Beartooth Electric Cooperative, Inc.

ADMINISTRATIVE POLICY NO. 631

1. SUBJECT: SECURITY & USAGE OF TELEPHONES, COMPUTERS, THE INTERNET AND OTHER ELECTRONIC EQUIPMENT

2. OBJECTIVE:

   2.1. To establish guidelines for the use of telephones and electronic equipment, including cell/camera/smart phones, computers, the Internet and related equipment at Beartooth Electric Cooperative, Inc. (BEC).

3. POLICY:

   3.1. All electronic and telephonic communication systems and all communications and information transmitted by, received from or stored in these systems are the property of BEC are to be used solely for job-related purposes. The use of any software and business equipment, including, but not limited to, facsimiles, telecopiers, computers, BEC's e-mail system, the Internet, Blackberrys, PDAs or other wireless devices, instant messaging systems and copy machines for private purposes is strictly prohibited.

   3.2. Employees using the equipment for personal purposes do so at their own risk. Further, employees are not permitted to use a code, access a file or retrieve any stored communication unless authorized to do so or unless they have received prior clearance from an authorized BEC representative. All passwords are the property of BEC. No employee may use a password or voice-mail access code that has not been issued to that employee or that is unknown to BEC without authorization. Moreover, improper use of the e-mail system (e.g., transmitting or spreading sexually, racially or other discriminatory or harassing jokes or remarks, abusive or profane language, threatening others, etc.), including via the Internet or any other equipment, will not be tolerated.

   3.3. To ensure that the use of electronic and telephone communications systems and business equipment is consistent with BEC's legitimate business interests, authorized representatives of BEC may monitor the use of such equipment from time to time. This includes monitoring Internet usage of any kind, including while using BEC's systems. This may also include listening to stored voice-mail messages or reviewing stored e-mail messages. Monitoring may occur, among other purposes, to:

      3.3.1. Ensure that all BEC electronic equipment, including computers and other communication resources are being used in a cost-effective matter strictly for business purposes.

      3.3.2. Carry out its business activities without disruption.

      3.3.3. Investigate suspicion of wrongdoing or illegal activities.

3.3.4. Protect the integrity, confidentiality and security of its computer networks and data.

3.3.5. Accomplish other appropriate objectives at BEC's discretion.

3.4. BEC provides access to the Internet. The Internet represents a useful tool for the company in conducting its business, but like any other tool, it must be used properly. For purposes of this policy, Internet includes any public electronic data communications network.

3.5. Each employee's computer access password generally is known only to the employee and should be kept confidential. Employee computer access passwords are to be registered with the system administrator. An employee's computer login ID/password combination may not be used by other employees to access those functions and data files restricted to that employee. Access rights, however, may be extended to the employees' immediate supervisor or others when necessary to meet business needs.

3.6. Because computers are vital to our business, computer virus contamination must be diligently avoided. To protect against computer viruses:

3.6.1. BEC shall install antivirus software on all computers. BEC shall update all software as updates become available.

3.6.2. Only BEC authorized software may be downloaded, installed or used on BEC equipment. Any question regarding authorized software should be directed to the system administrator. Users are responsible for ensuring software is approved before installing. Responsibility for maintenance of the user installed software remains with the user.

3.6.3. No data files or e-mail attachments should be opened, downloaded or loaded into any BEC computer unless the user is familiar with the source or sender and it is relevant to BEC business. This includes files from discs, flash drives, as well as downloads from the Internet
.

3.7. BEC strives to maintain a workplace free of harassment and is sensitive to the diversity of its employees. Therefore, BEC prohibits the use of electronic equipment, computers, the Internet and the e-mail system in any way that is not relevant to BEC business, including any ways that are disruptive, offensive to others or harmful to morale.

3.8. Attempts to access unauthorized machines via the computer network, to decrypt encrypted materials or to obtain access to areas where the user is not entitled (hacking) is prohibited. Member/Customer information, employee information, manipulation of files, access to unauthorized parts of BEC's managed computers and network infrastructure, attempts to circumvent data protection schemes, discovery of security loopholes or possession of such software by users is prohibited.

3.9. Abuse of telephone, cell/camera/smart phones and computer use or Internet access provided by BEC in violation of the law or BEC's policies will result in disciplinary action, up to and including termination of employment. Employees may also be held liable for any violations of this policy. Examples of actions and activities that are prohibited and can result in disciplinary action are identified below, under Item 3.10.

3.10. Examples of misuse include, but are not limited to, the activities in the following list. Activities will not be considered misuse when authorized by appropriate BEC officials for security or performance testing.

3.10.1. The display or transmission of sexually explicit images, messages and cartoons: participation in the viewing or exchange of pornography or obscene materials.

3.10.2. Sending or posting messages or material that could damage the organization's image or reputation.

3.10.3. Sending or posting discriminatory, harassing or threatening messages or images.

3.10.4. Examples of unacceptable content may include, but are not limited to, sexual comments or images, racial slurs, gender-specific comments or any other comments or images that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation or any other characteristic protected by law.

3.10.5. Using a computer account that you are not authorized to use or obtaining a password for a computer account without consent of the owner.

3.10.6. Using BEC's network to gain unauthorized access to any computer system.

3.10.7. Knowingly performing an act which will interfere with normal operation of computers, terminals, peripherals or networks.

3.10.8. Knowingly running or installing on any computer system or network or giving to another user, a program intended to damage or to place excessive load on a computer system or network. This includes, but is not limited to, programs known as computer viruses, Trojan horses and worms.

3.10.9. Attempting to circumvent data protection schemes or uncover security loopholes.

3.10.10. Violating terms of applicable software licensing agreements or copyright laws.

3.10.11. Deliberately wasting computing resources.

3.10.12. Masking the identity of an account or machine.

3.10.13. Posting materials on electronic bulletin boards that violate existing laws or BEC's code of conduct.

3.10.14. Attempting to monitor or tamper with another user's electronic communications or reading, copying, changing or deleting another user's files or software without the explicit agreement of the owner.

3.10.15. Participating in web-based surveys or interviews without authorization.

3.10.16. Using BEC's systems and equipment for personal blogging, i.e., keeping online journals that chronicle various aspects of the blogger's life, such as problems on the job, issues in their personal life, politics, their favorite TV shows, etc. Prohibited by this policy is spending time on the job writing one's own blogs, reading personal blogs those created by others or otherwise making disparaging or derogatory comments or remarks about BEC or any of its current or trustees, officers or employees at any time.

3.10.17. Violating copyright law.

3.10.18. Engaging in any other illegal activities.

4. REPORTING OBLIGATIONS:

4.1. Employees must notify the General Manager when:

4.1.1. sensitive or confidential information is lost, disclosed to unauthorized parties or suspected of being lost or disclosed to unauthorized parties;

4.1.2. unauthorized use of computing resources has taken place or is suspected of taking place;

4.1.3. passwords or other system access control mechanisms are lost, stolen or disclosed or are suspected of being lost, stolen or disclosed; or

4.1.4. there is any unusual systems behavior, such as missing files, frequent system crashes or misrouted messages.

4.2. Employees are prohibited from reading, modifying, copying or deleting files of others without permission.

5. EMPLOYEE ACKNOWLEDGMENT FORM:

5.1. As a condition of employment and continued employment, employees are required to sign an e-mail and voice-mail acknowledgment form (see sample form following this policy statement). Applicants are required to sign this form on acceptance of an employment offer by BEC.

6. RESPONSIBILITY:

6.1. The General Manager shall ensure that the provisions of this policy are followed.

Adopted: 02/22/2013
Revised: 06/30/2015
Reference: BEC VI-A-9
Review Date: June 2017

Attest: /s/ Richard Nolan
Secretary/Treasurer

Attest: /s/ Roxie Melton
Board President