

CAPE HATTERAS ELECTRIC
COOPERATIVE BOARD POLICY NO. 113

**SECURITY OF PERSONAL
INFORMATION**

I. OBJECTIVES:

To provide for the security and safeguarding of personal records and identifying information maintained in company records and/or contained in company communications, as well as compliance with applicable state and federal law.

II. POLICY:

- A. Cape Hatteras Electric Cooperative (CHEC) will endeavor to safeguard and protect the privacy of its employees and other individuals whose personal information has been obtained and maintained by the company in the performance of its obligations and operations. Personal information is defined as a person's name (or any part of a person's name), in combination with any identifying information, including social security number, employer identification number, driver's license, passport, or state identification number, checking or savings account number, credit or debit card number, personal identification number ("PIN"), or any other number or information that can be used to access a person's financial resources.
- B. The primary objective of this policy is the protection of such personal information from misappropriation, misuse, and inappropriate or inadvertent disclosure.
- C. Unless compelled by legal process, CHEC will not communicate or otherwise disclose employee social security numbers to the general public. Moreover, the Cooperative will not require the use of social security numbers for any individual to access its services or facilities. Use of social security numbers will not be communicated via unprotected electric communication, and shall be limited to legitimate payroll or employee benefit purposes. Even such legitimate use shall be limited to the extent feasible, and the CHEC will demand of its vendors and outside consultants that its transactions with the Cooperative, to the extent possible, not require the use or disclosure of social security numbers.
- D. CHEC will ensure that during the disposal of personal information that such information is not inadvertently disclosed to the general public or stolen.

In the process or disposing of paper records, CHEC will take all necessary precautions to destroy records containing personal information, including, but not limited to, the burning, pulverizing, or shredding of said records so that information cannot be practicably read or reconstructed.

In the process of disposal of electronic records, CHEC will take all necessary precautions to assure that personal information is properly deleted or destroyed

In the process of disposal of electronic media and equipment, CHEC will take all necessary precautions to assure that personal information is not inadvertently disclosed in the discarding, donating or selling of used computer equipment. E. In the event that personal information is compromised, whether through theft, loss, or otherwise, CHEC shall report such breach of security to anyone who's personal information may have been compromised, as soon as feasible. Such notice- will include:

- A description of the incident in general terms;
- A description of the type of personal information that was subject to the unauthorized access and acquisition;
- A description of the general acts of the business to protect the personal information from further unauthorized access;
- A telephone number for the business that the person may call for further information and assistance, if one exists;
- The toll-free numbers and addresses for the major consumer reporting agencies;
- The toll-free numbers, addresses, and Web site addresses for the Federal Trade Commission and the North Carolina Attorney General's Office, along with a statement that an individual can obtain information from these sources about preventing identity theft.

F. In the event CHEC provides notice to an affected person pursuant, CHEC shall notify without unreasonable delay the Consumer Protection Division of the Attorney General's Office of the nature of the breach, the number of consumers affected by the breach, steps taken to investigate the breach, steps taken to prevent a similar breach in the future, and information regarding the timing, distribution, and content of the notice.

G. CHEC will assign an individual employee to manage compliance with this policy. Such person shall be responsible for training those employees whose jobs require access to personal information on the proper methods for safeguarding such information, the importance of doing so, and the content of this policy and written guidelines.

III. RESPONSIBILITY

The Executive Vice President and General Manager shall be responsible for the administration of this policy and in addition, shall be responsible for making recommendations to the Board of Directors for any needed revisions or additions.

Approved by Board of Directors:
October 18, 2007

Policy No. 113
Effective Date October 18, 2007

Reviewed and Approved: May 21, 2015

Norm Campbell, Secretary