East Coast Satellite Communications CPNI Compliance Policy

Fiscal Year 2017

CPNI Security Measures

East Coast Satellite Communications does not allow on-line access to customer accounts. Therefore customers are not issued logins to access CPNI.

East Coast Satellite Communications employees do not release CPNI information over the phone unless the customer can be clearly identified with a PIN or password. It the customer cannot provide a password or a PIN, information can only be mailed to the address on record or by the company calling the customer with the phone number on record.

If the customer is able to provide call detail information without East Coast Satellite Communications employee assistance, then the East Coast Satellite Communications employee is permitted to discuss call detail information with the customer.

East Coast Satellite Communications does not have retail location and does not give out CPNI information at it place of business.

East Coast Satellite Communications password protects access to internal record files and folders which contain CPNI.

Employee Training Policies

East Coast Satellite Communications has instituted a program to oversee and supervise employees with access to CPNI.

East Coast Satellite Communications employees will be reprimanded, suspended or terminated an employee for failing to follow CPNI procedures.

Use of CPNI in Marketing Campaigns

East Coast Satellite Communications does not participate in third party marketing campaigns.

Advertising does not include CPNI.

East Coast Satellite Communications does not provide on-line access to CPNI information, this notifying customers of their right to restrict access, the opt-in clause, opt out-clause and records for customer approval are not applicable.

Third party use of CPNI

East Coast Satellite Communications does not allow third party access to CPNI information

Unauthorized access to CPNI

East Coast Satellite Communications is committed to protecting all client information, including CPNI information. Any breach in access to information will be reported to the proper law enforcement authorities.

All records around the breach will be kept for a minimum of two years.