

**Clean Energy Alliance
Administrative Policy**

SUBJECT:		EFFECTIVE DATE:	
Protection of Confidential Information		February 20, 2020	
POLICY #:	SUPERSEDES	STAFF CONTACT	# OF PAGES:
CEA-02	N/A		3

1.0 Purpose

To establish a policy to protect confidential customer information

2.0 Organizations affected

Clean Energy Alliance
All Clean Energy Alliance Member Agencies

3.0 References

Privacy & Customer Confidentiality Policy #CEA-03

4.0 Definitions

4.1 Confidential Information

Customer information that is not considered public information including but not limited to social security number, taxpayer ID number, San Diego Gas & Electric (SDGE) or Clean Energy Alliance (CEA) customer or service account information including customer name(s), service addresses, billing addresses, telephone numbers, email addresses, account numbers and electricity consumption.

5.0 Policy

5.1 Ensuring Customer Confidentiality is Protected

To ensure that all employees protect the integrity of the CEA's confidential information as well as the confidentiality of others, confidential information may not be shared with unauthorized individuals within or outside of the organization and may not be transmitted via email, except where reasonably necessary to conduct CEA's business or provide services to customers as required by the California Public Utilities Commission (CPUC).

5.2 Examples of reasonably necessary business purposes include but are not limited to when such disclosure is necessary to:

- a) Comply with law, regulation, or court order;
- b) Enable CEA to provide services to its customers;
- c) Collect unpaid bills;

- d) Obtain and provide credit reporting information;
- e) Resolve customer disputes or inquiries;
- f) Communicate about demand response, energy efficiency, energy management and conservation programs; or
In situation of imminent threat to life or property.

6.0 Procedure

- 6.1 Confidential information shall not be transmitted or forwarded to individuals within or outside of the organization who do not have an authorized need to know the information.
- 6.2 Confidential information shall not be transmitted via email.
- 6.3 Confidential information shall not be posted on the CEA's website.
- 6.4 Employees must lock their computers when leaving them unattended for any length of time.
- 6.5 Passwords may not be shared with any person, including administrative assistants, secretaries, managers, co-workers, or family members, and shall not be written down or stored physically or digitally.
- 6.6 Documents containing confidential information must be secured at all times.
- 6.7 Documents containing confidential information must be shredded when destroyed when no longer used and as per the adopted retention schedule if applicable, except where such documents are required to be retained by law.
- 6.8 Employees are responsible for any action that is performed under their username and password for any CEA system, network or server.
- 6.9 Failure to comply with the provisions of this policy and procedure may result in discipline up to and including termination.

Barbara Boswell
Barbara Boswell
Interim Chief Executive Officer

2/23/20
Date

PROTECTION OF CONFIDENTIAL INFORMATION POLICY ACKNOWLEDGEMENT

I have read the Protection of Confidential Information Policy and understand its provisions. I understand that to ensure protection of the integrity of the CEA's confidential information as well as the confidentiality of others, confidential information may not be shared with unauthorized individuals within or outside of the organization and may not be transmitted via email.

I accept responsibility for any action performed under my user name and password.

I understand that handling and use of confidential information in violation of the Protection of Confidential Information Policy may result in employee discipline, up to and including termination.

By signing this form, I agree to abide by the Policies currently in place and I agree to review periodically any changes or modifications. I understand that my regular review of policies is required.

Employee Name (Print): _____

Employee Signature: _____ Date: _____

Department Head
Signature: _____ Date: _____

(To be filed with Human Resources)