ENERGYUNITED ELECTRIC MEMBERSHIP CORPORATION

OPERATIONAL AND MANAGEMENT POLICY MANUAL

ENERGYUNITED MEMBERSHIP CORPORATION
OPERATIONS AND MANAGEMENT POLICY MANUAL
TABLE OF CONTENTS

OMP-01: OPERATIONS AND MANAGEMENT POLICY MANUAL 4

OMP-02: ORGANIZATION 6

OMP-03: BOARD-MANAGEMENT-EMPLOYEE RELATIONS 7

OMP-04: USE OF CONSULTANTS 9

OMP-05: LONG RANGE PLANNING 10

OMP-06: EMERGENCY RESTORATION PLAN 11

OMP-07: AREA COVERAGE AND LINE CONSTRUCTION 13

OMP-08: INSURANCE REQUIREMENTS 14

OMP-09: RETENTION OF CORPORATE RECORDS 15

OMP-10: DOCUMENT HOLD NOTICES AND ELECTRONIC DISCOVERY 25

OMP-11: MAINTAINING A SECURE PHYSICAL AND CYBER ENVIRONMENT 28

OMP-12: SECURING CONFIDENTIAL MEMBER AND EMPLOYEE DATA WHILE RETAINING AND DESTROYING RECORDS 30

OMP-13: PRIVACY OF MEMBER NON-PUBLIC INFORMATION 34

OMP-14: RED FLAG PROGRAM FOR IDENTITY THEFT AND CREDIT REPORTING ACCURACY 36

OMP-15: USE OF COOPERATIVE COMMUNICATIONS AND COMPUTER SYSTEMS 39

OMP-16: CYBERSECURITY INCIDENT MANAGEMENT 41

OMP-17: ACCEPTABLE USE POLICY 44

OMP-18: WEB ACCESSIBILITY 56

OMP-19: ACCEPTABLE USE OF ARTIFICIAL INTELLIGENCE 57

OMP-20: RELATIONSHIP WITH RURAL UTILITIES SERVICE AND NATURAL RURAL UTILITIES COOPERATIVE FINANCE CORPORATION 60

OMP-21: MEMBERSHIP IN OTHER ORGANIZATIONS 61

OMP-22: POLICY THAT COOPERATIVE IS NOT FOR SALE 62

OMP-23: POTENTIAL SALE OF ALL OR SUBSTANTIALLY ALL OF THE COOPERATIVE'S ASSETS TO ANOTHER ENTITY 66

OMP-24: HANDLING CASES OF METER TAMPERING, POWER THEFT, AND POWER DIVERSION 73

OMP-25: ELECTROMAGNETIC FIELDS 78
OMP-26: ENTERPRISE RISK MANAGEMENT 79

OMP-01: OPERATIONS AND MANAGEMENT POLICY MANUAL

Version: 2015.12.17

1. OBJECTIVE:

   To establish the basis for the formulation, approval, publication, and distribution of written operations and management policy statements to provide guidance to the Members, Board of Directors ("Board"), Chief Executive Officer ("CEO"), management, employees, contractors, and other persons and entities in furtherance of the purposes, objectives, plans, viewpoints, and operational requirements of the Cooperative.

2. POLICY CONTENT:

   a. The Board hereby recognizes its responsibility for operations and management policy planning and development through observation, study, and analysis of the affairs of the Cooperative which, together with the recommendations of the CEO, provide the basis for operations and management policy content.

   b. Operations and management policies will be developed and placed in written form. All operations and management policies shall be placed in a operations and management policy manual that is available to Members, Board of Directors ("Board"), Chief Executive Officer ("CEO"), management, employees, contractors, and other persons and entities in furtherance of the purposes, objectives, plans, viewpoints, and operational requirements of the Cooperative.

   c. If any position with the Cooperative referred to in operations and management policies is replaced by another position, then the operations and management policies shall be interpreted as referring to the replaced position without the necessity of any further action being taken.

   d. The Board may, in its sole discretion, modify operations and management policies at any time. The CEO and Corporate Attorney may make administrative corrections and non-substantive modifications to operations and management policies without Board approval. Administrative corrections and non-substantive modifications include, but are not limited to, format changes, spelling corrections, style modifications, numbering changes, etc.

3. RESPONSIBILITY:

   a. The Board is responsible for the review, consideration, and approval of operations and management policies.

   b. The CEO is responsible to the Board for recommendations covering the areas of need where operations and management policies are required, such recommendations shall

include the operations and management policy statement, content, and responsibility requirements which are to be reviewed for revision, correction, and appropriate action by the Board.

c. The requirements for operations and management policies are to be determined by the Board in consultation with the CEO. The CEO is solely responsible for all internal operational procedure statements that are required relative to procedures necessary in the accomplishment of their responsibilities.

OMP-02: ORGANIZATION

Version: 2015.12.17

1. OBJECTIVE:

   To create and maintain an effective organization that will best achieve the objectives of the Cooperative.

2. POLICY CONTENT:

   a. The organization plan shall be based upon functional activities necessary for the accomplishment of the Cooperative's goals.

   b. Position guides shall be written for each position which clearly state the responsibilities and delegation of authorities.

   c. Reporting and working relationships shall be clearly defined. Each person shall report to only one supervisor.

   d. The organization plan shall be flexible and shall be reviewed periodically in line with changing conditions and the development of personnel.

   e. Equal employment opportunity shall be given to all persons without regard to race, creed, color, sex, age, religion, handicap, veteran status, or national origin.

3. RESPONSIBILITY:

   a. The Board of Directors shall be responsible for reviewing and approving a "Statement of Board Objectives and Functions" and the position guide of the Chief Executive Officer (“CEO”).

   b. The CEO will be responsible for the organization plan, which is developed to illustrate and describe the structure and functions of the Cooperative. The plan is to be clearly and concisely described within the contents of an organization manual prepared by the CEO with the advice, counsel, and assistance of their immediate staff.

OMP-03: BOARD-MANAGEMENT-EMPLOYEE RELATIONS

Version: 2024.11.21

1. OBJECTIVE:

   To delegate management authority to the Chief Executive Officer ("CEO") and his or her staff and to set forth management's expectations of its employees.

2. POLICY CONTENT:

   a. The Board of Directors ("Board") hereby delegates the responsibility of management to the CEO and his or her staff. In addition, the Board delegates to the CEO full authority to organize and operate the Cooperative within established policies and procedures as they interpret them. The Board shall not bring pressure to bear, either directly or indirectly, on the CEO in the performance of his or her job duties, and the CEO shall organize and operate the Cooperative in a manner that best serves the needs of the Cooperative.

   b. The Cooperative's general expectations of its employees shall include, but shall not be limited to, those established by this policy.

3. PROVISIONS:

   a. The CEO, supervisory employees, and all other employees shall be guided by the conditions enumerated herein to create a basis for the daily operation of the Cooperative. These provisions and guidelines are not all-inclusive, but rather are illustrative, and all management rights not specifically listed herein are reserved to the Cooperative's Board and/or management personnel.

   b. The Board grants management the right and management reserves the right to:

      i. Control and supervise the operation of the Cooperative.

      ii. Establish, amend, and enforce employee policies and administrative policies and procedures. Management shall report the establishment or amendment of employee policies to the board at least annually. Management shall report the establishment or amendment of employee policies that have a substantial effect on the Cooperative, its operations, or its employees to the board no later than the next regular board meeting following such establishment or amendment.

      iii. Determine job requirements and the personnel needed.

      iv. Determine crew make-up and size.

      v. Direct the work force, including assignments of duties.

vi. Eliminate jobs determined unnecessary.

vii. Employ, discharge, transfer, promote, demote, and discipline employees.

viii. Schedule hours of work, including overtime work.

ix. Change methods of operation.

x. Subcontract work.

xi. Maintain control over standards of performance.

xii. Resolve all problems related to the daily operation of the Cooperative, including the interpretation of Board and Administrative policies.

c. Management expects each Cooperative employee to:

i. Respect the position, dignity, and rights of all other employees.

ii. Perform their work in an efficient manner and in the best interest of the Cooperative.

iii. Protect and preserve the property of the Cooperative to the best of his or her ability.

iv. Hold inviolate confidential information about the Cooperative and its employees.

v. Conduct himself or herself with members and the general public in such a way as to reflect favorably upon the Cooperative.

4. RESPONSIBILITY:

The CEO, supervisory management, and individual employees shall be responsible for the administration of this policy.

OMP-04: USE OF CONSULTANTS

Version: 2015.12.17

1. OBJECTIVE:

   To establish the basis on which consultants will be retained by the Cooperative.

2. POLICY CONTENT:

   a. Auditing Services: The Cooperative shall retain the services of a competent auditing firm which shall be approved by the Rural Utilities Service ("RUS") to audit records of the Cooperative immediately following the close of the fiscal year, which shall include the preparation of an application of funds statement, determination of the amount of general funds invested in plant, and review the audit report at a Board of Directors ("Board") meeting.

   b. Engineering Services: The Cooperative shall retain as needed the services of a competent engineering firm subject to the approval of RUS, to render engineering advice and to contract engineering work for the Cooperative.

   c. Management Consulting Services. The Cooperative shall retain as needed the services of a competent management consultant to assist the Board and the management in evaluating and improving the management functions within the Cooperative.

   d. Legal Counsel: The Cooperative shall retain competent legal counsel subject to the approval of RUS to handle all legal matters for the Cooperative and to advise the Board and the management on all legal questions pertaining to the operations of the Cooperative ("Corporate Counsel"). Special counsel may be retained by the Chief Executive Officer ("CEO"), upon the advice and counsel of the Corporate Counsel, to assist management with specific legal projects where special expertise is required.

   e. Other Services: The Cooperative shall retain such other consultants, engineers, and professional persons to assist the Board and management as shall from time to time be in the best interest of the Cooperative.

3. RESPONSIBILITY:

   The CEO shall include planned and recommended consultant services and expenses in the annual budget for review and approval of the Board. The CEO shall recommend unplanned and recommended consultant services and expense to the Board as soon as practical after the Cooperative's need for the services of such consultants arises. The Board shall take such action as is necessary to retain the services of such consultants.

OMP-05: LONG RANGE PLANNING

Version: 2015.12.17

1. OBJECTIVE:

   To assure that adequate guidelines exist for the operation of the Cooperative to achieve its objectives the following policy is hereby adopted.

2. POLICY CONTENT:

   The Cooperative shall plan for the future in all areas of its operations and from time to time authorize specific studies to be made relative to engineering, finance, power use, member relations, organization, and other phases of operations as the need arises.

3. RESPONSIBILITY:

   a. It shall be the responsibility of the Chief Executive Officer to administer this policy.

   b. It shall be the responsibility of the Board of Directors to review and approve all long range plans put into effect with the Cooperative.

OMP-06: EMERGENCY RESTORATION PLAN

Version: 2015.12.17

1. OBJECTIVE:

   To create and maintain an Emergency Restoration Plan ("ERP") in order to reduce the vulnerability and risks associated with the reliability of the Cooperative's electric system. The plan shall consider both physical assets (poles, wires, transformers, etc.) and cyber assets (telecommunication systems, financial systems, business systems, etc.).

2. POLICY CONTENT:

   a. Requirements: The Cooperative shall develop an ERP which offers the most efficient means in which to restore systems in the event of either a small isolated outage or a system wide outage resulting from a major natural disaster or other cause. The plan is the foundation under which the Cooperative will restore its systems including both the physical and cyber components and efficiently utilize its resources. In order to maintain compliance with Rural Utility Service Bulletin 1730B-2, the Cooperative will maintain a written ERP incorporating the following:

      i. A list of key contact emergency telephone numbers.

      ii. A list of key management and other personnel, which includes chain of command and delegation of authority.

      iii. Procedures for recovery from loss of power to the headquarters or key offices.

      iv. A business continuity section describing a plan to maintain or reestablish business operations following an event, which disrupts business systems.

   b. Exercising the Plan: The ERP shall be exercised at least annually to ensure operability and employee competency. The plan may be exercised in the following ways:

   c. After a natural event that requires the Cooperative to utilize a significant portion of the ERP, review the plan and verify that numbers and points of contacts are correct.

      i. Participate in a joint exercise with other utilities or state or county agencies.

      ii. Perform a tabletop exercise identifying a hypothetical emergency response scenario in which participants join together around a table and identify policy, communications, resources, data, coordination, and organizational elements associated with an emergency response.

   d. ERP Record Keeping: The Cooperative will maintain records that confirm than an ERP has been completed on an annual basis.

3. RESPONSIBILITY:

   a. The Chief Operating Officer ("CEO") is responsible for the administration of this policy.

   b. The CEO is responsible for the review and any subsequent revision to this policy, subject to approval by the Board of Directors.

OMP-07: AREA COVERAGE AND LINE CONSTRUCTION

Version: 2004.05.17

1. OBJECTIVE:

   To set forth the guidelines to be followed in the construction of power facilities to serve the Membership.

2. POLICY CONTENT:

   a. The Cooperative will make diligent effort to extend electric service to all unserved consumers within the Cooperative's service area who desire such service and meet all reasonable requirements established as a condition of such service.

   b. If economically feasible and reasonable considering the cost of providing such service and the effects on consumers' rates, permanent services will be provided, to the maximum extent practicable, at the rates and minimum charges established in the Cooperative's Rate Schedules, without the payment of such persons, other than seasonal or temporary consumers, of a contribution in aid of construction. A seasonal consumer is one that demands electric service only during certain seasons of the year. A temporary consumer is a seasonal or year-round consumer that demands electric service over a period of less than five years.

   c. The Cooperative may assess contributions in aid of construction provided such assessments are consistent with this policy. The Cooperative may also require a service security deposit from any type consumer, no matter where located, if, in accordance with its security deposit policy, such is deemed necessary to assure payment of the power bill.

3. RESPONSIBILITY:

   It shall be the responsibility of the Chief Executive Officer to implement this policy.

OMP-08: INSURANCE REQUIREMENTS

Version: 2015.12.17

1. OBJECTIVE:

   To protect the assets of the Cooperative through providing adequate insurance coverage, the following policy is hereby established.

2. POLICY CONTENT:

   a. Insurance Requirements and Carriers: The Cooperative shall carry insurance to adequately protect the physical assets of the Cooperative and that meets the minimum requirements of the Rural Utilities Service and the National Rural Utilities Cooperative Finance Corporation. This insurance will be with such carriers as the Board of Directors ("Board") may approve.

   b. Review of Coverage: All insurance coverage shall be reviewed annually.

3. RESPONSIBILITY:

   It shall be the responsibility of the Chief Executive Officer to administer this policy and to report annually to the Board in this area.

OMP-09: RETENTION OF CORPORATE RECORDS

Version: 2022.05.19

1. OBJECTIVE:

    a. To comply with various federal and state mandates concerning retention of Cooperative records.

    b. To establish systematic procedures concerning the retention and disposal of Cooperative records.

    c. To allow for the creation and retention of electronic records.

2. POLICY CONTENT:

    a. The Cooperative shall retain and dispose of all Cooperative records according to the schedules established in this policy.

    b. The Cooperative shall create and retain electronic records whenever possible.

    c. This Policy establishes minimum periods for retention of records. It is possible and allowable for the Cooperative to retain records for longer than documented within the policy.

3. PROVISIONS:

    a. Corporate and General Records:

        i. Annual reports and statements to the Members shall be retained for a period of five years.

        ii. All general written communications to the Members shall be retained for a period of three years.

        iii. Records of actions approved by the Members shall be retained for a period of three years.

        iv. Organizational Documents:

            (1) Minute books of Member, Director, and Director Committee meetings shall be retained indefinitely as a permanent record.

            (2) Titles, franchises, licenses, and copies of formal orders of regulatory commissions served upon the Cooperative shall be retained indefinitely as a permanent record.

v. Contracts:

(1) Service contracts for management, accounting, and financial services, and any related memoranda and revisions, shall be retained for a period of four years after expiration of the contract or until the conclusion of any contract disputes pertaining to such contracts, whichever is later.

(2) Contracts with others for the transmission, purchase, sale, or interchange of a product will be retained for a period of four years after expiration of the contract or until the conclusion of any contract disputes or governmental proceedings pertaining to such contracts, whichever is later.

(3) Any memoranda that is essential to clarify or explain provisions of the contracts listed above, including requests for discounts, shall be retained for the same period as the contracts to which they relate.

(4) All card or book records of contracts, leases, and agreements that show the date of expiration and renewal, and all memoranda of receipts and payments under such contracts, will be retained for the same period as the contracts to which they relate.

vi. Accountant and Auditor Reports:

(1) Reports of examinations and audits by accountants and auditors not in the regular employ of the Cooperative shall be retained for seven years from the date of such report.

(2) Internal audit reports and working papers shall be retained for seven years after the date of the report.

b. Information Technology Management:

i. Automatic Data Processing Records:

(1) Original source data used as input for data processing and data processing report printouts shall be retained for the applicable periods prescribed in this policy.

(2) Software documentation shall be retained as long as the software is active and viable or for periods prescribed for related output data, whichever is longer.

c. General Accounting Records:

i. General and Subsidiary Ledgers:

(1) General ledgers and indexes to general ledgers shall be retained for a period of ten years.

(2) Ledgers subsidiary or auxiliary to general ledgers and indexes to subsidiary ledgers shall be retained for a period of ten years.

(3) Trial balance sheets of general and subsidiary ledgers shall be retained for a period of ten years.

ii. Journals:

(1) General and subsidiary journals shall be retained for a period of ten years.

(2) Journal vouchers and journal entries, including supporting detail, shall be retained for a period of ten years.

(3) Analyses, summarization, distributions, and other computations which support journal vouchers and journal entries for charging plant accounts shall be retained for a period of twenty-five years.

(4) Analyses, summarization, distributions, and other computations which support journal vouchers and journal entries for all other accounts shall be retained for a period of six years.

iii. General and subsidiary or auxiliary cash books shall be retained for a period of five years after the close of fiscal year.

iv. Vouchers:

(1) Voucher registers or similar records, when used as a source document, shall be retained for a period of five years.

(2) Paid and canceled vouchers shall be retained for a period of five years.

(3) Original bills and invoices for materials, services, etc., paid by vouchers shall be retained for a period of five years.

(4) Paid checks and receipts for payments of specific vouchers shall be retained for a period of five years.

(5) List of unaudited bills (accounts payable), list of vouchers transmitted, and memoranda regarding changes in audited bills can be destroyed at the Cooperative's option.

(6) Voucher indexes can be destroyed at the Cooperative's option.

d. Insurance: Prior to destruction and disposal, insurance policies and related records shall be carefully reviewed for the possibility that they could provide coverage for a loss that occurs or is otherwise discovered at some point in the future. If such possibility does not

exist, outdated policies (other than general liability policies) shall be destroyed according to the following standards:

i. Records of general liability policies showing coverage, premiums paid, and expiration dates shall be retained in perpetuity.

ii. Records of other insurance policies showing coverage, premiums paid, and expiration dates shall be retained for twelve years.

iii. Records of amounts recovered from insurance companies in connection with losses and claims against insurance companies, including reports of losses and supporting papers, shall be retained for a period of six years.

e. Transmission and Distribution - Public Utilities and Licensees:

i. Substation and transmission line logs shall be retained for a period of three years or until the completion of the next inspection/maintenance cycle, whichever is longer.

ii. System operator's daily logs and reports of operations shall be retained for a period of three years.

iii. Transformer history records shall be retained for a period of thirty-five years.

iv. Records of transformer inspections, oil tests, etc., shall be maintained for a period of thirty-five years.

v. Maintenance Work Orders and Job Orders:

(1) Authorizations for expenditures for maintenance work to be covered by work orders, including memoranda showing the estimates of costs to be incurred, shall be retained for a period of five years, the duration of any warranty period, or until the completion of the next inspection/maintenance cycle, whichever is longer.

(2) Work order sheets to which are posted in detail the entries for labor, material, and other charges in connection with maintenance and other work pertaining to utility operations shall be retained for a period of five years, the duration of any warranty period, or until the completion of the next inspection/maintenance cycle, whichever is longer.

(3) Summaries of expenditures on maintenance and job orders and clearances to operating other accounts (exclusive of plant accounts) shall be retained for a period of five years, the duration of any warranty period, or until the completion of the next inspection/maintenance cycle, whichever is longer.

f. Plant and Depreciation:

i. Plant Ledgers:

(1) Ledgers of utility plant accounts, including land and other detailed ledgers showing the cost of utility plant by classes, shall be retained for a period of twenty-five years.

(2) Continuing plant inventory ledger, book, or card records showing description, location, quantities, cost, etc., of physical units (or items) of utility plant shall be retained for a period of twenty-five years.

ii. Construction Work in Progress Ledgers, Work Orders, and Supplemental Records:

(1) Construction work in progress ledgers shall be retained for a period of five years after clearance to plant account, provided continuing plant inventory records are maintained. Otherwise, five years after plant is retired.

(2) Work order sheets for labor, materials, and other charges for utility plant additions and the entries closing the work orders to utility plant in service at completion shall be retained for a period of five years after clearance to plant account, provided continuing plant inventory records are maintained. Otherwise, five years after plant is retired. Notwithstanding the forgoing, work order sheets shall be maintained indefinitely if they could be used to establish adverse possession.

(3) Authorizations for expenditures for additions to utility plant, including memoranda showing the detailed estimates of cost, and the bases therefore (including original and revised or subsequent authorizations), shall be retained for a period of five years after clearance to plant account, except where there are ongoing RUS proceedings.

(4) Requisitions and registers of authorizations for utility plant expenditures shall be retained for a period of five years after clearance to plant account, except where there are ongoing RUS proceedings.

(5) Completion or performance reports showing comparison between authorized estimates and actual expenditures for utility plant additions shall be retained for a period of five years after clearance to plant account, except where there are ongoing RUS proceedings.

(6) Analysis or cost reports showing quantities of materials used, unit costs, number of man-hours, etc., in connection with completed construction project shall be retained for a period of five years after clearance to plant account, except where there are ongoing RUS proceedings.

(7) Records and reports pertaining to progress of construction work, the order in which jobs are to be completed, and similar records which do not form a basis of entries to the accounts shall be destroyed at the option of the Cooperative.

iii. Retirement Work in Progress Ledgers, Work Orders, and Supplemental Records:

(1) Work order sheets to which are posted the entries for removal costs, materials recovered, and credits to utility plant accounts for cost of plant retirement shall be retained for a period of five years after the plant is retired.

(2) Authorizations for retirement of utility plant, including memoranda showing the basis for determination to be retired and estimates of salvage and removal costs, shall be retained for a period of five years after plant is retired.

(3) Registers of retirement work shall be retained for a period of five years.

iv. Summary sheets, distribution sheets, reports, statements, and papers directly supporting debits and credits to utility plant accounts not covered by construction or retirement work orders (including all supporting records) shall be retained for a period of five years.

v. Appraisals and Valuations:

(1) Appraisals and valuations made by the Cooperative of its properties or investments, or of the properties or investments of any associated companies (including all records essential thereto), shall be retained for a period of three years after such appraisal.

(2) Determinations of amounts by which properties or investments of the Cooperative, or any of its associated companies, will be either written up or down as a result of:

(a) Mergers or acquisitions: Shall be retained for a period of ten years after completion of transaction or as ordered by any Agency.

(b) Asset Impairments: Shall be retained for a period of ten years after recognition of asset impairment.

(c) Other Bases: Shall be retained for a period of ten years after the asset was written up or down.

vi. Original or reproduced engineering records, drawings, and other supporting data for proposed or as-constructed utility facilities, such as maps, diagrams, profiles, photographs, filed survey notes, plot plan, detail drawings, records of engineering

studies, and similar records showing the location of proposed or as-constructed facilities shall be retained until the plant is retired.

vii. Rights of way and easements shall be retained indefinitely.

viii. Contracts Relating to Utility Plant:

(1) Contracts relating to the acquisition or sale of a utility plant shall be retained for six years after such plant is retired or sold.

(2) Contracts and other agreements relating to services performed in connection with construction of a utility plant (including contracts for the construction of the plant by others for the utility and for supervision and engineering relating to construction work) shall be retained for six years after such plant is retired or sold.

ix. Records pertaining to reclassification of utility plant accounts to conform to prescribed systems of accounts, including supporting papers showing the bases for such reclassifications, shall be retained for a period of six years.

x. Records of Accumulated Provisions for Depreciation and Depletion of Utility Plant and Supporting Computation of Expense:

(1) Detailed records or analysis sheets segregating the accumulated depreciation according to functional classification of plant shall be retained for a period of twenty-five years.

(2) Records reflecting the service life of property and the percentage of salvage and cost of removal for property retired from each account for depreciable utility plant shall be retained for a period of twenty-five years.

g. Purchases and Stores:

i. Procurement:

(1) Agreements entered into for the acquisition of goods or the performance of services, including all forms of agreements such as letters of intent, exchange of correspondence, master agreements, term contracts, rental agreements, and the various types of purchase orders, shall be retained for a period of six years.

(2) Supporting documents, including accepted and unaccepted bids or proposals (summaries of unaccepted bids or proposals may be kept in lieu of originals), evidencing all relevant elements of the procurement shall be retained for a period of six years.

ii. Ledger sheets of materials and supplies received, issued, and on hand shall be retained for a period of six years after the date the records/ledgers were created.

iii. Records showing the detailed distribution of materials and supplies issued during accounting periods shall be retained for a period of six years.

iv. Records of authorization and contracts for sale of scrap materials and supplies shall be retained for a period of three years.

h. Revenue Accounting and Collecting:

i. The Cooperative shall maintain consumer account records sufficient to calculate and allocate patronage capital, including any reductions in such capital as a result of debts owed to the Cooperative.

ii. Member service applications and contracts, including amendments for extensions of service, shall be retained for a period of four years.

iii. General files of published rate sheets and schedules of utility service, including schedules suspended or superseded, shall be retained for six years after published rate sheets are superseded or no longer used to charge for utility service.

iv. Maximum demand and demand meter record cards shall be retained for a period of one year, except where the basic chart information is transferred to another record, in which case the charts need only be retained for six months, provided the basic data is retained one year.

v. Billing department copies of contracts with Members (other than contracts in general files) may be destroyed at the Cooperative's option.

vi. Summaries of monthly operating revenue according to classes of service, including summaries of forfeited discounts and penalties, shall be retained for a period of five years.

i. Tax Records:

i. Copies of tax returns and supporting schedules filed with taxing authorities, supporting working papers, records of appeals of tax bills, and receipts for payments shall be retained, according to the following:

(1) For income tax returns, a period of seven years after final tax liability is determined.

(2) For property tax returns, a period of seven years after final tax liability is determined.

(3) For sales and other use taxes, a period of seven years.

(4) For agreements between associate companies as to allocation of consolidated income taxes, a period of seven years after final tax liability is determined.

(5) For a schedule of allocation of consolidated Federal income taxes among associate companies, a period of seven years after final tax liability is determined.

(6) For filings with tax authorities to qualify employee benefit plans, a period of five years after discontinuance of plan.

(7) For information returns and reports to taxing authorities, a period of three years after final tax liability is determined.

j. Treasury Records:

i. Statements of Funds and Deposits:

(1) For statements of periodic deposits with fund administrators or trustees, records shall be retained from the most recent three years.

(2) For statements of periodic withdrawals from funds, records shall be retained from the most recent three years.

(3) Statements prepared by the fund administrator or trustees of fund activity, including beginning of year fund balance, deposits with the fund, acquisition of investments held by the fund, disposition of investments held by the fund, disbursements from the fund, including the party to whom disbursement was made, and end of year fund balance shall be retained until the fund is dissolved or terminated.

ii. Records of Deposits:

(1) Statements from depositories showing the details of funds received, disbursed, transferred, and balances on deposit may be destroyed at the Cooperative's option after completion of an audit by independent accountants.

(2) Check stubs, registers, or other records of checks issued shall be retained for a period of three years.

k. Department of Transportation Inspection Forms and Vehicle Repair Reports:

i. Annual vehicle inspection, repair, and maintenance records indicating their date and nature shall be retained for a period of fourteen months.

ii. Daily post-trip inspection reports and the certification of repairs shall be retained for a period of three months from the date of preparation.

iii. Vehicle inspection, repair, and maintenance records indicating their date and nature shall be retained for a period of six months after the motor vehicle leaves the Cooperative's control.

iv. Accident records shall be maintained for a period of three years after an accident occurs.

l. Miscellaneous Records:

i. Financial, operating, and statistical reports used for internal administrative or operating purposes shall be retained for a period of five years.

ii. Budgets and other forecasts of estimated future income prepared for internal administrative or operating purposes shall be retained for a period of three years.

iii. Receipts and expenditures in connection with financing, construction, and operations, including acquisitions and disposals of properties or investments, shall be retained for a period of three years.

iv. Records of predecessor companies shall be retained consistent with the requirements for the same types of records of the Cooperative.

v. Reports to Federal and State regulatory commissions, including annual financial, operating, and statistical reports will be retained for a period of five years.

m. Electronic Records:

i. Electronic records may be retained in place of the original record whenever possible.

ii. An electronic record shall have the same force and effect as the original record if:

(1) The information in the electronic record accurately reflects the information set forth in the original record's final form; and

(2) The record remains accessible for later reference.

iii. Once an electronic version of the original record has been created, the original record may, but shall not be required to, be destroyed.

n. Personnel records shall be maintained according to a separate Board policy on maintenance periods for personnel records, as administered by the Vice President of Human Resources.

4. RESPONSIBILITY:

The Chief Executive Officer shall be responsible for the administration of this policy.

OMP-10: DOCUMENT HOLD NOTICES AND ELECTRONIC DISCOVERY

Version: 2015.12.17

1. OBJECTIVE:

   a. To promote record preservation in the event of legal challenges.

   b. To comply with e-discovery obligations in the event of anticipated or actual litigation.

   c. To facilitate identification of all records and data potentially relevant to an actual or anticipated lawsuit, the types of computer hardware used to store electronic data, the types of software needed to review data, portions of data that are privileged or confidential, and types of records that may be inaccessible due to prior destruction or technical hurdles.

2. POLICY CONTENT:

   The Cooperative will comply with record preservation and electronic discovery obligations arising from litigation and other legal disputes according to the standards set forth below.

3. PROVISIONS:

   a. Preliminary Compliance:

      i. If the Cooperative should reasonably anticipate litigation, the Cooperative shall suspend all document destruction procedures. Obligations under this policy would arise, for instance, whenever the Cooperative receives an EEOC Charge, an investigatory request from an administrative agency, or notice of threatened litigation. Unsubstantiated rumors concerning a possible claim will not trigger obligations under this policy.

      ii. The Chief Executive Officer ("CEO") shall notify corporate or labor attorney concerning the circumstances giving rise to anticipated litigation. Counsel and management shall conduct a privileged conference concerning implementation of record preservation strategies.

      iii. The CEO or his or her designee shall issue and distribute a written Document Hold Notice ("DHN") to all personnel with knowledge relating to the anticipated litigation or claim, as well as all persons with the reasonable potential to have relevant records in their possession, custody, or control.

      iv. The Chief Information Officer ("CIO") shall be consulted immediately to determine whether there are any potentially relevant electronic records, including but not limited to e mails, spreadsheets, presentations, phone records, electronic payment

records, word processing records, draft documents, or other electronic files and documents.

v. The DHN shall include a simple and plain statement concerning each of the following:

(1) The nature of the actual or potential litigation.

(2) The subjects and timeframes of potentially relevant evidence.

(3) An explanation that the recipient has been recognized as someone with potential responsibilities under the policy.

(4) Instructions that the recipient is prohibited from deleting or destroying potentially relevant records, until the recipient receives written notice that the "hold" has been lifted.

(5) A statement of any specific instructions or special steps that the recipient should take upon receipt of the notice.

vi. The Cooperative shall provide timely updates regarding the status of any litigation holds, including information regarding any anticipated termination of the hold.

b. Investigations Following Hold Notice:

i. The Cooperative shall take prompt action to monitor compliance with the litigation hold process. This process shall include personal interviews with relevant staff to identify sources of potentially discoverable information and protect such information from inadvertent destruction.

ii. Personal interviews shall address the individual's experience and exposure to document retention practices, including an analysis of software programs, locations for saving documents, preservation of e-mails, the potential existence of recently deleted files on backup media, preservation of backup media, and access to servers and shared directories.

iii. IT personnel shall participate in all personal interviews to facilitate review and analysis of issues concerning:

(1) The nature of hardware and software used by the employees.

(2) Processes for identifying and preserving electronic data.

(3) The nature of the Cooperative's e-mail system.

(4) The existence and nature of any electronic backup protocols.

(5) Whether the Cooperative has any archival or legacy information.

(6) An evaluation of whether it would be prudent to mirror computer hard drives, taking into account the issues involved in the case, the identity and location of potential witnesses and other potential sources for the records.

(7) The existence of potentially relevant metadata.

c. Preservation of Records:

i. The Cooperative shall preserve all electronic and paper records potentially relevant to any actual or anticipated litigation until such time as they are advised by counsel that the hold can be rescinded.

ii. Upon termination of the litigation hold, the Cooperative shall revert to its normal document destruction policy and promptly destroy documents that were otherwise scheduled for destruction during the period of the hold.

4. RESPONSIBILITY:

a. The CEO shall be responsible for assuring compliance with these procedures.

b. The CIO Officer shall be responsible for supervising technological compliance.

c. Department heads shall be responsible for assisting in the identification of pertinent documents and records.

OMP-11: MAINTAINING A SECURE PHYSICAL AND CYBER ENVIRONMENT

Version: 2017.02.16

1. OBJECTIVE:

   a. To protect and maintain the security of people, physical, and cyber assets.

   b. To comply with regulatory and/or legal obligations relating to maintaining a secure cyber environment.

2. POLICY CONTENT:

   Proper security is important to preserve the well-being of the Cooperative's employees, members, board of directors, contractors, and visitors. It also protects EnergyUnited's physical and cyber assets to assure continuity of the enterprise for the benefit of members. Proper security is also necessary to comply with applicable regulatory and legal requirements.

3. PROVISIONS:

   a. The Cooperative shall:

      i. Maintain a workplace that provides employees, members, board members, contractors, and visitors with security that contributes to a productive environment.

      ii. Maintain administrative policies and procedures with defined objectives designed to apply appropriate controls and continuity plans assuring reasonable protection from loss of physical and cyber assets. On a periodic basis, perform an audit to ensure compliance.

      iii. Take steps to prevent the unauthorized access to the Cooperative's property and unauthorized use of physical and cyber assets.

      iv. Seek continuous improvement in practices and measures that maintain the security of people, physical, and cyber assets.

      v. Annually, perform an independent, third-party technical vulnerability and penetration assessment on both the internal and external networks. Employees are expected to assess and initiate appropriate remediation in accordance with the findings.

      vi. Comply with all applicable laws and regulations regarding security.

      vii. Cooperate with local, state, and federal authorities and other entities on matters relating to security.

viii. Provide on a regular basis appropriate information security and awareness training for employees, contractors, and others.

ix. Maintain and test business continuity, disaster recovery, and incident response plans on an annual basis. Any actual or suspected information security breaches will be reported in accordance with the incident response plan. All breaches will be investigated thoroughly and logged.

x. Communicate this policy to all employees.

4. RESPONSIBILITY:

a. The Chief Information Officer is responsible for the administration of this policy.

b. The Chief Executive Officer is responsible for the review and any subsequent revision to this policy, subject to board approval.

OMP-12: SECURING CONFIDENTIAL MEMBER AND EMPLOYEE DATA WHILE RETAINING AND DESTROYING RECORDS

Version: 2008.07.17

1. OBJECTIVE:

   a. To protect and secure the confidentiality of identifying information and other sensitive records concerning Members and employees.

   b. To comply with legal obligations relating to the use and destruction of confidential identifying information.

2. POLICY CONTENT:

   The Cooperative will secure confidential Member and employee data as required by law and principles of sound business judgment.

3. PROVISIONS:

   a. The term "Confidential Identifying Information" as used in this policy includes documents containing any of the following information:

      i. Social Security numbers or Taxpayer Identification numbers.

      ii. Driver's license numbers, State identification numbers, or passport numbers.

      iii. Checking, savings, or other bank account numbers.

      iv. Credit card or Debit Card numbers.

      v. Personal Identification Number (PIN) codes relating to any financial accounts.

      vi. Electronic identification numbers, e-mail names or addresses, internet account numbers, or internet identification numbers.

      vii. Digital signatures.

      viii. Any other numbers or information that can be used to access a person's financial resources.

      ix. Biometric data.

      x. Fingerprints.

      xi. Passwords.

xii. Member's surname prior to marriage.

b. kWh usage information regarding a vacant premises shall not be regarded as confidential information.

c. The term "Confidential Personnel Records" as used in this policy shall include:

i. Applications.

ii. Personnel files.

iii. Credit and background reports.

iv. Employment Eligibility Verification Forms (I-9).

v. Performance reviews.

vi. Disciplinary records.

vii. Payroll records.

viii. Separation records.

ix. Employee benefit records.

x. Medical records.

xi. Worker injury records.

xii. Any other record relating to any current or former employee that contains identifying information.

d. Confidential Identifying Information and Confidential Personnel Records shall be stored in secured cabinets and/or locked rooms. Access to such information shall be restricted to Cooperative personnel who require access for the purpose of serving the Cooperative's business requirements.

e. The Cooperative shall insure that confidential Member information and Confidential Personnel Records are destroyed in a manner that will protect against unauthorized access to or use of the information in connection with or after its disposal. Approved methods for destroying paper records under this policy shall be limited to burning, pulverizing, or shredding.

f. The Cooperative shall not sell, donate, transfer or otherwise dispose of any electronic medium, including but not limited to computer equipment, disks, tapes, electronic files, and other non-paper media, until after the Cooperative's Chief Information Officer has

verified that all confidential information on said media has been erased or destroyed in a manner that would prevent reading or reconstructing of any Confidential Identifying Information contained therein.

g. The Cooperative shall maintain technologically appropriate methods and procedures of protecting against unauthorized access to its computer networks.

h. The Cooperative may, after due diligence, enter into a written contract with another entity engaged in the business of record destruction to destroy personal information in a manner consistent with all confidentiality obligations. The Cooperative shall conduct ongoing monitoring of the security practices of any firm selected under this subsection. Initial due diligence under this subsection shall include one of the following:

   i. Reviewing an independent audit of the disposal business's operations or its compliance with the North Carolina Identity Theft Protection Act.

   ii. Obtaining information about the disposal business from at least three references or other reliable sources and requiring that the disposal business be certified by a recognized trade association or similar third party with a reputation for high standards of quality review.

   iii. Reviewing and evaluating the disposal business's information security policies and procedures or taking other appropriate measures to determine the competency and integrity of the disposal business.

i. The Cooperative shall protect the confidentiality of Social Security numbers in accordance with the requirements of N.C. Gen. Stat. § 75-62. Such numbers shall not be communicated to the general public, printed on mailings to the individual, or disclosed to third parties that lack a legitimate purpose for obtaining access to the affected Social Security number. The Cooperative shall obtain a legal audit of all existing uses of Social Security numbers and shall not thereafter change its practices involving Social Security numbers without obtaining privileged legal guidance concerning the permissibility of the changed practice.

j. <u>Notification of Security Breaches</u>:

   i. In the event of a security breach involving misappropriation of Confidential Identifying Information where harmful or illegal use of the information has occurred or is likely to occur, the Cooperative shall provide prompt notice of said breach to the affected person. However, notification may be delayed if a specific law enforcement officer provides a written statement that timely notification may impede a criminal investigation or jeopardize national or homeland security.

   ii. The notification obligation is intended to alert persons to breaches involving sensitive data giving rise to an appreciably increased risk of illegal or harmful conduct.

Accordingly, the notice obligation shall not apply to inadvertent security breaches involving electronic identification numbers, e-mail names and addresses, internet account numbers, internet identification names, Member's legal surnames prior to marriage, or passwords unless this information would permit access to a person's financial account or resources. Similarly, the notification obligation shall not apply to security breaches involving personnel records that do not otherwise meet the definition of Confidential Identifying Information subject to the notification provision of this policy.

iii. Notice under this policy shall be in the form of a written letter delivered via U.S. Mail, shall be clear and conspicuous, and shall include a description of the following:

(1) The incident in general terms.

(2) The type of Confidential Identifying Information that was subject to the unauthorized access and acquisition.

(3) The Cooperative's general efforts to protect the Confidential Identifying Information from further unauthorized access.

(4) A telephone number that the person may call for further information and assistance, if one exists.

(5) Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.

iv. In the event that notice is due to more than one thousand persons at one time, the Cooperative shall promptly notify the Consumer Protection Division of the Attorney General's Office and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. § 1681a(p), of the timing, distribution and content of the notice.

4. RESPONSIBILITY:

The Chief Executive Officer shall be responsible for the administration and enforcement of this policy.

OMP-13: PRIVACY OF MEMBER NON-PUBLIC INFORMATION

Version: 2015.12.17

1. OBJECTIVE:

   To provide for the sharing of Member non-public information with Cooperative affiliates.

2. POLICY CONTENT:

   The Cooperative's privacy policy shall be governed by the following rules and procedures:

   a. "Affiliate" means one or more members of the EnergyUnited family of companies, including, but not limited to, EnergyUnited Services Corporation and EnergyUnited Propane, LLC. "Non-affiliate" means companies that are not part of the EnergyUnited family of companies.

   b. The Cooperative collects Member non-public information from the following sources:

      i. Information received on applications or other forms, such as name, address, and Social Security number.

      ii. Information about member transactions, such as account balance and payment history.

      iii. Information received from consumer reporting agencies, such as credit history.

   c. The Cooperative does not disclose Member non-public information to anyone, except as required by law or as hereafter stated.

   d. The Cooperative may disclose a Member's non-public information, such as name and mailing address, to its Affiliates if, in the Cooperative's discretion, such disclosure would be in the Member's best interests. The Cooperative may disclose Member non-public information to Non-affiliates as reasonably necessary to perform services for or on behalf of the Cooperative or its Affiliates, or in connection with products, programs, or services made available to Members through the Cooperative, provided that such Non-affiliates are contractually required to maintain the confidentiality and security of the information and to use the information only for the purposes for which it was disclosed.

   e. The Cooperative restricts access to Member non-public information to those employees who need to know that information to provide products or services to Members. The Cooperative maintains physical, electronic, and procedural safeguards to protect Member nonpublic information.

   f. The Members shall be provided written notice of this policy.

g. Each Member shall have the right to prohibit the disclosure of the Member's non-public information.

3. RESPONSIBILITY:

It will be the responsibility of the Chief Executive Officer and their staff to implement this policy.

OMP-14: RED FLAG PROGRAM FOR IDENTITY THEFT AND CREDIT REPORTING ACCURACY

Version: 2008.10.16

1. OBJECTIVE:

   To implement a red flag program to prevent identify theft and ensure credit report accuracy.

2. POLICY CONTENT:

   a. To comply with regulations concerning "red flags" for identity theft of Member and applicant information, including obligations to identify red flags, detect the occurrence of red flag events, respond appropriately to red flags, and ensure periodic assessments and updates to the program.

   b. To implement reasonable procedures regarding the detection, prevention, and mitigation of identity theft.

   c. To implement reasonable procedures in the event of address discrepancies on consumer credit reports.

3. PROVISIONS:

   a. Identity theft under this policy is defined as an actual or attempted fraud using the identifying information (name, address, Social Security number, account number, etc.) of a Member or applicant.

   b. A "red flag" under this policy is defined as a pattern, practice, or specific activity indicating a risk of identity theft. Such red flags may include:

      i. Incidents of identity theft experienced or detected in the past.

      ii. Alerts from consumer reporting agencies.

      iii. The presence of suspicious documents or inconsistent data.

      iv. Suspicious name or address changes, or other personal identifying information.

      v. Suspicious account activity.

      vi. Notices from Members, other electric utility systems, victims of identity theft, and law enforcement personnel concerning the possibility or reasonable suspicion of fraudulent activity involving a Member account.

vii. Material changes in the rates of usage of cooperative services.

viii. Returned and undeliverable mail, despite continued usage of Cooperative services.

ix. Data breaches in violation of Board Policy 3-38B.

c. The relevance of red flags shall be evaluated based on principles of common sense and sound business judgment, taking into account all relevant factors relating the Member or applicant, the account, and other circumstances.

d. The Cooperative shall implement reasonable procedures to prevent and detect identity theft in the application for service, which will include the use of a data verification service, and in the event of discrepancies or concerns, may include a requirement that applicants apply for membership in person and present photo identification and reasonable proof of eligibility to establish service at the location. In the event of any instance of identity theft, the Cooperative shall review then-existing verification procedures and determine whether they remain adequate under the circumstances.

e. The Cooperative shall implement reasonable procedures to verify the identity of persons for whom it obtains consumer reports, and reasonable procedures for reconciling the address of the consumer with the consumer reporting agency, and shall refrain from using a report where the consumer's identity cannot be so verified.

f. In the event of genuine address discrepancies, the Cooperative shall use reasonable means to verify the consumer's correct address and then provide such confirmed addresses to the consumer reporting agency, within the reporting period. Verification steps may include verification with the applicant, reviewing the accuracy of the Cooperative's records, verifying the address through third-party sources, or using other reasonable means.

g. Management shall establish and implement reasonable training programs to ensure day-to-day application of this policy.

h. Management shall continue to monitor the adequacy of this policy, and other policies and procedures that may already be in place, relating to the detection of red flags and other risks to the security of Member and applicant data. The Cooperative shall update its program from time to time based on experiences with identity theft, changes in methods of identity theft, changes in methods to detect, prevent, and mitigate identity theft, changes in the types of accounts offered to Members, and other changes in business arrangements and practices.

4. RESPONSIBILITY:

a. The Board of Directors shall be responsible for approving the initial written policy.

b. The Chief Executive Officer and his designees among senior management shall be responsible for ensuring oversight of the development, implementation and administration of the Program, training relevant staff, periodically updating the program and overseeing service provider arrangements. The CEO shall tailor the program to the size, complexity, and nature of the Cooperative's operations.

OMP-15: USE OF COOPERATIVE COMMUNICATIONS AND COMPUTER SYSTEMS

Version: 2022.06.16

1. OBJECTIVE:

   To establish standards for the proper use of communications and computer equipment, systems, and networks owned, operated, or furnished by the Cooperative ("Cooperative Communications and Computer Systems").

2. POLICY CONTENT:

   Standards for the proper use of Cooperative Communications and Computer Systems.

3. PROVISIONS:

   a. Cooperative Communications and Computer Systems are Cooperative property and shall be used for conducting Cooperative business and other authorized uses.

   b. Use of Cooperative Communications and Computer Systems that violates the Cooperative's Governing Documents, is inconstant with Cooperative Values, or otherwise adversely impacts or adversely reflects upon the Cooperative is prohibited.

   c. Limited personal use of Cooperative Communications and Computer Systems is authorized provided that it is limited to the following considerations:

      i. It does not introduce cybersecurity risk to EnergyUnited.

      ii. It does not have a negative impact on overall employee productivity.

      iii. It does not cause additional expense to the company.

      iv. It does not compromise the company in any way.

      v. It does not disrupt the network performance in any way.

      vi. It does not contradict any other EnergyUnited policies in any way.

   d. Private, commercial, competitive, or political use of the Cooperative's Communications and Computer Systems are not authorized.

   e. Passwords associated with Cooperative Communications and Computer Systems are the property of the Cooperative.

f. Data stored in Cooperative Communications and Computer Systems are the property of the Cooperative, and shall be accessed only on a "need to know" basis and only for authorized purposes.

g. Cooperative software license agreements shall be honored. Duplication of software is prohibited, unless expressly authorized by the terms of the software license. Only software approved by the Department Head and the Network Administrator, or the IT representative shall be installed or operated on Cooperative Communications and Computer systems.

h. Examples of Cooperative Communications and Computer Equipment, Systems, and Networks include, but are not limited to but are not limited to:

   i. Computers, tablets, telephones, mobile devices, and other hardware.

   ii. Operating systems, office suites, and other software.

   iii. Printers, copiers, cameras, scanners, and other peripherals.

   iv. Intranets, internet access points, mobile networks, and other data networks and associated bandwidth.

   v. Transmitted, received, and stored data and the media upon which such data is stored.

4. Separation from the Cooperative:

   a. Upon separation, all physical equipment assigned is to be returned to the Cooperative inventory.

   b. Upon separation, previously granted access to business equipment, software, electronic devices, and telephone communication systems shall be revoked or reassigned as applicable.

   c. Standard operating procedures and separation checklists will be used to insure that Section (4)(a) and Section (4)(b) have been followed to protect the interests of the Cooperation.

5. RESPONSIBILITY:

   The Chief Executive Officer is responsible for the administration of this policy and any subsequent revision, subject the approval of the Board of Directors.

OMP-16: CYBERSECURITY INCIDENT MANAGEMENT

Version: 2022.06.16

1. OBJECTIVE:

   a. The purpose of this policy is to ensure proper recognition, management, and communication of cybersecurity events and weaknesses through a formal process.

   b. The quality and integrity of EnergyUnited incident response capabilities are used to monitor cybersecurity incidents, determine the magnitude of the threat presented by these incidents, and respond to these incidents. Without an incident response capability, the potential exists that in the event that a cybersecurity incident occurs, it will go unnoticed, and the magnitude of harm associated with the incident will be significantly greater than if the incident were noted and corrected sooner.

   c. This policy applies to all business processes and data, information systems and components, personnel, and physical areas of EnergyUnited's Information and Operational Technologies.

2. GOVERNING LAWS, REGULATIONS, AND STANDARDS:

Guidance	Section
PCI-DSS 3.2.1	11.1.2; 12.4; 12.5.3; 12.8.3; 12.10
CFR Title VII Volume 3	§ 1730.21 Inspections and tests
COBIT-19	APO12.06; CSC 19; DSS04.02; DSS04.03; DSS02.05; DSS04.06

3. POLICY CONTENT:

   a. Management of Cybersecurity Incidents and Improvements:

      i. Incident management responsibilities and procedures are established to ensure timely response to incidents and timely activation of business continuity procedures. Members of the ELT and MLT are responsible for maintaining business continuity procedures for mission-critical services in their respective areas.

      ii. IT serves as the incident response team, referred to as "incident responders," and will have primary responsibility in handling the intake, communication, and remediation of cybersecurity incidents, engaging business stakeholders as needed.

(1) Incident responders must provide primary and secondary contact information to be reached in the event of a relevant cybersecurity incident.

(2) Incident responders will establish a method of communication alternative to the primary method to be used if the primary communication method is affected by or is otherwise unavailable during the cybersecurity incident.

(3) Communication with affected parties will be provided on an as-needed basis, but not less than once every 4 hours until the incident is contained. It is up to the discretion of the incident responders to withhold information if the disclosure of said information deems a reasonable risk to EnergyUnited's security while the response is ongoing.

iii. The incident response capability includes a defined plan and addresses the seven stages of incident response:

(1) Preparation.

(2) Detection.

(3) Analysis.

(4) Containment.

(5) Eradication.

(6) Recovery.

(7) Post-Incident Activity.

iv. Cybersecurity events must be reported through proper channels. Incidents will be tracked as they occur in EnergyUnited's ticketing system.

v. Any weaknesses, suspected or verified, in systems and services must be reported by users (employees or third-party contractors) using those systems and services. End users should contact the Service Desk by dialing 704-924-5340 or emailing help@energyunited.com to submit a ticket.

vi. As cybersecurity events are assessed, determinations are made about whether they can be identified as cybersecurity incidents. Once an event is deemed an actual cybersecurity incident, the incident will be classified as such, and relevant incident responders will be notified.

vii. Cybersecurity incidents will be identified and classified into different severity levels to make the incident response process more effective.

viii. Incidents will be responded to with the appropriate procedures based on documented organizational processes.

ix. Incident response procedures will be reviewed annually, and any required updates will be communicated to the appropriate parties.

x. Definitions and procedures around identifying, collecting, acquiring, and preserving evidence will be established.

(1) This data will be recorded and stored on SharePoint and the ticketing system for three years.

(2) The records of this data will be reviewed annually and timestamped.

xi. In a major incident, only a designated spokesperson will address the media as outlined in EnergyUnited's Crisis Communication Manual.

xii. After all relevant cybersecurity incidents, a post-incident review will be conducted by incident responders to determine the root cause of the incident, the consequences, and the lessons learned. The information gained from responding to and resolving incidents will be used to reduce potential future incidents. Any affected parties, including end-users, may be contacted for additional insight.

4. RESPONSIBILITY:

The Vice President of Information Technology is responsible for the implementation of this policy.

OMP-17: ACCEPTABLE USE POLICY

Version: 2022.06.16

1. OBJECTIVE:

    a. EnergyUnited provides various technology resources to its employees and contractors to enhance their productivity and to enable them to fulfill their roles and responsibilities.

    b. EnergyUnited requires that these resources be used in a responsible way, ethically, and in compliance with all legislation and other EnergyUnited policies, guidelines, and contracts.

    c. Noncompliance could have a severe, negative impact on the cooperative, its employees, and its members. This policy does not attempt to anticipate every situation that may arise and does not relieve anyone accessing these resources of their obligation to use common sense and good judgment.

2. POLICY CONTENT:

    a. This policy is applicable to all employees of EnergyUnited, including full-time, part-time, and temporary employees; contractors; students; and interns. The requirements defined in this policy are applicable to all technology resources owned and/or managed by EnergyUnited. EnergyUnited Resources include, but are not limited to, physical equipment, such as desktop computers, servers, printers, laptops, telephones, mobile devices, and removable media (such as USB flash drives), as well as data, systems, and services, such as the network, internet, wireless, voicemail, and more.

    b. EnergyUnited allows limited use of technology resources for personal reasons (personal correspondences, online banking, etc.), but personal use must not be abused. Personal use is acceptable when limited to the following considerations:

        i. It does not introduce cybersecurity risk to EnergyUnited.

        ii. It does not have a negative impact on overall employee productivity.

        iii. It does not cause additional expense to the company.

        iv. It does not compromise the company in any way.

        v. It does not disrupt the network performance in any way.

        vi. It does not contradict any other EnergyUnited policies in any way.

c. EnergyUnited resources may not be used for illegal or unlawful purposes, including copyright infringement, obscenity, personal gain, libel, slander, fraud, defamation, plagiarism, intimidation, forgery, impersonation, illegal gambling, soliciting for pyramid schemes, and computer tampering (e.g., spreading computer viruses). Additionally, users are not to engage in any inappropriate use of EnergyUnited resources. Inappropriate use includes, but is not limited to:

i. Transmitting any information or data, in any form, that violates any local, state, federal, or applicable international law or regulation, or that is harmful, threatening, abusive, harassing, tortious, defamatory, vulgar, obscene, libelous, and invasive of another's privacy, hateful, or otherwise objectionable.

ii. Engaging in any activity or device to disguise the origin of any transmission (e.g., Anonymizers).

iii. Transmitting any information or data that contains any computer virus, or any material designed to interrupt, destroy, or limit the functionality of any computer hardware or software.

iv. Users must not introduce or contribute to security breaches or disruptions of network communication. For the purposes of this section, "disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

v. Port scanning or security scanning is expressly prohibited unless prior authorization is granted in writing by the VP of Information Technology or performed by IT in the normal course of assessing EnergyUnited's security posture.

vi. Users must not execute any form of network monitoring that will intercept data not intended for the employee's device unless this activity is a part of the employee's normal job/duty.

vii. No servers or devices that actively listen for network traffic are allowed to be put on the corporate network without prior written authorization by the VP of Information Technology.

viii. Collecting personal data or attempt to collect personal information about third parties without their knowledge or consent.

ix. Reselling access to EnergyUnited communications and computer systems without EnergyUnited's express written authorization.

x. Accessing and/or purchasing technology, devices, applications, or services that are not formally authorized and approved by IT.

xi. Connecting technology, devices, applications, or services to the EnergyUnited network that are not formally authorized and approved by IT.

xii. Viewing, copying, altering, or destroying data, software, documentation, or data communications belonging to EnergyUnited or another individual without prior clearance from an authorized EnergyUnited representative.

xiii. Engaging in any activity that adversely affects the ability of other people or systems to use EnergyUnited communications and computer systems.

xiv. Circumventing user authentication or security controls.

xv. Installing or using encryption software on any of EnergyUnited's communications or computer systems that hasn't been provided by IT.

xvi. Allowing non-authorized users to use EnergyUnited resources (e.g., family member).

xvii. Engaging in any other activity deemed by EnergyUnited to conflict with the spirit or the intent of this policy.

d. Removable media, such as USB flash drives, CDs, etc., may be used with the following requirements:

i. Information should only be stored on removable media when required in the performance of the user's role (e.g., USB shared between two employees during a conference).

ii. Mobile devices that are not owned by EnergyUnited (e.g., smartphones, tablets) are not permitted to be used as removable media to transfer or store any business or customer data.

iii. Any unknown removable media that is found unattended must be reported to the IT Department and NOT inserted into any EnergyUnited issued device.

iv. Users must take reasonable measures to secure removable media (e.g., storing it in a secure/locked location when not in use; not sharing with unauthorized users).

v. Use of removable media that contains EnergyUnited data is not allowed on external or non-company-issued systems.

vi. Upon completion of the assigned duties, all data shall be deleted from the removable media.

vii. All removable media must be turned in to the Service Desk for proper disposal when no longer required for business use.

e. The use of EnergyUnited communication and internet systems and services (including email, instant messaging, voicemail, forums, social media, and more) is provided to support the performance of regular job duties. The use is a privilege, not a right, and therefore must be used securely, with respect and common sense, and in accordance with the following requirements:

i. The email systems and other messaging services used at EnergyUnited are owned by the company and are therefore its property. This gives EnergyUnited the right to monitor all email traffic passing through its email system. This monitoring may include, but is not limited to, inadvertent reading by IT staff during the normal course of managing the email system, review by the HR and legal team during the email discovery phase of litigation, and observation by management in cases of suspected abuse or employee inefficiency.

ii. EnergyUnited often delivers official communications via email. As a result, employees of EnergyUnited with email accounts are expected to check their email in a consistent and timely manner so that they are aware of important company announcements and updates, as well as for fulfilling business and role-oriented tasks.

iii. EnergyUnited communication platforms and internet are not to be used for purposes that could be reasonably expected to strain storage or bandwidth (e.g., emailing large attachments instead of pointing to a location on a shared drive).

iv. Users are prohibited from using accounts that do not belong to them and are prohibited from using platforms to impersonate others.

v. Users are not to give the impression that they are representing or providing opinions on behalf of EnergyUnited unless otherwise authorized.

vi. Users shall not open message attachments or click on hyperlinks sent from unknown or unsigned sources through any platform (email, instant message, social media, etc.). Attachments/links are the primary source of malware and social engineering and should be treated with utmost caution.

vii. EnergyUnited prohibits use of email or other messaging platforms for mass unsolicited mailings, chain letters, and competitive commercial activity unless preapproved by EnergyUnited.

viii. If you receive a suspicious email, do not forward, delete, or reply to the message. Instead, report it using the Phish Alert option.

ix. Email users are responsible for mailbox management, including organization and cleaning.

x. Archival and backup copies of email messages may exist, despite end-user deletion, in compliance with EnergyUnited's record retention guidelines.

xi. Email access will be terminated when the employee or third party terminates their association with EnergyUnited, unless other arrangements are made. EnergyUnited is under no obligation to store or forward the contents of an individual's email inbox/outbox after the term of their employment has ceased, even if those contents are deemed personal.

xii. Users shall not send sensitive information that is not appropriately protected (encrypted). Appropriate means of protection include but are not limited to OneDrive or email encryption.

xiii. Users shall take extra precautions when transmitting company, member, and/or other regulated information via electronic communications. Sensitive material should be marked and encrypted appropriately.

xiv. Users are not permitted to automatically forward emails received by their EnergyUnited account to an external email address or other messaging system.

xv. EnergyUnited assumes no liability for direct and/or indirect damages arising from the user's use of EnergyUnited's email system and services. Users are solely responsible for the content they disseminate. EnergyUnited is not responsible for any third-party claim, demand, or damage arising out of use EnergyUnited email systems or services.

xvi. However, email users are expected to remember that email sent from EnergyUnited email accounts reflects on the company. Users are expected to comply with normal standards of professional and personal courtesy and conduct.

xvii. EnergyUnited may monitor any/all internet activity originating from company-owned equipment or accounts or taking place over company networks. If EnergyUnited discovers activities that do not comply with applicable law or corporate/departmental policy, records retrieved may be used to document the wrongful content in accordance with due process.

xviii. Users are permitted to remotely access the corporate network while off-site. When using a public network, (e.g., a wireless network at a hotel) users must use the approved VPN service(s).

xix. EnergyUnited social media accounts are permitted to be used for business purposes only. These purposes include building positive brand image, providing customer support, monitoring public opinion, professional networking, and more. The following requirements are imposed for appropriate use of social media:

(1) Access to social media will be open to staff who have received approval from their manager. Approval will be provided given a legitimate business purpose.

(2) All actions and communications through social media must adhere to all previously defined acceptable use of electronic communications.

(3) The use of personal social media accounts and user IDs for company use is prohibited.

(4) The use of EnergyUnited social media user IDs for personal use is prohibited.

f. Maintaining the confidentiality, integrity, and availability of EnergyUnited data is paramount to the security and success of the cooperative. The following requirements are defined to keep data secure:

i. All organizational data is owned by EnergyUnited and, as such, all users are responsible for appropriately respecting and protecting all data assets.

ii. Users must keep all data secure by taking sensible precautions and following requirements defined in this policy.

iii. Users will only access data provided to them for duties in connection with their employment or engagement and in accordance with their terms and conditions of employment or equivalent. Access to some applications and information sources will be routinely recorded and/or monitored for this purpose.

iv. Extraction, manipulation, and reporting of EnergyUnited data is for business purposes only. Personal use of EnergyUnited data is prohibited.

v. Users will not store EnergyUnited data on devices that are not owned or managed by EnergyUnited.

g. A clean desk policy is an important tool to ensure that all sensitive materials, such as information about an employee, a member, or intellectual property, are removed from an end-user workspace and locked away when the items are not in use, or an employee leaves his/her workstation. This will reduce the risk of security breaches in the workplace and is part of standard basic privacy controls.

i. Employees are required to ensure that all sensitive information in hardcopy or electronic form is secure at the end of the day and when they expect to be gone for an extended period.

ii. Users must log off or lock their workstation when their workspace is unoccupied.

iii. Laptops must be locked away in a drawer if not taken home at the end of the workday.

iv. Any sensitive information (e.g., member data) must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the workday.

v. Passwords are not to be written down anywhere or under any circumstances.

vi. File cabinets containing sensitive information must be locked when not in use or unattended.

vii. Keys/badges used for access to sensitive information must not be left unattended.

viii. Printouts containing sensitive information must be immediately removed from the printer.

ix. Upon disposal, sensitive documents should be shredded.

x. Whiteboards containing sensitive information should be erased.

h. Passwords are an important aspect of cybersecurity. A poorly chosen password may result in the compromise of EnergyUnited's technology resources. The following requirements are in place to protect those passwords and access to technology resources and data:

i. Users may not share account or password information with another person. Accounts are to be used only by the assigned user of the account and only for authorized purposes.

ii. Users may not use the "Save Password" feature of web browsers (e.g., Chrome, Safari, Firefox).

iii. Passwords cannot be written down, instead use an encrypted password manager like LastPass.

iv. A user must contact the Service Desk to obtain a password reset if they have reason to believe any unauthorized person has learned their password.

v. Users may not use passwords used to access EnergyUnited communications and computer systems for other services (e.g., social media accounts, personal bank accounts). If other services are compromised, it could leave EnergyUnited accounts compromised as well.

vi. Passwords are not to include common usage words such as:

(1) Names of family, pets, friends, co-workers, fantasy characters, etc.

(2) Birthdays and other personal information

(3) Character patterns like aaabbb, 123321, or a month or year (e.g., January 2021)

(4) Password complexity will be enforced by IT through system-enforced policies to ensure strong passwords and proper password hygiene:

(5) Passwords will expire every 180 days and users will be forced to change them. Users should reset their passwords prior to the expiry date to minimize any access interruption.

(6) A minimum lifespan of 1 day is enforced to prevent too frequent password changes.

(7) The previous 5 passwords cannot be reused.

(8) Password complexity requirements enforce the use of uppercase, lowercase, numbers, and special characters.

(9) Upon 5 failed login attempts, accounts will be locked for 30 minutes. Accounts can be unlocked by contacting Service Desk or waiting for the 30 minutes to elapse.

i. EnergyUnited has an incident response program for efficient remediation of cybersecurity incidents. Employees are expected to comply with the following requirements to ensure effective and efficient incident remediation:

   i. Users must report any suspected security incident to the Service Desk, including but not limited to lost/stolen equipment, both personally owned equipment used to access EnergyUnited resources and EnergyUnited owned equipment, suspected malware infection, compromised credentials, and any other possible compromises of EnergyUnited resources and/or data.

   ii. Users must cooperate with incident response processes, such as surrendering their equipment to the Service Desk for investigation if it is potentially compromised.

j. Users may have the opportunity to use their personal electronic devices in accordance with this policy when authorized in writing. This section outlines requirements for bring your-own-device (BYOD) usage and establishes requirements for both users and the IT department to initialize, support, secure, and remove devices from access to EnergyUnited systems, networks, software, and/or data. BYOD devices include (but are not limited to):

   i. Desktops, laptops, and tablet computers.

   ii. Smartphones (defined as any cellular telephone that connects to the internet via Wi-Fi or a mobile provider network).

   iii. Flash, memory, and/or thumb drives.

iv. External hard disks.

v. Portable entertainment or music devices that connect to Wi-Fi networks.

vi. Entertainment and gaming consoles that connect to Wi-Fi networks and can be used to access EnergyUnited systems, networks, software, and/or data.

vii. Wearable devices such as watches, VR headsets, and augmented reality glasses with Wi-Fi or Bluetooth.

k. IT Responsibilities:

i. The IT department will implement administrative and technical controls to ensure secure and authorized use of BYOD to access EnergyUnited resources.

ii. The device does not have a detectable virus, spyware, or malware infection.

iii. The device does not have any third-party software or applications that pose a threat to EnergyUnited or that could introduce application incompatibilities. The IT department reserves the right to make judgment calls regarding which applications (current or future) are appropriate for devices associated with EnergyUnited systems, networks, software, and/or data.

iv. The device is properly protected against viruses, spyware, and other malware infections and that the device has properly licensed anti-malware software, when appropriate.

v. A security policy will be applied to enforce a password/biometric policy that will automatically lock the device after one-minute period of inactivity and erase the contents of memory and storage after a maximum of 10 failed authentication attempts.

vi. A security policy will be applied to remotely erase (wipe) devices in the event of loss or theft.

vii. The device has all critical and security patches installed.

viii. The device is properly encrypted if the potential exists for the device to save, cache, or even temporarily store organization data.

ix. The device is properly configured to access resources remotely and that it does so in the most secure fashion possible.

x. When a device is to be decommissioned, the IT department will remove any EnergyUnited software (e.g., anti-malware, mobile device management) from the user's device. It will also confirm that the user's device does not contain any traces of

protected, sensitive, corporate, or proprietary information and when possible, will delete any that remains on the device.

xi. IT reserves the right (and should proceed) to remotely wipe a device if it has been lost or stolen.

xii. When an employee has been terminated, IT is responsible for ensuring that EnergyUnited does not have a pending or ongoing investigation or litigation hold prior to wiping a device.

xiii. IT reserves the right to adjust the security policy applied to personally owned devices (current or future) to protect EnergyUnited systems, networks, software, and/or data.

l. User Responsibilities:

i. Users are not authorized to connect any personally owned device to EnergyUnited systems, networks, software, and/or data or access EnergyUnited systems, networks, software, and/or data via any personally owned device that has not been authorized under this policy and enrolled in EnergyUnited's device management software.

ii. Users are not authorized to change or disable any security settings or software applied to the device by the IT department.

iii. If a user believes a personally owned device used to connect to EnergyUnited's systems, networks, software, and/or data might be infected with a virus, spyware, or other malicious threat or might be somehow compromised, they must immediately call the IT department to notify them of the potential security risk.

iv. If a user loses or misplaces a personally owned device used to connect to EnergyUnited's systems, networks, software, and/or data, they must immediately call the IT department to notify them of the potential security risk.

v. When a user decommissions, prepares to return, or otherwise ceases using a personally owned device used to connect to EnergyUnited's systems, networks, software, and/or data, the user must notify the IT department that the device will no longer be used. Users may not discard previously authorized devices until the IT department approves the device for disposal.

vi. User whose personal devices have camera, video or recording capability are restricted from using those functions on company property at any time unless authorized in advance by management.

vii. While at work, users are expected to exercise the same discretion in using their personal devices as is expected for the use of EnergyUnited devices. EnergyUnited policies pertaining to harassment, discrimination, retaliation, trade secrets,

confidential information and ethics apply to employee use of personal devices for work-related activities.

viii. Users may not allow family, friends or other non-authorized individuals use of personal devices that are used to access EnergyUnited systems or data.

ix. EnergyUnited reserves the right to review or retain personal and company data on personal devices or to release the data to government agencies or third parties during an investigation or litigation. EnergyUnited may review the activity, analyze use patterns, and publicize these data to ensure that EnergyUnited's resources in these areas are being used according to this policy.

x. Personally owned devices may only connect to EnergyUnited resources through EnergyUnited's wireless access using the EU-Guest account, which does not provide access to internal systems or data. User's authorized to use personally owned devices requiring access to internal systems or data must connect via EnergyUnited's VPN through the EU-Guest wireless network.

xi. Employees are expected to protect personal devices used for work-related purposes from cybersecurity threats, loss, damage, or theft.

xii. Users understand and accept that EnergyUnited will not be responsible for loss or damage of personal devices, applications or data resulting from the use of personal devices to access EnergyUnited resources. Additionally, EnergyUnited is not responsible for maintaining, supporting use of, backing up, or restoring data or applications on personally owned devices.

m. Human error and negligence are common sources of security issues. EnergyUnited takes a proactive approach by requiring security awareness and training:

i. During onboarding, users will be required to undergo information security awareness and training.

ii. Users must complete ongoing security awareness and training as scheduled by the IT Department. Employees will be kept up to date on new improvements and emerging threats.

n. Technology resources are EnergyUnited's property as well as, for access and security purposes, the information they contain. We respect our employees' right to privacy; however, we grant access to our systems for business use. Employees must not expect that information contained in these systems is private. EnergyUnited reserves the right, from time to time, for commercial, legal, or otherwise valid reasons, to read, monitor, control, and access user files and messages created, saved, transmitted, or received. In the event of intercepted illegal activity, we will bring them to the attention of the appropriate authority without prior notification to the sender or receiver.

3. RESPONSIBILITY:

The Vice President of Information Technology is responsible for the implementation of this policy.

OMP-18: WEB ACCESSIBILITY

Version:

1. OBJECTIVE:

   To ensure accessibility of the Cooperative's website to people with disabilities.

2. POLICY CONTENT:

   a. The Cooperative is committed to ensuring accessibility of its website to people with disabilities.

   b. The Cooperative will apply the most current version of the Web Content Accessibility Guidelines (WCAG) as developed by the World Wide Web Consortium (W3C) in the design, creation, and maintenance of its web site content and all transactions that rely on web browsers for content presentation.

   c. The Cooperative's web content and transactions will conform with level "A," satisfying all priority one checkpoints, unless an "undue hardship," would be imposed on the Cooperative, as that term is defined by the Americans with Disabilities Act (ADA).

   d. The Cooperative's web site content and transactions will be reviewed at least annually to ensure compliance with this policy.

   e. This policy does not apply to user-generated content.

3. RESPONSIBILITY:

   a. The Chief Information Officer is responsible to carry out the responsibilities set out in this policy.

   b. The Chief Executive Officer is responsible for the review and any subsequent revision to this policy, subject to board approval.

OMP-19: ACCEPTABLE USE OF ARTIFICIAL INTELLIGENCE

Version: 2024.11.21

1. OBJECTIVE:

   Artificial Intelligence ("AI") and its maturation into easy-to-use tools will transform the workplace. EnergyUnited recognizes the potential of this technology and its value for our organization. This includes better decision making, automation of tasks, insights from company data, and other operational efficiencies. This policy provides requirements for EnergyUnited on the acceptable and ethical use of AI.

2. DEFINITIONS:

   a. Artificial Intelligence Technologies ("AI Technologies"): Machine-based systems that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI Technologies use machine and human-based inputs to perceive real and virtual environments and use model inference to formulate options for information or action.

   b. Confidential Data: Sensitive information that must be protected from unauthorized access, disclosure, or theft. Confidential information includes but is not limited to: Personally Identifiable Information ("PII"), business and competitive information, proprietary information, and any other information that would likely cause harm to the Cooperative or its Members if improperly divulged through unauthorized access, disclosure, or theft.

3. POLICY CONTENT:

   a. The Cooperative recognizes there is value in the proper use of AI Technologies and risk in the improper use of AI Technologies.

   b. To maximize the value and minimize the risks associated with the use of AI Technologies, the following principles shall be observed in connection with the implementation and use of AI Technologies:

      i. The privacy and protection of confidential information is the Cooperative's most important priority in the development, implementation, procural, and use of AI Technologies.

      ii. Implementation or use of unauthorized AI Technologies is prohibited.

      iii. Improper disclosure of confidential information in the use of AI Technologies is prohibited.

iv. It is the responsibility of every individual who uses AI Technologies to:

(1) never disclose confidential information in the use of AI Technologies.

(2) never use unauthorized AI Technologies.

(3) always ensure AI Technologies used are trusted, safe, and secure.

(4) always verify the accuracy of information produced by AI Technologies.

(5) always enter the minimum amount of data into AI Technologies necessary to achieve a goal.

(6) always ensure use of AI Technologies is consistent with the Cooperative's values, governing documents, and policies.

(7) Always immediately report to Information Technology any use of AI technologies or use of any products of AI Technologies that violate the Cooperative's values, governing documents, or policies.

c. Authorization To Implement or Use AI Technologies:

i. Requests for authorization to implement or use AI Technologies shall be submitted to Information Technology ("IT").

ii. IT shall not authorize the implementation or use of AI Technologies until a Cyber Security Risk Assessment has been performed to assess how the AI Technologies will be used and the risks associated with the AI Technologies and their use.

iii. IT shall maintain and publish a list of authorized and unauthorized AI Technologies.

iv. IT shall provide ongoing evaluations of approved AI Technologies and perform periodic audits, including random sampling of data generated by approved AI Technologies.

d. The Cooperative's Contracting Officers shall:

i. Ensure that use of AI Technologies by any third-party (e.g., agents, assigns, contractors, affiliates, partners, vendors, consultants, etc.) doing business with or acting on behalf of the Cooperative has AI Technology policies and procedures in place that:

(1) regulate the third-party's use of AI Technologies consistent with this policy; and

(2) when that third party has access to the Cooperative's confidential information, prevent such confidential information from being improperly divulged through

unauthorized access, disclosure, or theft in connection with the third-party's use of AI Technologies.

4. RESPONSIBILITY:

   a. Every user of AI Technologies is responsible to ensure such use is consistent with this policy.

   b. The Board President is responsible for the implementation and administration of this policy with regard to the Board of Directors.

   c. The CEO is responsible for the Cooperative's implementation of this policy.

   d. The Vice President of IT is responsibility for the Cooperative's administration of this policy.

   e. The Chief Human Resources Officer and Vice President of IT is responsible for promulgating employee policies as necessary to ensure the implementation and administration of this policy.

   f. Contracting Officers are responsible to ensure that use of AI Technologies by third parties doing business with or acting on behalf of the Cooperative is consistent with this policy.

   g. All supervisors are responsible for communicating the provisions of this policy to employees and ensuring employee compliance with this policy.

OMP-20: RELATIONSHIP WITH RURAL UTILITIES SERVICE AND NATURAL RURAL UTILITIES COOPERATIVE FINANCE CORPORATION

Version: 2015.12.17

1. OBJECTIVE:

   To set forth guidelines for the Cooperative's relationship with the Rural Utilities Service ("RUS") and National Rural Utilities Cooperative Finance Corporation ("CFC"), the following policy is hereby adopted.

2. POLICY CONTENT:

   The Board of Directors ("Board") and management shall at all times work in harmony with RUS and CRC and avail themselves of the services that would be of assistance in the operations of the Cooperative.

3. RESPONSIBILITY:

   a. It shall be the responsibility of the Chief Executive Officer to carry out this policy as it relates to management relationships.

   b. It shall be the responsibility of the President to advise the Board of any non-adherence to this policy on the part of the Board.

OMP-21: MEMBERSHIP IN OTHER ORGANIZATIONS

Version: 2015.12.17

1. OBJECTIVE:

   To assure participation in those organizations which will aid in the growth and development of the Cooperative, the Membership, the communities within the Cooperative's service area, the State of North Carolina, and the Nation, the following policy is established.

2. POLICY CONTENT:

   a. General: The Cooperative shall look with favor upon affiliating with or joining other organizations when in the opinion of the management and the Board of Directors ("Board") such would serve the best interests of the Cooperative.

   b. Active Memberships: The Cooperative shall be a member of or maintain an active interest in the following organizations: Tarheel Electric Membership Association, National Rural Electric Cooperative Association, Farmers Cooperative Council of North Carolina, North Carolina Electric Membership Corporation, North Carolina Association of Electric Cooperatives, and the Chambers of Commerce and Merchants Associations located within the Cooperative's service area.

3. RESPONSIBILITY:

   The Chief Executive Officer shall be responsible for the administration of this policy and shall bring to the attention of the Board such information as needed to fully implement the policy.

OMP-22: POLICY THAT COOPERATIVE IS NOT FOR SALE

Version: 2004.05.17

1. OBJECTIVE:

   To provide the underlying basis to the Board of Director's ("Board") Resolution that the Cooperative is not for sale.

2. POLICY CONTENT:

   a. The position of the Board is that the Cooperative is not for sale.

   b. This position of the Board does not mean that a proposal to purchase the Cooperative ('Proposal to Purchase') necessarily would not be recommended by the Board or approved by vote of the Members. Rather, the position is simply that the Board presently views the Cooperative as an excellent, viable cooperative enterprise, performing the services for which it was organized on the basis of the principles and purposes embodied in its organization. Therefore, the Board perceives no need or useful purpose in inviting, much less encouraging, Proposals to Purchase.

3. UNDERLYING CONDITIONS:

   In acting on a Proposal to Purchase from an Investor-owned utility ('IOU'), certain precepts will be taken into account:

   a. Value of Cooperative Structure: The Cooperative operates as a nonprofit, mutual benefit organization whose cardinal purpose is to provide its members/consumers with adequate and reliable electric service on an area coverage basis at the lowest cost consistent with sound business principles. All revenues received by the Cooperative in excess of its costs and expenses are allocated to its consumers on a patronage basis as capital credited to the accounts of the consumers. Those capital credits are retired to the consumers in accordance with the Cooperative's Bylaws and policies.

   b. IOU Has Profit Motive: An IOU is primarily an outlet for capital, preponderantly owned by absentee shareholders. Its purpose is to render utility service so as to earn the greatest profits for its shareholders at the least capital risk.

   c. Cooperatives and IOUs Coexist: In North Carolina, both cooperatives and IOU's exist and operate.

   d. Institutional Differences between Cooperatives and IOUs: The institutional differences between cooperatives and IOUs are both profound and important. These differences will be taken into account by the Board in its evaluation of any Proposal to Purchase. Two of these differences support the Board's position the Cooperative is not for sale:

i. Cooperative Not Organized for Profit: The Cooperative does not operate for the purpose of increasing the value of its consumer market, of its physical properties, and of its property interests with the view of converting them into profits. The Cooperative's market is its own consumer-member-owners on an area coverage scale, who govern the Cooperative by electing its Board and making certain other important decisions. This identity of market-member-ownership is an integral aspect of the Cooperative's objective of furnishing the best electric service at the lowest cost consistent with sound business principles and on a nonprofit basis.

ii. Cooperative is Socioeconomic Institution. The Cooperative is a socioeconomic institution with continuing community concerns. Thus, it exists not merely for the benefit of its present consumer-members, but for the benefit of future new consumers in the communities served by the Cooperative.

e. Nature of Proposal. A Proposal to Purchase, therefore, is not a proposal to acquire and continue the Cooperative as such, since a purchasing IOU will not operate the purchased entity as a cooperative. The Cooperative structure is wholly incompatible with the cardinal purpose of an IOU to earn profits on behalf of its absentee shareholders. Furthermore, an IOU seeks, in attempting to purchase a cooperative, not only the Cooperative's properties, going business and promising service areas, but also the cessation of competition.

f. Importance of Power Pluralism. Neither a cooperative utility nor an IOU merits particular praise or criticism as opposed to the other. Both are vital participants in a pluralistic industry that is otherwise necessarily affected by horizontal market monopolism. The pluralism consists in the fact that these types of utilities represent competing motives. Indeed, it has been the dynamic competition of these motives, as identified in (3)(a) and (3)(b), that has been primarily responsible for the fact that all Americans today, wherever situate, have access to reliable electric power at affordable rates. The preservation of this pluralism is therefore of vital concern not only to the Cooperative and its present and future constituency, but throughout American society in general.

4. RESPONSIBILITY:

It shall be the responsibility of the Board to ensure that this policy is implemented.

EXHIBIT A

ENERGYUNITED ELECTRIC MEMBERSHIP CORPORATION

RESOLUTION

ADOPTED: October 1, 1998

WHEREAS, EnergyUnited Electric Membership Corporation (the 'Cooperative') was created, and for more than 56 years has served, to bring electric service to homes, businesses, and farms in areas where service was not otherwise available;

WHEREAS, the Cooperative was organized to provide its members with adequate and reliable electric service, to assist its members in the efficient and economical use of energy;

WHEREAS, the Cooperative is a viable business, which is efficiently performing the services for which it was organized;

WHEREAS, the Cooperative is also a vital part of the community which it serves, and as such, has concerns that include the interests of that community;

WHEREAS, the Cooperative is operated as a non-profit corporation, whereby all revenues in excess of the Cooperative's expenses are allocated to its members on a patronage basis as capital credited to the members' accounts, and those capital credits are retired to the members in accordance with state law and the Articles of Incorporation and Bylaws of the Cooperative;

WHEREAS, the Cooperative is one of 28 distribution cooperative members of Carolina Electric Cooperatives, a generation and transmission electric cooperative (collectively, the 'Affiliated Cooperatives'); and

WHEREAS, the Cooperative is part of a closely related, interdependent cooperative system, and the effects of an action taken by one Affiliated Cooperative may materially affect the operations and viability of the other Affiliated Cooperatives.

NOW THEREFORE BE IT RESOLVED, that the Board of Directors of this Cooperative, having reviewed the current status of the Cooperative's affairs, and having considered the unique nature of the Cooperative and its benefits to its members, hereby determines that until the Board of Directors determines otherwise, the Cooperative is not for sale; and

BE IT FURTHER RESOLVED, that the Board of Directors hereby determines that until further notice, any employee of the cooperative who is presented with any inquiry regarding the sale, lease, merger, or other form of acquisition of the Cooperative shall immediately respond to the inquiry by stating that the Board of Directors has determined that the Cooperative is presently not for sale, and that the employee shall promptly notify the Chief Executive Officer who shall in turn notify the Board of Directors of any such inquiry.

BE IT FURTHER RESOLVED, that the Bylaws Adopted dated October 1, 1998, be approved as presented, and

BE IT FURTHER RESOLVED, that the Board Policy titled ‘Philosophy Behind Board Resolution That the Cooperative is Not For Sale’ be adopted as presented, and

BE IT FURTHER RESOLVED, that the Board Policy titled ‘Procedure for Potential Sale of All or Substantially All of the Cooperative's Assets to Another Entity’ be adopted as presented.

OMP-23: POTENTIAL SALE OF ALL OR SUBSTANTIALLY ALL OF THE COOPERATIVE'S ASSETS TO ANOTHER ENTITY

Version: 2004.05.17

1. OBJECTIVE:

   To establish, consistent with the Bylaws, procedures to follow in the event that an offer to purchase the Cooperative is presented by a third party.

2. POLICY CONTENT:

   a. Procedures:

      i. Inquiry: If an offer is received by the Cooperative and such offer is not a Qualifying Offer ("QO"), as defined in (2)(a)(iii), it shall be considered an "Inquiry." The recipient of any Inquiry shall notify the person, corporation, or other entity submitting the Inquiry, that, under the terms of this policy, the Board of Directors ("Board") shall not consider an offer unless it qualifies as a QO as defined in (2)(a)(iii).

      ii. Notice of QO: The Chief Executive Officer ("CEO") shall notify the Board of any Inquiry or QO immediately upon its receipt.

      iii. Provisions of QO: The Board shall consider only offers which meet all of the criteria listed in this paragraph. An offer that meets the criteria shall be considered a QO. If at any time it is determined that an offer does not meet all of the criteria in this paragraph, it shall be rejected by the Board, and the person, corporation, or other entity submitting the offer (the "Interested Party") shall be notified of the rejection. The Interested Party, however, shall be given an opportunity to submit additional information to meet these criteria within a reasonable period of time, not to exceed three months.

         (1) A QO must be a written offer, containing the acquisition price and all other material terms, and be binding upon the Interested Party until a specified date or until rejected.

         (2) A QO must specify the date on which it will expire if not accepted by the Cooperative.

         (3) A QO must disclose the identity of the Interested Party and be executed by authorized representatives of the Interested Party.

         (4) A QO must contain the names, addresses, and telephone numbers of persons representing the Interested Party with whom the Board may communicate and from whom it may secure authoritative answers regarding the QO.

(5) In light of the expense in responding to a QO, a QO must be accompanied with an escrow agreement acceptable to the Cooperative, which agreement shall require the Interested Party to deposit an amount equal to at least ten percent of the Cooperative's Total Utility Plant in an escrow account. The terms of the escrow agreement shall provide that the principal amount of the deposit may be drawn on by the Cooperative to pay for all costs (including accounting, engineering, legal, etc.) of studies, reviews, analysis, and appraisals by and for the Cooperative in its evaluation of the QO, and pay for all costs incurred by the Cooperative in seeking regulatory approvals. If the offer is withdrawn or rejected, any remaining balance in the escrow account shall be paid to the Interested Party when the Board certifies that all costs set forth in this section have been paid in full. In any event the deposited amount shall not be applied to the purchase price if a QO is eventually accepted by the Members, but shall be used to offset all costs incurred by the Cooperative in evaluating the offer.

(6) A QO must contain an agreement by the Interested Party to keep all terms and conditions of the offer confidential, not to issue press releases or discuss the QO with the media without prior written notification to the Cooperative, and to refrain from issuing misleading statements or advertising.

(7) A QO must not be in direct conflict with the terms of the Cooperative's Articles of Incorporation, Bylaws, this policy, any applicable law, or other policies.

iv. Acts Upon Receipt of QO: Upon a determination by the Board that it has received a QO, the Board shall:

(1) Designate an individual from the Cooperative to receive all communications, including telephone calls and written communications, from the Interested Party, the members, and the media. This individual shall understand and follow this policy, but shall not have the authority to bind the Board or the Cooperative on any matter regarding the QO.

(2) Notify the Members of the receipt of the QO. The Notice should include the following:

(a) A summary of the QO.

(b) A statement that the Board has taken the QO under advisement.

(c) A brief description of the procedures the Board shall follow in evaluating the QO.

(d) A statement that the Members may review a copy of the QO at the Cooperative's office during its regular business hours.

(e) The name of the person whom the Members may contact with questions regarding the QO.

(3) Send a copy of the QO to the Corporate Attorney.

(4) Send a copy of the QO to the G&T Cooperative of which it is a member and request a statement as to the effects of the QO upon the Cooperative's Wholesale Power Contract.

(5) Send a copy of the QO to any entity that has a Right of First Refusal according to the Bylaws or any existing First Refusal Agreement.

(6) Send a copy of the QO to the Rural Utilities Service ("RUS") and any other lenders and request a statement to the effects of the QO upon the Cooperative's Mortgage and Loan Agreement or other instruments relating to the Cooperative's outstanding debt.

(7) Have appointed or appoint three independent appraisers to determine the value of the Cooperative and its assets. The appraisers should use commonly accepted valuation methods, which shall be approved by the Cooperative.

(8) Obtain a comparison of the Cooperative's and the Interested Party's present and reasonably foreseeable future rates, fees, and charges, including service extension requirements, other service rules and regulations, adequacy and reliability of service, and any other considerations relevant to the provision of electric service.

(9) Request detailed information from the Interested Party, such as annual reports, tax returns and form 10-K filings dating back at least five years, full copies of all relevant audits, internal planning documents, employee policy manuals and union contracts, a current stockholder list, a list of all pending court and administrative proceedings, and any relevant operations manuals, engineering studies, construction plans, and environmental impact statements.

(10) Request the Interested Party to submit an expert opinion on the potential tax liabilities of the transaction to the Cooperative and the Members.

(11) Undertake any other investigations, studies, or comparisons, which the Board considers relevant to its evaluation of the QO.

(12) Evaluate the QO in accordance with the terms of this policy, considering the evaluation criteria set forth in paragraph (2)(b), and any other criteria which the Board deems relevant.

v. Rejection of QO. After evaluation, if the Board determines that the QO should be rejected, it shall notify the Interested Party and the Members of the rejection. The

Board shall also notify the Corporate Attorney, its G&T cooperative, any entities with First Refusal Agreement, RUS, and any other lenders of the Board's decision.

vi. Acceptance of QO. If, after evaluation, a two-thirds majority of the Board determines that the sale, lease, merger, or other acquisition proposed by the QO is in the best interest of the Cooperative and its Members, the Board shall notify the Interested Party of its intent to further pursue the transaction, subject to written agreement by the Interested Party to the following terms and conditions:

(1) That the Cooperative is released from or otherwise satisfies its Wholesale Power Contract.

(2) That any adverse tax impacts upon the Cooperative as an entity and its present and former Members will be minimized to the extent practicable.

(3) That all existing employees of the Cooperative are offered continued employment for at least three years upon terms at least equal to those enjoyed by the Cooperative's employees at the time the QO was submitted to the Board. The terms to be considered shall include wages, salaries, severance benefits, insurance and pension benefits, fringe benefits, rank and job title, union membership, place of employment, and residence.

(4) That the Interested Party will indemnify and hold harmless any employees, Directors, Officers, agents, servants, attorneys, accountants, consultants, representatives, affiliates, subsidiaries, and insurers of and all others acting in privity with the Cooperative for any actions taken in connection with the QO.

(5) That the total consideration for the acquisition will be paid directly to the Cooperative or its account; provided however, that a QO of merger may provide for acquisition of stock by the Members in exchange for their capital credits and membership.

(6) That the transaction will become void if all regulatory and contractual approvals are not obtained within a reasonable time after member approval.

vii. Notice of First-Refusal Opportunity. After the Board has received the Interested Party's written agreement to the terms and conditions in (2)(a)(vi), the Board shall submit a "Notice of Opportunity to Exercise Refusal" as provided in the Bylaws or any First Refusal Agreement to those parties having such rights thereunder. Once the Notice of Opportunity to Exercise Refusal has been submitted, the Board shall not permit the Interested Party to change any material terms in either its QO or its written agreement to the terms and conditions in (2)(a)(vi).

viii. Exercise of Right of First Refusal. If a party to the First Refusal Agreement exercises its rights thereunder (the "First Refusal Offer"), the Board shall proceed with a vote of

the Members on the First Refusal Offer pursuant to (2)(a)(ix) through (2)(a)(xii). The Board shall only proceed under (2)(a)(ix) through (2)(a)(xii), on a QO if no party to the First Refusal Agreement has exercised its rights thereunder, or if the Cooperative's Members have rejected the First Refusal Offer.

ix. Notice to Advisors of Vote. Before submitting the QO or the First Refusal Offer to a vote of the Members, the Board shall notify its corporate attorney, its G&T cooperative, RUS, and any other lenders of the Board's intention to submit it to a vote of the Members.

x. Notice to Members. Once the above procedures have been followed, the Board shall notify the Members in writing of its intent to submit the QO or the First Refusal Offer to the Membership for a vote. The notice shall include a summary of the final terms and conditions of the QO or the First Refusal Offer and comply with the Notice requirements of State law or the Bylaws. A Membership meeting shall be called for the purpose of voting on the QO or the First Refusal Offer. The meeting shall be called pursuant to the Cooperative's Articles of Incorporation, Bylaws, and applicable laws and regulations. Alternative positions may be mailed to the Members before the called meeting if a request to mail the positions is made by Member petition according to the Bylaws.

xi. Winding Up of Affairs. If the Members vote to accept the QO or the First Refusal Offer, the Board shall take all actions necessary to finalize the transaction and, if necessary, dissolve and wind up the business of the Cooperative; provided, however, that it shall be the responsibility of the Interested Party to obtain all necessary regulatory and contractual approvals. Unless such approvals are obtained within nine months of the date that the Members accept the QO, the transaction shall be deemed to be null and void.

xii. Two-Year Moratorium if Offer Rejected. If at any time a QO is rejected, whether by the Board or by the Members, or if a QO is withdrawn by the Interested Party, any further such QO by the Interested Party or any of its affiliates or subsidiaries within two years after the date of rejection shall be rejected by the Board unless the offer materially differs from the withdrawn or rejected QO.

b. Evaluation Criteria:

As provided in (2)(a)(iv)(9), above, the Board may consider any criteria which the Board deems relevant in its evaluation of a QO. To the extent practicable, and so long as not inconsistent with the best interests of the Members, the Board shall consider each of the following criteria:

i. The Interest of Members. Whether the QO is in the best interest of the present and future Members. In determining whether the Offer is in the Members' best interest,

the Board should consider both economic and non-economic matters, both at the present time and for the reasonably foreseeable future. Also, the factors contained in Board policy 6-16B, Philosophy Behind Board Resolution That The Cooperative Is Not For Sale, shall be considered in evaluating any offer.

ii. Financial Appraisals. The results of the independent appraisals concerning the fair value of the Cooperative. Although the Board shall consider all such information and opinions, it shall have the final responsibility to make the Cooperative's official determination of value and whether acceptance of the QO is in the best interests of the Cooperative and its Members.

iii. Legality of Offer. Whether the QO is in compliance with all applicable laws, regulations, and requirements of the Cooperative's Articles of Incorporation, Bylaws, and policies.

iv. Co-op Mortgage. Whether the QO complies with all requirements of the Cooperative's mortgage and loan documents.

v. Co-op Contracts. Whether the QO is in compliance, or would allow the Cooperative to comply, with all contractual obligations with other parties.

vi. Power Rates. Whether rates, fees, and other charges, and service rules and regulations of the Interested Party will be at least equivalent to, or better than, those of the Cooperative, both at the time of the QO and for the reasonably foreseeable future, but for a minimum of five years. In evaluating rates, the Cooperative's capital credit system shall be taken into account. In addition, the Board should consider how the Members' rates may be impacted in the future by the costs of the acquisition.

vii. Service Reliability. Whether the Interested Party's electric service would be at least as reliable as that provided by the Cooperative at the time of the QO and as projected into the reasonably foreseeable future.

viii. Other Service Qualities. Whether other service functions affecting the Members would be at least as good as those afforded by the Cooperative, and whether services provided to its Members will be as good or better than those provided by the Cooperative.

ix. Financial Strengths of Buyer. Whether the Interested Party is financially able to consummate the QO. The Board should also consider the source and feasibility of the proposed financing.

x. Community Involvement. Whether the Interested Party would continue or enhance the Cooperative's community involvement and continue any community-oriented Cooperative programs.

xi. Decimation of Inaccurate Information. If the Board determines that false or incorrect information is being decimated by one or more persons regarding an Inquiry or QO, the Board may either refuse to consider or reject the Inquiry or QO; or if a special meeting has been called, the Board may cancel the called meeting and reject the QO at that time, or take whatever other action it deems appropriate.

3. RESPONSIBILITY:

It shall be the responsibility of the Board to implement this Policy.

OMP-24: HANDLING CASES OF METER TAMPERING, POWER THEFT, AND POWER DIVERSION

Version: 2015.12.17

1. OBJECTIVE:

   To establish rules and procedures for the uniform treatment and handling of all cases involving apparent or potential meter tampering, power theft, and power diversion.

2. POLICY CONTENT:

   a. North Carolina General Statute 14-151, which is attached, declares that it shall be unlawful for any unauthorized person to alter, tamper with, or bypass a meter which has been installed for the purpose of measuring the use of electricity.

   b. Section 2.7 of the Bylaws addresses the responsibility and liability of a Member with regard to Cooperative property, including meters installed for the purpose of measuring electric current utilized by the Member. It is the policy of the Board of Directors ("Board") to carry out the intent of the Bylaws and to comply with the laws of North Carolina.

   c. In keeping with the principles of the Bylaws, this policy has been established to provide for the uniform, nondiscriminatory treatment of cases involving meter tampering, power theft, and power diversion.

   d. Electric service may be disconnected immediately and without prior notice for one or more of the following reasons:

      i. Discovery of meter tampering or bypassing.

      ii. Diversion of electric current.

      iii. Use of power for reasons prohibited by law.

      iv. Discovery of a condition determined by the Cooperative to be imminently and unduly hazardous.

      v. Use prohibited by the Bylaws, Board policies, Service Rules and Regulations, and Schedule of Rates and Charges.

   e. Electric service will be reconnected in the above cases under the following conditions:

      i. Correcting or ceasing the infraction.

      ii. Correction of any hazardous condition.

iii. Agreement to comply with reasonable requirements to protect the Cooperative against further infraction.

iv. Payment of:

(1) Triple the losses and damages suffered, to include, but not limited to, the actual or estimated lost revenues, field trip charges, disconnection and reconnection charges, investigation charges, any other applicable charges set forth in the Cooperative's Service Rules and Regulations or $5,000.00, whichever is greater.

(2) The cost of repair or replacement of the Cooperative's meter or any other properties, if tampered with or otherwise damaged or destroyed.

(3) Any service security deposits and providing the Cooperative with an adequate guaranty if the Cooperative so requires.

f. Definition of Terms:

i. Meter Bypassing: Providing or installing secondary conductor for electricity in order to avoid proper measurement of kilowatt hours of usage by a meter installed to measure such usage.

ii. Meter Tampering: Engaging in any improper and/or unauthorized entry to meter base and/or kilowatt-hour meter.

iii. Diversion of Electric Current: Changing the path of electricity to avoid proper measurement of such electricity by a kilowatt hour meter installed for such purpose.

g. This policy is supplemental to and in no way in lieu of any action taken by law enforcement authorities pursuant to the provisions of the North Carolina General Statute 14-151.

3. RESPONSIBILITY:

The Chief Executive Officer of the Cooperative shall be responsible for the administration of this policy.

EXHIBIT A

NORTH CAROLINA GENERAL STATUTES §14-151

§ 14-151. Interfering with gas, electric, and steam appliances or meters; penalties.

(a) It is unlawful for any person to willfully, with intent to injure or defraud, commit any of the following acts:

(1) Connect a tube, pipe, wire, or other instrument or contrivance with a pipe or wire used for conducting or supplying illuminating gas, fuel, natural gas, or electricity in such a manner as to supply the gas or electricity to any burner, orifice, lamp, or motor where the gas or electricity is or can be burned or used without passing through the meter or other instrument provided for registering the quantity consumed.

(2) Obstruct, alter, bypass, tamper with, injure, or prevent the action of a meter or other instrument used to measure or register the quantity of illuminating fuel, natural gas, water, or electricity passing through the meter by a person other than an employee of the company owning or supplying any gas, water, or electric meter, who willfully detaches or disconnects the meter, or makes or reports any test of, or examines for the purpose of testing any meter so detached or disconnected.

(3) In any manner whatever change, extend, or alter any service or other pipe, wire, or attachment of any kind, connecting with or through which natural or artificial gas or electricity is furnished from the gas mains or pipes of any person, without first procuring from the person written permission to make the change, extension, or alterations.

(4) Make any connection or reconnection with the gas mains, water pipes, service pipes, or wires of any person, furnishing to consumers natural or artificial gas, water, or electricity, or turn on or off or in any manner interfere with any valve or stopcock or other appliance belonging to that person, and connected with the person's service or other pipes or wires, or enlarge the orifices of mixers, or use natural gas for heating purposes except through mixers, or electricity for any purpose without first procuring from the person a written permit to turn on or off the stopcock or valve, or to make the connection or reconnections, or to enlarge the orifice of mixers, or to use for heating purposes without mixers, or to interfere with the valves, stopcocks, wires, or other appliances of them, as the case may be.

(5) Retain possession of or refuse to deliver any mixer, meter, lamp, or other appliance which may be leased or rented by any person, for the purpose of furnishing gas, water, electricity, or power through the appliance, or sell,

lend, or in any other manner dispose of the appliance to any person other than the person entitled to the possession of the appliance.

(6) Set on fire any gas escaping from wells, broken or leaking mains, pipes, valves, or other appliances used by any person in conveying gas to consumers, or interfere in any manner with the wells, pipes, mains, gate boxes, valves, stopcocks, wires, cables, conduits, or any other appliances, machinery, or property of any person engaged in furnishing gas to consumers unless employed by or acting under the authority and direction of that person.

(7) Open or cause to be opened, or reconnect or cause to be reconnected any valve lawfully closed or disconnected by a district steam corporation.

(8) Turn on steam or cause it to be turned on or to reenter any premises when the steam has been lawfully stopped from entering the premises.

(9) Reconnect electricity, gas, or water connections or otherwise turn back on one or more of those utilities when they have been lawfully disconnected or turned off by the provider of the utility.

(10) Alter, bypass, interfere with, or cut off any load management device, equipment, or system which has been installed by the electricity supplier for the purpose of limiting the use of electricity at peak-load periods. However, if there has been a written request to remove the load management device, equipment, or system to the electric supplier and the electric supplier has not removed the device within two working days, there is no violation of this section.

(b) Any meter or service entrance facility found to have been altered, tampered with, or bypassed in a manner that would cause the meter to inaccurately measure and register the electricity, gas, or water consumed or which would cause the electricity, gas, or water to be diverted from the recording apparatus of the meter is prima facie evidence of intent to violate and of the violation of this section by the person in whose name the meter is installed or the person or persons so using or receiving the benefits of the unmetered, unregistered, or diverted electricity, gas, or water.

(c) For the purposes of this section, the term "gas" means all types and forms of gas, including, but not limited to, natural gas.

(d) Criminal violations of this section are punishable as follows:

(1) A violation of this section is a Class 1 misdemeanor.

(2) A second or subsequent violation of this section is a Class H felony.

(3) A violation of this section that results in significant property damage or public endangerment is a Class F felony.

(4) Unless the conduct is covered under some other provision of law providing greater punishment, a violation that results in the death of another is a Class D felony.

(e) Whoever is found in a civil action to have violated any provision of this section is liable to the electric, gas, or water supplier in triple the amount of losses and damages sustained or five thousand dollars ($5,000), whichever is greater.

(f) Nothing in this section applies to licensed contractors while performing usual and ordinary services in accordance with recognized customs and standards. (1901, c. 735; Rev., s. 3666; C.S., s. 4323; 1993, c. 539, s. 88; 1994, Ex. Sess., c. 24, s. 14(c); 2013-88, s. 1; 2018-142, s. 2(a).)

OMP-25: ELECTROMAGNETIC FIELDS

Version: 2015.12.17

1. OBJECTIVE:

   To provide employees and Members with a policy statement regarding the Cooperative's position concerning EMF issues and to provide for the timely sharing of information about EMF issues.

2. POLICY CONTENT:

   a. The Cooperative recognizes the need for scientific study of this issue and is proactively supporting a portion of the costs of research through regular dues to the National Rural Electric Cooperative Association. EMFs are present in all electrical applications whether man-made or natural. At this time, there is no conclusive evidence that EMFs post a health risk.

   b. The Cooperative on has a demonstrated commitment to providing electricity in a manner that protects the health and safety of all our Members and employees. This commitment includes the EMF issue. At this time, the Cooperative will not change its practices in design, construction, or routing of power lines in anticipation of a perceived EMF issue.

   c. The Cooperative will undertake measurements of EMF strengths on behalf of a Member or employee. Reasonable request of measurements will be performed even though no determination has been made that EMFs are harmful. Even if so determined, there is not yet a determined "unsafe level" of exposure to EMFs or the amounts originating from different sources, both man-made and natural. Until scientific research develops methods of measurement and meaningful levels of exposure to EMF any measurements made will not produce meaningful information. This practice will change over time as more understanding is achieved and scientific methods developed.

   d. The Cooperative will provide Members and employees with information concerning any significant events in the course of EMF research or practices by other utilities as such information becomes known to the Cooperative. The Cooperative's collection of EMF materials and literature will not be comprehensive but will be shared with any employee or Member that requests more information.

3. RESPONSIBILITY:

   The Chief Executive Officer shall be responsible for the administration of this policy.

OMP-26: ENTERPRISE RISK MANAGEMENT

Version: 2024.11.21

1. OBJECTIVE:

    a. To establish common risk language and direction related to risk management, the Board of Directors ("Board") and Chief Executive Officer ("CEO") commit to develop a structured Enterprise Risk Management ("ERM") plan to increase the likelihood that strategic objectives will be achieved.

    b. Understanding the material risks faced by the Cooperative and assessing the adequacy of the Cooperative's response to those risks requires an understanding of the Cooperative's underlying business.

2. POLICY CONTENT:

    The purpose of this policy is to create, enhance, and protect the members' cooperative by designing, implementing, and maintaining an effective, structured, and enterprise-wide risk management approach. The ERM approach is designed to be an integral process of the ongoing strategic and operational activities of the Cooperative. Accordingly, the approach is intended to minimize vulnerabilities and exploit opportunities by employing a systematic process of Risk Identification, Risk Assessment, Risk Management and Response, Risk Monitoring, and Risk Communication. The Board believes that adopting this policy will result in both immediate and long-term benefits to internal and external stakeholders.

3. EXPECTATIONS:

    a. GENERAL:

        i. The Board, in consultation with the CEO, will establish an ongoing strategic planning process to ensure the strategic plan considers potential enterprise risks and opportunities and leads to an understanding of the nature and magnitude of significant risks to which the Cooperative is exposed.

        ii. The Board will oversee, and the CEO will implement and manage, a process to provide that material risks which potentially pose a significant threat to the success of the Cooperative, are continuously identified, assessed, managed, monitored, and reported on a consistent basis and within acceptable risk tolerances. Reports on the assessment or risk levels compared to established strategic risk targets will be reviewed as needed.

        iii. The development and implementation of the ERM process and framework will be based on best practices in risk management. The scope of the risk management policy is intended to be "enterprise-wide," and the application of risk management aims to

enhance and protect the unique combination of tangible and intangible assets comprising the Cooperative's business model.

b. RISK IDENTIFICATION:

i. The Board, in consultation with the CEO, will determine the key risks which have been identified as, but not be limited to:

(1) Financial.

(2) Operational.

(3) Reputational.

(4) Technology.

(5) Safety.

(6) Power Supply.

(7) Cybersecurity.

(8) Regulatory.

(9) Legal.

(10) Member.

c. RISK ASSESSMENT:

i. The Board will analyze the potential severity, probability, timing, and cost of the impacts associated with each of the identified risks. The Board, in consultation with the CEO, will determine the appropriate risk assessment tools to utilize (e.g., qualitative approaches, statistical data, reports, impact matrix, etc.).

ii. RISK APPETITE AND RISK TOLERANCE:

(1) The CEO will define and set the acceptable risk appetite and tolerance levels for review and approval by the Board, which will be incorporated into the Cooperative's strategic planning and decision-making processes. Risk appetite is the amount of risk, on a broad level, that the Cooperative is willing to accept in pursuit of its strategic objectives, whereas tolerance levels set the acceptable boundaries of performance variability in achieving those objectives.

(2) The Board, in consultation with the CEO, will determine an acceptable level of risk appetite and risk tolerance for each key function within the cooperative, recognizing the interdependence of the functions.

(3) The risk appetite will be defined (e.g., Low/Modest/High, etc.) by the CEO for review by the Board for each key function, including quantitative or qualitative attributes. In addition to this policy, significant identified risks must have Board-approved risk management policies or risk management strategies in place.

(4) Risk tolerances that reflect the level of risk appetite determined by the CEO will be approved by the Board and be developed for each identified significant risk which will be set out in the Cooperative's Risk Appetite and Risk Tolerance Matrix.

d. RISK MANAGEMENT & RESPONSE:

i. The Cooperative will develop and implement a risk management system that includes the possible strategies to avoid, transfer, mitigate or accept risks.

e. RISK MONITORING:

i. The Board, in consultation with the CEO, will identify and determine what methods will be used to monitor risks. The Board reviews the monitoring process with the CEO to ensure that monitoring process is in place and working effectively.

ii. The Board will ensure adequate resources and expertise are dedicated to risk management:

(1) Provide adequate budgeting for risk management and oversight activities.

(2) Ensure risk management is supported by adequate and robust information technology ("IT") and management information systems ("MIS") to enable identification, measurement, assessment, and reporting of risk in a timely and accurate manner.

(3) Annually, and additionally as needed, review the enterprise risk management plan to ensure that risk exposures remain appropriate and prudent.

f. RISK COMMUNICATION:

i. The Board will ensure that the Cooperative identifies, captures, and communicates relevant information in a form and timeframe that enables employees, members, lenders, regulators, law enforcement, media, and others to carry out their responsibilities.

ii. Orientation for new Directors and employees and ongoing training programs for all Directors and employees will be encouraged to enable Directors and employees to

maintain an understanding of the Cooperative's risk profile and to help keep Directors and employees abreast of current industry trends and the Cooperative's specific developments and specialized issues.

4. RESPONSIBILITIES:

   a. The Board President shall see that this policy is carried out.

   b. The Board is responsible for establishing a strategic planning process, ensuring the strategic plan considers potential enterprise risks and opportunities, understanding the nature and magnitude of significant risks to which the Cooperative is exposed, providing adequate resources, monitoring ERM process and, ensuring the Cooperative's internal controls are working effectively.

   c. The CEO is responsible for identifying emerging strategic and operational risks and assessing them based on likelihood and impact, reporting on key risks and the effectiveness of the corresponding mitigation strategies, ownership and day-to-day oversight and management of individual risks and ensuring alignment between the Cooperative's strategic objectives and risk management.