POLICY

SUBJECT: Cyber Security

OVERVIEW & PURPOSE

Delaware County Electric Cooperative (DCEC) is committed to protecting DCEC employees, stakeholders and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, Internet Web browsing, and FTP, are the property of DCEC. These systems are to be used for business purposes in serving the interests of the company, and our customers in the course of normal operations. DCEC's intentions in publishing a Cyber Security Policy are not to impose restrictions that are contrary to DCEC's established culture of openness, trust and integrity.

Effective security is a team effort involving the participation and support of every DCEC employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

The purpose of this policy is to outline the acceptable use of computer equipment and Information Technology (IT) infrastructure at DCEC. These rules are in place to protect the employee's and DCEC. Inappropriate use exposes DCEC to risks including computer virus attacks, compromise of network systems and services, and legal issues. The policy balances the employee's ability to benefit fully from information technology with the company's need for secure and effectively allocated IT resources.

This policy applies to employees, contractors, consultants, temporaries and other workers at DCEC, including all personnel affiliated with third parties. This policy applies to all equipment, software and/or applications that are owned, licensed or leased by DCEC.

POLICY

A. General Use and Ownership

1. While DCEC's board of directors and managers desire to provide users with reasonable access to IT infrastructure to accommodate both the demands of the work environment and permitted personal use, users should be aware that data they create on the corporate systems remains the property of DCEC. Because of the need to monitor the internal network (Intranet) in order to protect DCEC's IT resources and information, management cannot guarantee the confidentiality of personal information stored on any network device belonging to DCEC or in files on the DCEC Intranet.

2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. DCEC owned IT equipment and computers and related services may be used for incidental personal use during break periods provided that:
   - Usage is reasonable and does not interfere with work productivity.
   - Does not directly or indirectly interfere with DCEC business operations, IT facilities or electronic mail services.
   - Does not burden DCEC with noticeable incremental cost.
   - If there is any uncertainty as to what constitutes acceptable personal use, employees should consult their supervisor or the General Manager who will make the determination.

3. Since Internet activities may be monitored, all personnel accessing the Internet shall have no expectation of privacy.

B. Security and Proprietary Information

1. Users may not encrypt any emails without obtaining written permission from their supervisor and DCEC's General Manager. If approved, the encryption key(S) must be made known to DCEC's General Manager.

2. Data residing on DCEC corporate IT systems may be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines. Examples of confidential information include but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, and member lists. Employees should take all necessary steps to prevent unauthorized access to this information.

3. For security and network maintenance purposes, authorized individuals within DCEC may monitor equipment, systems and network traffic at any time, with prior authorization of the General Manager.

4. DCEC reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

5. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code. DCEC utilizes Anti-Virus software on each workstation and server as well as filtering all inbound email through an outside security firm, but some unsafe attachments may still find their way through the defenses. Users are expected to use reasonable caution in reviewing incoming emails, looking for any indication that the sender may different than as represented. If there are ever any questions or if an individual is unsure, please contact the General Manager prior to opening the attachment.

6. Because information contained on approved portable and laptop computers is especially vulnerable, special care should be exercised to protect both the computer and its information.

7. Employees shall not use DCEC e-mail, or other facilities to post to news groups, message boards, or websites unless the posting is in the course of business duties.

8. The General Manager shall report any known breaches of cyber security to the Board of Directors as soon as practical after discovery, no later than the next regular meeting of the Board of Directors. If no known breaches of cyber security become known to the General Manager within a calendar year, then the General Manager shall certify to that fact in the annual Red Flag Report to the Board of Directors.

C. Passwords

1. Passwords are used for various purposes at DCEC. Some of the more common uses include: user-level accounts, web accounts, email accounts, screen saver protection, and router logins. Since very few systems have support for one-time tokens (i.e. dynamic passwords which are only used once), everyone should know how to select strong passwords

2. Poor, weak passwords have the following characteristics:
   - The password contains less than eight characters
   - The password is a word found in a dictionary (English or Foreign)
   - The password is a common usage word such as:
     - Names of family, pets, friends, co-workers, fantasy characters, etc.
     - Computer terms and names, commands, sites, companies, hardware, software.
     - The words "REA", "DCEC", "Delhi", or any derivation.
     - Birthdays and other personal information such as addresses and phone numbers.
     - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
     - Any of the above spelled backwards.
     - Any of the above preceded or followed by a digit (e.g. secret1, 1secret)

3. Strong passwords have the following characteristics:
   - At least eight alphanumeric characters long.
   - Contain both upper and lower case characters (e.g., a-z, A-Z)
   - Have digits and punctuation characters as well as letters (e.g., 0-9, !@#$%^&*()_+|~=\{}[]",'<>?)
   - Not a word in any language, slang, dialect, jargon, etc.
   - Not based on personal information, names of family, etc.
   - Try to create a password that can be easily remembered. One way to do this is create a password based on a song title, affirmation or other phrase. For example, the phrase might be: "This may be one way to remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

4. Password Creation
   - All user-level and system-level passwords must conform to the guidelines for strong passwords described above.

- Users shall never use the same password for DCEC accounts as for other non-DCEC access (for example, personal ISP account, option trading, benefits, and so on).
- User accounts that have administrator/system-level privileges must have a unique password from all other accounts held by that user.
- Where Simple Network Management Protocol (SNMP) is used, the community strings must be defined as something other than the standard defaults of public, private, and system and must be different from the passwords used to log in interactively. SNMP community strings must meet password construction guidelines.

5. Password Change
   - All system-level passwords (for example, root, enable, Windows Domain admin, application administration accounts, and so on) must be changed on a reasonable periodic basis.
   - All user-level passwords (for example, email, web, desktop computer, and so on) must be changed at least every 90 days.
   - Password cracking or guessing may be performed on a periodic or random basis by the General Manager or a designee. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Password Construction Guidelines.
   - Passwords may be required to be changed upon identification or notification of a cybersecurity incident or threat.

6. Password Protection
   - Passwords must not be shared with anyone, including administrative assistants, secretaries, managers, co-workers, and/or IT contractor without the permission of the General Manager. In cases where a password is shared with another employee or IT contractor for a specific purpose and defined time period as approved by the General Manager, the password shall be changed by the password's owner at the conclusion of the approved activity or time period, whichever ends first.
   - Passwords must never be shared with anyone other than General Manager approved employees or IT contractors, including friends and/or family members.
   - Passwords must not be inserted into email messages or other forms of electronic communication.
   - Do not reveal a password on questionnaires or security forms.
   - Do not hint at the format of a password (for example, "my family name").
   - Do not write passwords down and store them in an unlocked location in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) in clear text.
   - Do not use the "Remember Password" feature of applications (for example, web browsers).
   - Any user suspecting that his/her password may have been compromised must report the incident to DCEC's General Manager and change all passwords.

D. <u>Anti-Virus Protection And Prevention</u>

1. Virus Protection Overview
   All computing systems, both physical and virtual, connected to the Cooperative network shall have an anti-virus and anti-malware application installed, configured, activated and updated with the latest threat definitions. The Cooperative network shall include the office headquarters and any location connected via virtual private network tunnel to the office headquarters (e.g., operations shop and substations). This anti-virus and anti-malware software application must be capable of real-time scanning protection of files and applications running on the target system.

2. Guidelines
   - Employees shall be instructed NOT to trust any other source for virus protection patches.
   - Ensure that the current version is installed with anti-virus updates as they become available. Updates shall be no more than four weeks out of date.
   - The anti-virus and malware software should be configured so as to always scan removable media and devices attached to cooperative computers prior to use. If this is not an available option, this can be accomplished by opening the anti-virus client software and selecting the appropriate media and manually executing a scan.
   - Whenever new threats are identified, and determined by the General Manager to be of sufficient concern to cooperative business, the General Manger shall notify all corporate computer users about the new threat and appropriate measures to take, if any.
   - Virus or malware infected computers must be isolated from the Cooperative's network until they are verified as virus-free.
   - Employees will be educated about safe anti-malware practices such as, but not limited to;
     - Not opening unexpected attachments
     - Not downloading files from unknown sources
     - Deleting spam, chain mails, junk emails
   - To expedite the recovery from any virus/malware threats the General Manager shall ensure that all critical network data and system configurations are backed up in accordance with this policy.

E. <u>Backup and Recovery</u>

1. Backup Overview
   DCEC requires that server computer systems be backed up on a regular basis and that the backup media is located/stored in a secure off-site location. The purpose of the systems backup is to provide a means to restore the integrity of the computer systems in the event of a hardware/software failure or physical disaster and provide a measure of protection against human error or the inadvertent deletion of important files. Systems backups are not intended to serve as an archival copy or to meet records retention requirements.
   - The frequency and extent of backups must be in accordance with the importance of the information and the acceptable risk as documented in this policy.

- DCEC information technology backup and recovery processes for each system and service should be annually reviewed by the General Manager.
- Backup procedures should be periodically tested to ensure that the IT resource is recoverable.
- Procedures for the offsite backup storage should be reviewed periodically.
- Backup media must be readily identified by appropriate labeling, and noted in a centralized log as to its physical storage location.
- All critical information used on workstations should be placed on networked file server drives for backup.

2. Network Storage Structure
   DCEC has network servers in place in Delhi, NY. DCEC management and staff have file storage folders allocated for their account on network servers. These storage areas are usually referred to as the users "X: drive", where X denotes a mapped storage area on a network server as described below;
   H: Drive - Users personal folder on the network server
   When the user successfully logs on to their workstation, network connections are established to these folders, which can then be accessed as the "X: Drive" in Windows Explorer, Microsoft Word, Excel, and other software programs. Files can be copied from the user's workstation to their "X Drive", or software programs may be configured to save files directly to these mapped drives. These mapped drives are backed up to network storage and removable media. The removable media shall be rotated to an off-site storage facility and securely stored to provide for security and disaster recovery.

3. Storage of User Data Files
   In order to be able to recover lost data, management and staff should store essential data files requiring backup to one of the network mapped drives. Data files on the user's local workstation will generally not be recoverable if the drive fails. Appropriate use of network storage will ensure ample capacity for archival storage of user data files. Users should store and maintain data files (or current copies) that are important to the company and that would be costly or impossible to recreate, on the network mapped drives. Users should not store non-business or non-essential data files on the network drives. No data files should be stored on thumb drives or other portable data storage devices and removed from DCEC facilities, except as authorized by the General Manager.

4. Backup Schedule
   The systems backups will consist of regular full and incremental backups in accordance with Appendix A, "DCEC Backup Schedule by System".

5. Documentation
   DCEC information technology backup and recovery processes for each system and service must be documented by the General Manager.
   - Backup documentation includes identification of all critical data, programs, documentation, and support items that would be necessary to perform essential tasks during a recovery period.

- Documentation of the restoration process must include procedures for the recovery from single-system or application failures as well as a total data center disaster scenario.
- Backup and recovery documentation will be reviewed and updated annually to account for new technology, business changes, and migration of application to alternative platforms. Recovery procedures will be tested on an annual basis where feasible.

6. Backup verification
   Test restores from backup archives must be performed at least annually where feasible. This ensures that both the archive media and backup procedures work properly. It must at least once be proven that complete data restoration is possible. This ensures reliable testing as to whether:
   - Data restoration is possible
   - The data backup procedure is practical
   - There is sufficient documentation of the data backup process, thus allowing a substitute to carry out a data restoration if necessary
   - The time required for the data restoration meets the availability requirements

7. Offsite Storage
   In order to provide disaster recovery capability, backup media are rotated to an offsite storage location from the backup source. Backup media are maintained in offsite storage according to the schedule outlined in Appendix A, DCEC Backup Schedule by System"

8. File Recovery
   In order to have a file restored from the backup archive, the user should contact the General Manager and provide the date of the last known good version of the file – this will help identify the set of backup media to use in attempting to restore the file.

   Files can usually be restored within a few hours or less. DCEC cannot restore data files which were not archived on the network servers. As the media is rotated, users should request restoration of data files as soon as possible to prevent data being overwritten on the backup media.

9. Open Data Files
   The backup server software is unable to archive data files which are open at the time the backup is run. Each user should ensure that all files that are to be archived are closed at the end of each business day.

10. Backup Failures
    All backup failures will be logged and investigated as soon as practical upon detection.

F. <u>Unacceptable Use</u>

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use. The following activities are strictly prohibited, with no exceptions:

1. System and Network Activities
   - Under no circumstances is an employee of DCEC authorized to engage in any activity that is illegal under local, state, federal or international law, while utilizing DCEC owned resources.
   - Violation of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by DCEC.
   - Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which DCEC or the end user does not have an active license is strictly prohibited.
   - Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
   - Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.)
   - Using DCEC computing assets to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
   - Making fraudulent offers of products, items or services originating from any DCEC account.
   - Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
   - Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee in not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service (DOS), and forged routing information for malicious purposes.
   - Port scanning or security scanning is expressly prohibited unless prior notification to General Manager is made.
   - Executing any form of network monitoring which will intercept data not intended for the intercepting employee, unless the activity is a part of the employee's normal job/duty.
   - Circumventing user authentication or security of any computer, network or account.
   - Interfering with or denying service to any user other than the employee's computer (for example, denial of service attack).
   - Using any program/script/command, or sending messages of any kind with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
   - Providing information about, or lists of, DCEC employees or members to parties outside DCEC without prior approval of the General Manager.

- Viewing, storing, disseminating, or printing pornography.

2. Email and Communications Activities
   The e-mail system is the property of DCEC and as such shall not be misused in any of the following manner:
   - Sending unsolicited email messages, including the sending of "junk e-mail" or other advertising material to individuals who did not specifically request such material (e-mail spam), unless part of a corporate approved targeted marketing campaign.
   - Any form of harassment via email, telephone, or paging, whether through language, frequency, or size of messages
   - Send or forward e-mails including any of the following: disruptive or offensive messages, still images, audio, or video images, including but not limited to offensive comments about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. If you receive an email of this nature, promptly notify your immediate supervisor or manager.
   - Forge or attempt to forge e-mail messages.
   - Disguise or attempt to disguise your identity when sending e-mail.
   - Send e-mail messages using another person's e-mail account unless authorized to do so.
   - Copy a message or attachment belonging to another user without permission of the originator.
   - Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
   - Posting the same or similar non-business-related messages to large numbers of Usenet Newsgroups, or message boards.

3. Internet Access Activities
   The following uses of the Internet, either during working hours or personal time, using DCEC equipment or facilities, are strictly prohibited:
   - Access, retrieve, or print text and graphics information, which exceeds the bounds of generally accepted standards of good taste and ethics.
   - Access, retrieve, store, disseminate, or print pornography.
   - The Internet may not be used to access other systems for which the user has no authorization.
   - The Internet or Internet connections shall not be used to access or transfer information that is in violation of Local, State, Federal, or copyright laws, or that contradicts the intent or spirit of these policies and procedures.
   - Engage in personal commercial activities on the Internet, including offering services or merchandise for sale.
   - Engage in any activity which would compromise the security of any DCEC computer or system.
   - Endorse any product or services, participate in any lobbying activity, or engage in any active political activity. The prohibition against engaging in any political activity or fundraising activity does not apply to employees who engage in such activities during the performance of their job responsibilities.
   - Employees and contractors working for DCEC are prohibited from initiating non-work-related Internet sessions using DCEC information resources from remote locations. That is,

employees shall not connect into DCEC resources from home or other non-DCEC locations for the purpose of participating in non-job-related Internet activities.

- Employees and contractors working for DCEC shall not engage in the transmittal of DCEC information or data for non-business purposes and/or personal gain or benefit.

G. Compliance

1. Compliance Measurement
   The General Manager will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits.
2. Exceptions
   Any exception to the policy must be approved by the General Manager in advance.
3. Non-Compliance
   An employee found to have violated this policy may be subject to disciplinary action in accordance with the Cooperative's employee relations policies.

H. Related Standards, Policies, and Processes (cross references to industry standards)

Adapted from the work of the Kentucky Association of Electric Cooperatives (KAEC) Information Technology Association, which was likewise derived from

- "Acceptable Use Policy"@ http://www.sans.org/security-resources/policies/general/doc/acceptable-use-policy
- "Malware Defenses" @ http://www.sans.org/critical-security-controls/control/5

I. Definition of Terms

- **Chain Letter –** Chain letter (email) is a term used to describe emails that encourage you to forward them onto someone else
- **Malware** – a general term used to refer to a variety of forms of hostile or intrusive software such as; computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs
- **Ponzi –** A Ponzi scheme is a fraudulent investment operation that involves paying returns to investors out of the money raised from subsequent investors
- **Pyramid Scheme –** A fraudulent scheme in which people are recruited to make payments to the person who recruits them while expecting payments from the persons they recruit
- **Simple Network Management Protocol (SNMP)** - is a popular protocol for network management. It is used for collecting information from, and configuring, network devices, such as servers, printers, hubs, switches, and routers on an Internet Protocol (IP) network.
- **Single Sign On** - a session/user authentication process that permits a user to enter one name and password in order to access multiple applications.

- **Spam** – Unauthorized and/or unsolicited electronic mass mailings
- **Spyware** – malware that aids in gathering information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge
- **Virus** – a computer program or piece of code that is installed on, or executed by any computer without the knowledge of the owner and runs against the owner's wishes. Viruses are often destructive and malicious.

RESPONSIBILITY: General Manager

DELAWARE COUNTY ELECTRIC COOPERATIVE, INC.

Approved by the Board of Directors	May 26, 2015
Revised by the Board of Directors	Jun 27, 2017

Appendix A: DCEC Backup Schedule by System

System	Responsible Party	Schedule
iVUE ABS CIS OMS Admin Cash Register	NISC Technical Services	Nightly Backup to an offsite location.
GIS Database	ISD Contractor – configures backup executable DCEC Admin Assistant – Changes Tape Daily DCEC Finance Manager – takes tape to bank safe deposit box weekly	Nightly Backup to Windows Server and indirectly to on-site removable media. Weekly transfer of backup tape to off-site safety deposit box.
Windows Server	ISD Contractor – configures backup executable DCEC Admin Assistant – Changes Tape Daily DCEC Finance Manager – takes tape to bank safe deposit box weekly	Nightly Backup to on-site removable media. Weekly transfer of backup tape to off-site safety deposit box.
SCADA (Survalent) Server	ISD Contractor – configures backup executable	Nightly Backup to Windows Server, which is then backed up as described above.
NISC Call Capture Interactive Voice Response (IVR) Server	NISC Technical Services	No regular backup. All member-specific data is written directly to the CIS database and backed up. The IVR software itself could be recreated from images managed by NISC.

Individual workstations, portable computers, and hand-held devices are not backed up. Only those files stored on DCEC's central servers are backed up in accordance with this schedule.