Policy:	10.2	**Type:**	Staff
Title:	Information Privacy and Confidentiality		
Responsible:	Office of General Counsel and Information Technology		
Approved By:	Chief Executive Officer		
Effective Date:	04/01/2013	**Amendment Date:**	03/02/2018

Policy

NRECA collects a wide variety of information and holds itself to the highest standards in safeguarding the confidentiality, integrity and availability of such information. The appropriate method of safeguarding depends upon its information classification. Therefore, employees must adhere to the standards and rules set forth in this policy, and department specific policies, for properly using, storing, sharing or disclosing information to ensure compliance with federal or state information privacy and data protection laws.

Introduction and Definitions

Using, storing, sharing and disclosing information is a necessary part of NRECA's routine business operations, however, failure to comply with NRECA's policies can have adverse consequences or violate federal or state information privacy and data protection laws. This policy sets forth employees' obligations for handling different types of information based on business and regulatory requirements and other needs. NRECA employees must understand the classifications of information they are handling to know the appropriate privacy and confidentiality controls to apply. Before responding to any information requests, it's important for employees to determine who has the specific authority to share information internally with other staff of NRECA (including NRECA's subsidiaries and affiliated entities) or to disclose information externally to a third party. Refer to Policy 10.1 Information Technology Assets, Information, Security and Systems for NRECA's policy on how to apply information security requirements when using, storing, sharing or disclosing information.

Using	Any internal activity in support of the business operation of NRECA (including its subsidiaries and affiliated entities).
Sharing	Providing information *internally* to other staff of NRECA (including its subsidiaries and affiliated entities).
Disclosing	Providing information *outside* NRECA to individuals, members or other third parties.
Storing	The method and location in which you keep information either physically or digitally.
Third Party	Individuals, members, or any service providers that have a formal or informal relationship with NRECA (e.g. government, media, contractors, cooperative consumers).
Information	Data, Documents, and Records which are used in operating NRECA's business. • Data – Information in digital form that can be structured or unstructured. • Document – Information formatted for a particular business purpose that can include both digital and paper formats. • Record – All information that must be preserved for a prescribed period due to a business, legal or compliance obligation.

Information Use

NRECA's Information Use Policy – hereby incorporated by reference - describes how employees must use such information collected on its website. All information collected, created or developed internally by NRECA employees shall be used solely for NRECA purposes subject to any additional restrictions identified by each department. Any information received from or owned by a third party shall only be used or disclosed in a manner consistent with any copyright law, license restrictions or non-disclosure obligations contained in any applicable agreement or understanding with such third party.

Information Classifications: Storing, Sharing and Disclosing

Information collected and used by NRECA is given an "information classification" based on regulatory requirements, business requirements, and/or NRECA's responsibility to protect and safeguard the privacy and confidentiality of such information. Appendix A's NRECA Information Classification Matrix defines the information classifications adopted by NRECA. These classifications are a fundamental component of the NRECA information security program because they provide rules for storing, sharing and disclosing information that employees must follow.

Information Type: Sharing and Disclosing

Depending on the type of information, NRECA employees may share information internally, across departments and systems and with NRECA's subsidiaries and affiliated entities as necessary and legally permissible. However, there are situations where sharing or disclosing information should not occur, or should be limited, to avoid adverse consequences for NRECA or its members, and to ensure compliance with applicable federal and state privacy laws. Examples include:

- some information purchased as fee-for-service or on a subscription basis, should only be provided to the purchasers of that information; or
- in other cases, information sharing between NRECA and its subsidiaries and affiliated entities is strictly prohibited as specified in the NRECA Information Use Policy; and
- NRECA employees must never share information obtained from a third party without verifying that there are no contractual or legal restrictions from doing so.

Requests for *Internal Information*, *Confidential Information* or *Protected Information* (as defined in this policy) can only be shared internally or disclosed externally, as applicable, at the discretion of the NRECA department responsible for that information. Employees must handle all internal and external information requests in accordance with the NRECA Information Requests Matrix found in Appendix B. This matrix provides general guidance for the type/source of information requests, information descriptions, the specified department and the process to handle or authorize the sharing or disclosure of the requested information.

If an employee is ever unsure of how to respond to a request for information, the employee should contact his/her manager.

Department or Business Unit Specific Guidelines

Specific departmental or business unit guidelines for sharing, using, storing, disclosing information may be more extensive because of their business activities and applicable regulatory requirements. Employees are expected to be familiar and comply with any specific guidelines or instructions of their department.

Identity Verification for PII and PHI

Before sharing or disclosing personally identifiable information or protected health information or participating employer benefit plan information, employees must follow the procedures in the Identity Verification Policy. Adhering to these procedures will ensure that information is not incorrectly disclosed to an unauthorized person.

Mistaken Use, Sharing or Disclosure of PII and PHI

If an employee mistakenly shares or discloses, or becomes aware that another person has shared or disclosed, information in a manner that does not comply with this policy, the employee must immediately report the event to his/her manager, the Information Security team, or securityevent@nreca.coop Any occurrences of unauthorized or accidental disclosures of either *Protected* or *Confidential Information* must be reported immediately to your manager, the Information Security team, the Privacy Officer or securityevent@nreca.coop.

Clean Desk

Employees must secure all printed *Confidential Information* and *Protected Information* when not in use by placing such information in locked filing cabinets, desk drawers or secured storage rooms. When printed materials are in use, employees must take reasonable steps to ensure that these materials are viewable only by authorized employees. Employees should secure printed information before leaving their desks, and at no time should papers containing *Confidential Information* and *Protected Information* remain unsecured when the authorized employee has left the office premises. Under no circumstances should any papers containing Social Security numbers or HIPAA protected health information be removed from the office premises.

Information Safeguards

Consistent with Policy 1.4 – Record Retention & Destruction, Policy 10.1 – IT Assets, Information, Security and Systems Use, and NRECA's HIPAA Privacy and Security Policies and Procedures Manuals, employees shall use reasonable and prudent technical, administrative, and physical safeguards to maintain information consistent with its classification to protect against loss, unauthorized access, destruction, misuse, modification, and improper disclosure. Employees must ensure that agreements with third parties contain specified security controls appropriate to the information classification prior to disclosing and transmitting information to third parties. Employees shall be responsible for ensuring that Business Associate Agreements are in place prior to disclosing any HIPAA protected health information to third parties.

Employees who are uncertain about the confidential or protected nature of information in their possession should ask their manager for guidance. The Information Security team can assist in identifying the security controls needed to safeguard Information appropriately.

APPENDIX A - NRECA INFORMATION CLASSIFICATION MATRIX

If an appropriate classification is still unclear after considering this policy, please contact your manager for guidance.

Classification	Description	Compliance Categories	Record Type– not exhaustive
Public	Information that is publically available.	Anonymous information Publicly available information	www.electric.coop content Public Tax Filings NRECA Social Media
Internal	Information that is intended for general use within NRECA for which its unauthorized disclosure could adversely affect NRECA, its members or contractual obligations.	Internal Personally Identifiable Information (PII-I) Any other information classified by NRECA Management as “Internal” NRECA Member Information	Employment Data (not SSN, not Salary) Third Party Agreements NRECA Business Presentations Cooperative.com
Confidential*	Information intended strictly for use within designated areas inside NRECA. Information which may not be specifically protected by statute, regulations or other legal obligations but for which unauthorized disclosure or access could cause serious financial loss, reputational harm , privacy violations, or contractual violations.	Confidential Personally Identifiable Information (PII-C) Confidential Employment Information Confidential Demographic Information Confidential Information Security Program Information Intellectual Property Any other information classified by NRECA Management as “Confidential” or “Sensitive”	Patents and trade secrets Name AND salary Name AND date of birth Name AND email address Human Resources and Benefits Information NRECA Budgets and HR Information Political Activity Information Third party content subject to non-disclosure
Protected*	Information subject to regulatory/compliance requirements/contractual commitments or so identified by Management, and which if lost, compromised, or disclosed without authorization, could result in severe financial and/or reputational harm to NRECA, members or others, as well as embarrassment, inconvenience or unfairness to an individual or business.	Protected Personally Identifiable Information (PII-P) Protected Health Information (PHI) Nonpublic Personal Information (NPI) Personally Identifiable Financial Information (PIFI) Financial Account Data (CHD & ACH) Payment Card Information (PCI-DSS) Critical Energy/Electric Infrastructure Information (CEII) Protected Information Security Program Information Authentication Credentials Any other information classified by NRECA Management as “Protected” or “Restricted”	An individual’s first name or first initial and last name plus one or more of the following data elements Full SSN, Driver’s license, state issued ID card number. 401(k) or RS Account Balance Information Credit Card Data (Number, expiration date, security code) Tax ID Number Account Number

*Information security protocols must be followed as outlined in Policy 10.1 – Information Technology Assets, Information and Systems Use

APPENDIX A - NRECA INFORMATION CLASSIFICATION MATRIX

INFORMATION CATEGORY DEFINITIONS

Public Information

Information which is available to the general public with or without restriction.

Anonymous Information	Non-personal data that has no connection to an individual and itself, it has no inherent link to an individual.
Publicly Available Information	Any data that is either lawfully made available to the general public from federal, state or local government records or NRECA has determined to make widely available such as on its website.

Internal Information

Information that must be safeguarded and used only by employees who have a legitimate business purpose.

Employment-related Personally Identifiable Information (PII-I)	Any information that identifies an individual's employment (e.g. name, business title, employee number, work address, work phone number, work e-mail address, etc.) which is not Publicly Available Information but available for business purposes only.
NRECA Internal Information	Any information that is restricted to a select group of employees with a legitimate need to know, which may not be labeled "internal".
NRECA Member-Only Information	Information available to all members of NRECA and can be found on cooperative.com.

Confidential Information

Information that must be safeguarded with additional precautions and used only by employees who have a legitimate business purpose.

Confidential Personally Identifiable Information (PII-C)	Any non-employment related information that identifies an individual (e.g. name, address, phone number, e-mail address, date of birth, etc.) which is not Publicly Available Information.
Confidential Employment Information	Any information that identifies an individual and includes confidential employment data (e.g. compensation, employment dates, information concerning quality of work, union status, etc.) which is not Publicly Available Information.
Confidential Demographic Information	Any information that identifies an individual and includes confidential demographic data (e.g. race, citizenship, immigration status, national origin, sexual orientation, lifestyle information, disability, etc.) which is not Publicly Available Information.
Confidential Business Information	Any information that identifies confidential aspects of the information security programs (e.g. Risk, Threat and/or Vulnerability assessments, security events and incidents, etc.) which is not Publicly Available Information.
Intellectual Property (IP)	Creations of the mind for which exclusive legal rights are recognized and NRECA wishes to assert including copyrights, patents and trademarks.

Protected Information

Information that must be safeguarded in a particular manner outlined by NRECA and accessed by employees who have been identified as individuals who have a need to access such information for a specified purpose.

Protected Personally Identifiable Information (PII-P)	Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linkable to a specific individual which could be sufficient to perform identity theft or fraud against the person whose information was compromised.[1]
Protected Health Information (PHI)*	Individually identifiable health information created or received by a covered entity (a health care plan, health care provider, or health care clearinghouse), in any form or media, whether electronic, paper, or oral. Information about an individual's past, present or future physical or mental health or condition. [2]
Nonpublic Personal Information (NPI)	Personally Identifiable Financial Information (PIFI); and ii) any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any nonpublic personal information.[3]
Personally Identifiable Financial Information (PIFI)	Any information a consumer provides to you to obtain a financial products or services about a consumer resulting from any transaction involving a financial product or service between you and a consumer; or obtained about a consumer in connection with providing a financial product or service to that consumer.[4]
Financial Account Data (FAD) **	Any information that includes reference to financial account numbers (e.g., bank accounts, credit card accounts, etc.) for individuals or organizations. Cardholder data (CHD) and Automated Clearing House (ACH) data[5] are types of FAD.[6] The Primary Account Number (PAN) in the defining factor in this classification. Regulatory requirements apply if a PAN is stored, processed, or transmitted.
Authentication Credentials	An object that is verified when presented to the verifier in an authentication transaction. Credentials may be bound in some way to the individual to whom they were issued, or they may be bearer credentials. The former are necessary for identification, while the latter may be acceptable for some forms of authorization
Critical Energy/Electric Infrastructure Information (CEII)	CEII is defined as specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure that relates details about the production, generation, transportation, transmission, or distribution of energy; could be useful to a person in planning an attack on critical infrastructure; is exempt from mandatory disclosure under the Freedom of Information Act, 5 U.S.C. 552 (2000); and does not simply give the general location of the critical infrastructure.

*PHI uses and disclosures are subject to very specific requirements under the HIPAA privacy rule. For example, PHI disclosures may require either an individual's authorization or execution of a HIPAA Business Associates Agreement. If you have questions while working with PHI, please consult the HIPAA Privacy and Security Policies Manuals or contact NRECA's privacy officer.

**Consult with the Senior Vice President of Finance if working with FAD and have questions.

[1] OMB M-10-23 Appendix Definition
[2] HIPAA
[3] 17 CFR 248.3
[4] 17 CFR 248.3
[5] Define by the Electronic Payments Association (NACHA)
[6] Defined by Payment Card Industry (PCI) Security Standards Council Data Security Standard (DSS)

APPENDIX B - NRECA INFORMATION REQUESTS MATRIX

Proper handling of Information requests depends on what TYPE of information is being requested not necessarily WHO is making the request. Departmental procedures may reference Appendix B regarding the process below and/or provide additional details related to the specific type of requests their department receives.

Type/Source of Information Request	Record Type	Department or Division to Handle Request	Guidance
Legal & Operational Issues Involving NRECA Members	Subpoenas, administrative, judicial or adversary information requests; inquiries about litigation, investigations or disputes that involve the following: an NRECA member system; or NRECA members' operational or governance practices (e.g., capital credits, board elections, bylaws, line extension policies, service disconnections, billing and collection practices, etc.).	Office of General Counsel	The Office of General Counsel will either handle the request directly or provide legal advice and guidance to NRECA staff regarding any *unusual or sensitive requests* for Information and requests for NRECA assistance regarding a NRECA member's practices.
Legal & Operational Issues Involving NRECA & NRECA Owned and Affiliated Entities	Subpoenas; judicial, administrative or adversary information requests; inquiries from any source (including the public, government agencies, member cooperatives, or individuals) regarding litigation, investigations or disputes involving NRECA or an NRECA owned or affiliated entity (including, but not limited to the Group Benefits Program, the 401(k) Pension Plan, the Retirement Security Plan, NRECA International Foundation, NRECA International Limited, NRECA Electricity for Progress LLC, Foundation Energetica Boliviana, Cooperative Benefits Administrators, CES, CIS, ELCO, NRECA United Inc., Wood Quality Control, Touchstone Energy Cooperative and ACRE).	Office of General Counsel	The Office of General Counsel will either handle the request directly or provide legal advice and guidance to NRECA staff regarding any *unusual or sensitive requests* for Information and requests for NRECA assistance regarding NRECA and NRECA owned and affiliated entities listed in the description.

INFORMATION REQUEST MATRIX (Appendix B)

Type/Source of Information Request	Record Type	Department or Division to Handle Request	Guidance
Legal & Operational Issues Involving Homestead Funds, Inc., RE Advisers Corporation and RE Investment Corporation	Subpoenas; judicial, administrative or adversary information requests; inquiries from any source (including the public, government agencies, member cooperatives, or individuals) regarding litigation, investigations or disputes for Homestead Funds, Inc., RE Investment Corporation, and RE Advisers Corporation.	Office of General Counsel, Securities Compliance	The Office of General Counsel, – Securities Compliance will either handle the request directly or provide legal advice and guidance to NRECA staff regarding any *unusual or sensitive requests* for Information and requests for NRECA assistance regarding Homestead Funds, Inc., RE Advisers Corporation and RE Investment Corporation.
Media Inquiries	Request by representative of the media for information, a statement or quote from an NRECA spokesperson, etc.	Media & Public Relations Division within NRECA's Communications Department	Refer to Policy 7.1 – External Communications. Media & Public Relations shall consult with relevant Association staff in responding to inquiries from the media. The Office of General Counsel may be consulted related to legal and operational issues involving NRECA members and for requests about NRECA or its owned & affiliated entities. Government Relations may be consulted regarding regulatory, legislative and policy matters.
Financial or Tax Related Inquiries Regarding NRECA & NRECA Owned and Affiliated Entities	Requests for any NRECA or NRECA owned or affiliated entity's filings with the Internal Revenue Service or with state or local taxing authorities; financial statements; audit reports; or other financial or tax related records.	Finance Department	The Office of General Counsel shall be notified of any such request.
NRECA Membership Status, Eligibility Criteria or Requirements	Requests from an electric cooperative or other electric service provider, industry vendor, or other organization regarding membership eligibility criteria or requirements. Requests regarding the membership status of an NRECA current, former or prospective member.	Membership	Membership Department staff shall consult with the Office of General Counsel regarding eligibility for participation in NRECA-sponsored employee benefit plans. If a membership-related request is coming from the media, a public official or consumer-member, Membership Department staff shall consult with the Office of General Counsel before responding.

Type/Source of Information Request	Record Type	Department or Division to Handle Request	Guidance
Conference and Training Materials and Participation Records	Educational transcripts or attendance records for Benefits-Related Conferences and Training Educational transcripts or attendance records for Non-Benefits-Related Director and Staff Conferences & Training (e.g. Credentialed Cooperative Director, Board Leadership Certificate, etc.)	Insurance & Financial Services Education & Training	Generally, NRECA educational conferences and training materials are intended for NRECA members only, with certain exceptions. Disclosure of conference and training materials and participant records are within the discretion of the relevant business unit sponsoring the conference or training. Generally, only the attendee or participant, the manager/CEO of his or her cooperative, and the training coordinator for his or her cooperative or statewide organization, is entitled to attendance or participation records or confirmation of director training towards a credential or certificate. Other authorized recipients may include state continuing education credit authorities provided that the request for this information is made by the attendee or participant. To the extent that NRECA published a list of attendees or participants as part of conference or training materials, then such list may be provided to anyone who attended that conference or training or who purchases the past conference or training materials, provided that such materials are still readily available. To the extent that NRECA published a list of recipients of a credential or certificate in a meeting brochure or program, then NRECA staff may provide such brochure or program to any NRECA member, provided that such information is still readily available.
NRECA 401(k) Pension Plan, Retirement Security Plan or Group Benefits Program Inquiries and Requests for Records	Records relating to the NRECA 401(k) Pension Plan, Retirement Security Plan or Group Benefits Program participation.	Office of General Counsel or Insurance and Financial Services Department	The Office of General Counsel shall be notified of any such request. Information requests related to the Group Benefits Program are to also follow guidelines from NRECA's HIPAA Privacy and Security Policies and Procedures Manuals.

INFORMATION REQUEST MATRIX (Appendix B)

Type/Source of Information Request	Record Type	Department or Division to Handle Request	Guidance
NRECA Personnel Records	Employment information for any current or former NRECA employee or applicant for employment.	Human Resources Department	See Policy 6.3 – Release of Employee Information.
	Finance, payroll & accounts payable records related to NRECA employee salary and expense payments.	Finance Department	Finance Department staff may disclose this information as required to federal and state tax agencies, the Social Security Administration, employee benefit providers and for workers' compensation, unemployment insurance and similar purposes.
Government Relations Records	Records related to the administration of and participation in the Youth Tour, Legislative Conferences, NRECA Standing Committees, political action committees (ACRE and Co-op Owners for Political Action), lobbying, and related activities.	Government Relations Department	While certain Government Relations activities are subject to public filing and disclosure requirements, other information may be disclosed only to participants in the activities. In addition, the Government Relations Department maintains the www.ourenergy.coop web site, which is subject to its own privacy policy.
NRECA Web Sites, Databases, Computer Logs & Related Information	Databases, web sites, computer logs (e.g., web logs that track activity on NRECA web sites and the web sites of NRECA owned and affiliated entities), system logs, server logs, and security logs.	Information Technology Department	Information on a web site may be subject to specific web site privacy and security policies as well as terms of use. Web logs are subject to the privacy policy provisions of the particular web site. Other types of logs are generally considered confidential NRECA information and not shared with anyone outside NRECA except authorized NRECA consultants, contractors or business associates. Any requests for NRECA computer logs and related information shall be handled on a case-by-case basis through consultation with the Office of General Counsel depending on the source of the request.
Disputes or Complaints	Disputes arise in numerous situations, such as between NRECA Members, between an individual consumer and his or her cooperative, an individual and NRECA, or NRECA or an NRECA owned or affiliated entity and a government entity:	Office of General Counsel	In the event NRECA staff receives any indication that an Information request related to a dispute or complaint or requests for assistance, should be referred immediately. Also see Policy 1.6 – Whistleblower Protection.

Type/Source of Information Request	Record Type	Department or Division to Handle Request	Guidance
	NRECA Member System Employee or Board Member request for NRECA assistance regarding: (1) a dispute or other complaint involving an NRECA member system or that system's management or board or (2) allegations of wrongdoing by another employee or board member.	Office of General Counsel	Office of General Counsel
	A consumer-owner of an NRECA Member request for Information regarding cooperative practices or seeking NRECA's assistance in resolving some disputed matter with his or her cooperative.		Office of General Counsel
	NRECA Member System Employee or Board Member request regarding a dispute or complaint related to the Group Benefit Plans, 401(k) Pension, or Retirement Security Plan.		Office of General Counsel
	NRECA Member System Employee or Board Member request regarding a dispute or complaint related to the Homestead Funds, Inc., RE Advisers Corporation or RE Investment Corporation.		Office of General Counsel, Management Advisory Services – Securities Compliance
Student or Researcher Request	Information about NRECA, its Member Systems, or its policy positions.	Depends upon the subject matter of the request.	Refer to the appropriate department, division or unit with responsibility for the type of Information as outlined in this Appendix.
Government Official Request (including any court or administrative tribunal, legislative body, or regulatory agency)	Information related to a particular NRECA Member or NRECA Members or cooperatives generally.	Office of General Counsel	Any Information request that originates from a government official shall be referred immediately to the Office of General Counsel.
	Information related to NRECA or any NRECA owned or affiliated entity or to the NRECA 401(k) Pension, Retirement Security Plan or Group Benefits Plans.		

Type/Source of Information Request	Record Type	Department or Division to Handle Request	Guidance
NRECA Statistical /Research Information	Requests for statistics and related analyses regarding electric cooperatives created by Strategic Analysis that is not public (that is, not posted on www.electric.coop).	Strategic Analysis Department	Such non-public data is typically considered proprietary, and may be collected with certain promises of confidentiality or anonymity made to the respondents. Therefore, disclosure may be limited to NRECA members, survey participants, or subscribers.
	Other statistical or research data created or compiled by other groups within NRECA, such as the National Consulting Group (e.g. national compensation survey, directors survey, etc.), the Cooperative Research Network, and NRECA Market Research.	Creator of the data, e.g., NCG, CRN, NRECA Market Research, etc.	The owner of the data will determine whether the request for information will be fulfilled.