policy will be grounds for discipline up to and including termination of employment.

Understand and abide by these guidelines on the use of NERC's computer resources:

- Do not browse non-business web sites during business hours. Such sites include, but are not limited to, social networking (Facebook, Twitter, etc.), entertainment (e.g., online gaming, TV and movie sites, sports, celebrity gossip, etc.), and shopping.

- Never send, receive, or download any material, including pictures, videos, or music files that contain prohibited content as cited in the Code of Conduct Policy. This includes the sending, receiving, downloading, displaying, printing, or otherwise disseminating information that is sexually explicit, profane, obscene, harassing, threatening, intimidating, fraudulent, racially offensive, defamatory, or otherwise unlawful.

- Do not store copyrighted material such as videos, movies, and music that you have purchased for personal enjoyment on NERC's shared file servers or e-mail servers. Only devices approved by Information Technology (IT) may be used to store or transmit NERC data. Except as otherwise approved by the Director of Information Technology and Services, it is not permissible to send documents to your personal email address, store data on devices not owned by NERC or approved by the Director of Information Technology, or use non-IT-supported services such as cloud-based services not specifically authorized by the Director of Information Technology (e.g., Dropbox, etc.). Employees who have large storage needs should open a helpdesk ticket and outline their storage requirement.

- Do not store large or excessive amounts of personal files, including digital photographs, on NERC's shared file servers. Exceptions may include storage of small amounts of family or personal photos to the extent not otherwise inconsistent with these policies or consuming much storage space.

- Do not download or install unlicensed computer software, and, more generally, do not install non-standard software without prior authorization from IT (refer to the IT Help Desk Handbook for more information). Non-standard software is subject to removal.

- Do not purposefully disable or otherwise contravene the controls put in place to monitor and log computer usage.

Name, Logo, and Other Intellectual Property

NERC's name, logo, inventions, processes, and innovations are all valuable assets. These assets are NERC "intellectual property," and their protection is vital to the success of NERC's activities. In addition, NERC employees must respect the intellectual property rights of others. Violation of others' intellectual property rights may subject both the individual and NERC to substantial liability, including criminal penalties.

Understand and abide by these limitations on the use of intellectual property:

- Copyrights protect works like articles, drawings, photographs, video, music, audiotapes, and software and generally prohibit unauthorized copying or downloading of these works. Do not copy these materials without first determining that NERC has obtained permission from the copyright holder or that other limited copying is legally permitted. Consult with the general counsel if you have questions. Do not copy or distribute software or related documentation without reviewing the license agreement.

- Trademarks and service marks are words, names, and symbols that help consumers recognize a product or service and distinguish it from those of competitors. The use of NERC's name and logo must be properly authorized or licensed. The general counsel reviews requests for use of the NERC name, service marks, and trademarks. If you observe practices that are inconsistent with this policy, contact the general counsel. Do not use anyone else's trademark or service mark without permission.

    - All third-party use of NERC's trademarks is subject to the "nominative use rules" that allow the use of the trademark or name of the trademarked entity in a way that is minimal and does not imply a sponsorship relationship with the trademark owner (NERC). It is important to enforce this policy when NERC is sponsoring an event (e.g. the Grid Security Conference) to ensure that sponsoring vendors are not improperly creating an association with or an endorsement by NERC. NERC's trademarks should be used only to refer to NERC as the Electric Reliability Organization, NERC activities (e.g. the Grid Security Conference), or NERC Reliability Standards. There should be no third-party use of the NERC logo/symbol trademark in any form. Any questions regarding such uses should be directed to the general counsel.

- Patents permit inventors to exclude others from making, using, or selling their inventions. Only use inventions patented by others within the terms of a license agreement.

- A trade secret is valuable information that creates a competitive advantage by being kept secret. Treat as trade secrets and keep confidential all confidential and business market information of NERC and all similar information of other companies and persons that NERC has received under a confidentiality agreement.

- Intellectual property (that may include, among other items, inventions, discoveries, creations improvements or designs) that you create on behalf of NERC during the course of your employment is deemed "work made for hire" (as defined in the United States Code) and belongs to exclusively NERC, which includes copyrights, trademarks and patents.

    - As part of acknowledging this code of conduct, you agree to transfer and assign all intellectual property created by you on behalf of NERC during the course of your employment with NERC.

    - You also agree to share any innovations or inventions you create with your supervisor so that

NERC can take steps to protect these valuable assets.

- You also further agree **not** to share any potential inventions or discoveries with third parties, except as permitted by NERC management and consistent with applicable company policies.

- Employees shall cooperate and assist NERC in establishing and protecting its interests in any such intellectual property, including signing any necessary documentation or obtaining registrations, as deemed reasonably necessary by NERC.

- In the course of employment with NERC, all employees, to the extent using open source software, will do so only with the authorization of management and will at all times comply with all applicable open source licenses.

Representation Policy

Unless specifically designated the authority and responsibility to do so by the chairman or the chief executive officer, employees are not authorized to speak or communicate on behalf of NERC, officially or unofficially.

Employees should be keenly aware of the public perception that they represent NERC, and consider whether their remarks in writing or orally may be incorrectly interpreted as an expression of NERC's views.

An employee not specifically authorized by the chairman or chief executive officer to speak on behalf of NERC or the Board of Trustees is obligated to identify oral and written statements as their personal opinion, and not as an official or unofficial position of NERC.

Employees may state NERC policy where this can be done accurately. They may also describe NERC activities, plans, and involvement where this can be done accurately and in a manner consistent with requirements for confidentiality.

Acknowledgement of Receipt and Review of Code of Conduct

I have carefully read the information in NERC's employee code of conduct and I fully understand it. I agree as a condition of my employment to comply with these policies. I further understand that failure to comply with these policies may result in disciplinary action.

I understand that nothing in this code of conduct constitutes a promise or guarantee as to the duration of my employment at NERC. Just as I am free to leave my employment with NERC at any time and for any reason, NERC has the right to terminate my employment at any time, without prior notice, and with or without cause. This is known as employment at will.

I acknowledge responsibility for complying with future changes in NERC's policies and practices as communicated to employees from time to time, whether or not I have signed an acknowledgement of such changes.

_____ _____

Employee Signature ***Date***