Policy:	10.1	**Type:**	Staff
Title:	Information Technology Assets, Information Security and Systems		
Responsible:	Information Technology		
Approved By:	Chief Executive Officer		
Effective Date:	03/02/2018	**Amendment Date:**	

Policy

NRECA's Information Technology policies are in place to protect you and NRECA by safeguarding the confidentiality, integrity and availability of information. All NRECA employees have a responsibility to protect NRECA assets, information and systems, including members' data. This policy explains how users are accountable for protecting against theft or damage and reducing any potential user account or data breaches. Violation of this policy may result in corrective action, up to and including termination. NRECA employees will be collectively referred to as "Users".

Guidelines

The policy covers expectations, acceptable use and responsibilities regarding five areas:

1. User Responsibilities
2. NRECA Assets
3. NRECA Information and Data
4. NRECA Systems
5. Software

User Responsibilities

1. Users have no expectation of privacy with respect to their use of NRECA's assets or systems. NRECA can record, monitor, and disclose Users' access and use of NRECA's computer systems, including personal use, at any time to ensure that such access and use is consistent with this policy as well as state and federal law.
2. Users may use NRECA's assets and internet for the purpose of supporting business activities necessary to carry out their job functions, such as job-related communications and research. Users are expected to adhere to this policy and exercise good judgment by limiting their use of NRECA's assets and internet outside of job-related purposes. If there is a question or concern, Users should contact their supervisor.
3. Users must complete Security Awareness Training annually and comply with the policies and procedures as described in the Security Awareness Training: http://securitycbt.nreca.org/Welcome.aspx.
4. Information security events which include any real or potential loss or compromise of any data, lost or stolen NRECA assets, any attempted or successful unauthorized access, use, disclosure, modification, or destruction of NRECA data or interference with the operations of any NRECA Information System must immediately be reported directly to management, Information Security or by emailing securityevent@nreca.coop.
5. Users are responsible for all activity performed with their User credentials and on their assets, both on and off the NRECA network. User must immediately notify NRECA Information Security or the IT Help Desk if they suspect a security event or lose possession of any computing equipment or electronic media containing NRECA data so that NRECA, at its sole discretion, can take reasonable measures to safeguard NRECA data, including wiping the electronic contents of any computing equipment or electronic media storing NRECA data.

6. Do not use NRECA assets to send communications that are in violation of state or federal law or NRECA policy, including but not limited to, the transmission of defamatory, obscene, offensive, discriminatory, criminal, harassing messages, or the transmission of messages that disclose personal information about others without authorization.
7. Unacceptable and prohibited uses of NRECA assets, information and systems include:
    - Browsing sites or accessing data which are illegal, pornographic, or which negatively depicts race, sex or creed.
    - Perpetrating any form of fraud, hacking or piracy.
    - Sending or posting discriminatory, harassing, or threatening messages or images on the Internet or by email. It is a violation of NRECA's policy to discriminate in the provision of employment opportunities, training, wages, benefits or privileges, to create discriminatory work conditions, or to use discriminatory evaluative standards in employment if the basis of the discriminatory treatment is, in whole or in part, the person's race, color, national origin, age, religion, disability status, gender, sexual orientation, gender identity, genetic information, veteran status, or marital status or any other characteristic protected by law. Harassment on the basis of any protected classification also is prohibited.
    - Sharing confidential NRECA material, trade secrets, or proprietary information outside of the organization.
    - Downloading or installing software onto an NRECA computer without first receiving approval from the NRECA Help Desk.
    - Allowing anyone other than yourself to use any of your security credentials for NRECA systems, computers, tablets or mobile telephones.
8. Limit personal telephone calls to a minimum. NRECA recognizes that employees occasionally have personal business that must be conducted during working hours; however, personal calls must not interfere with NRECA business or the User's job performance. No personal long distance calls should be charged to NRECA.

NRECA Assets

1. Users are expected to safeguard and physically secure their NRECA assets, including but not limited to computers, tablets, phones, USB devices, electronic media, etc. Laptop computers should be secured with a cable lock during office hours and stored securely in a locked office, desk, cabinet or office during non-office hours.
2. Damaging, altering or disrupting the operation of NRECA assets is prohibited.
3. Modifying or disabling any security settings on your NRECA computer is prohibited.
4. Only NRECA approved and managed computing equipment is authorized to connect and/or synchronize with NRECA information systems.
5. For each issued NRECA computer, the User is responsible for connecting it to the internet during his or her normal work day Monday thru Friday to ensure the computer receives the latest security patches. Computers that have not connected for 17 days will be quarantined until they can be fully secured.

NRECA Information and Data

1. Users must take all reasonable steps to recognize and protect NRECA information consistent with its Information Classification regardless of the information system, equipment or electronic media that is used to access or store such information ***(Information Classification guidelines can be found in Policy 10.2 Appendix A)***. Users may not make copies of data for personal use or give copies of data to unauthorized persons or parties who do not have a business reason for knowing such information.
2. Users should use their U: drive to backup and store their data. The cloud-based storage option OneDrive is also available to Users for *Public*, *Internal*, and *Confidential* data. However, OneDrive is not appropriate for *Protected* data such as SSNs, *Financial* or *Protected Health Information*. Folders on file shares, such as the R: and V: drives, and SharePoint sites are available for project, team and work unit needs. If you need to store *Protected* data on the network, please contact Information Security to set up or grant access for those locations. Do not store *Protected* data on your C: drive. If you have the need to store NRECA *Internal, Confidential* or *Protected* data in another location, please contact Information Security for guidance.
3. *Protected* and *Confidential* data must be secured with additional safeguards.
    a. Access to *Protected* and *Confidential* data requires strong passwords in accordance with Information Security password standards.
    b. Users are prohibited from putting *Protected* or *Confidential* data on any removable storage devices such as USB drives, memory sticks, disks, CDs, DVDs, cassettes, etc. All data copied to removable storage devices (such as USB drives) must be encrypted and password protected. Users can contact the NRECA Help Desk for options to secure and/or transport data.
    c. Any NRECA *Protected* or *Confidential* data stored outside an NRECA facility must be:
        i. Encrypted in accordance with Information Security encryption standards available from Information Security.
        ii. Stored only on NRECA owned or managed information systems, computing equipment and electronic media.
        iii. The security of any NRECA *Protected* or *Confidential* data stored by third parties on non-NRECA owned or managed information systems, computing equipment and/or electronic media is controlled through formal services contracts or agreements executed by NRECA with such third parties that are approved by Information Security.
    d. The transmission of *Protected* data between NRECA and third parties, including cooperatives, must be controlled and be compliant with applicable NRECA policy, including any relevant legal restrictions or regulations, to prevent loss, modification or misuse as follows:
        i. *Protected* data must be encrypted before being electronically transmitted in accordance with Information Security Encryption Standards that are available from Information Security.
        ii. Users transmitting *Protected* data by email must take reasonable measures to limit the amount of *Protected* data contained in emails to the minimum necessary and to identify such data by using the appropriate encryption keys below so that the information can be encrypted during transmission.

#PHI#	HIPAA protected health information (PHI)
#NPI#	Non-Public personally identifiable information (401(k) pension plan, RS Plan)
#FAD#	Financial account data (credit card accounts, bank account numbers)
#encryptsend#	For any other protected data that doesn't fit into any of the primary categories above

NRECA Systems

1. Users must safeguard their NRECA passwords by logging off of their computers, and are prohibited from sharing their NRECA passwords with other individuals.
2. Users must not use their NRECA passwords as the password for any other site.
3. NRECA passwords must be 15+ characters and meet complexity requirements (upper case characters, lower case characters, numeric, special character).
4. Unauthorized access to NRECA's information systems is prohibited, as is damaging, altering, or disrupting the operations of these systems in any way.
5. NRECA expects Users to take all necessary steps to ensure that any messages sent, received, or stored on NRECA electronic communication systems that constitute confidential, proprietary or privileged NRECA information are treated in accordance with NRECA and work unit confidential information policies. Users should transmit such confidential information only to those persons with a legitimate business need for access to such information.
6. Third-party access to NRECA's information systems is controlled in order to safeguard NRECA information. All third-party access must be managed through formal contracts or agreements executed by NRECA in order to address the risks, security controls and procedures for information systems, networks and/or computing equipment environments in the contract between the parties based upon the work to be performed.

Software

1. Approval, acquisition and installation of software shall be acquired through the NRECA Help Desk and Strategic Sourcing & Procurement. Software requires Information Security, Help Desk and Business approval to ensure the software is appropriate and safe to run.
2. Software purchases or installations that involve End User License Agreements (EULA), Terms of Use and other contractual forms must first be reviewed by Strategic Sourcing & Procurement (see Policy 9.1).
3. Any purchase that may involve the use, disclosure, or access of Protected or Confidential Data must be coordinated with the Strategic Sourcing & Procurement department to ensure that information security provisions are contained in supplier contracts and agreements. An Information Security review is also required for acquiring the use of any software or hardware that may involve Protected Data (see Policy 9.1).NRECA does not permit any User to use software in any manner inconsistent with the applicable license agreement, including giving or receiving software from clients, contractors, customers and others. Duplication of software and making unauthorized copies of software is prohibited.