Customer Information Policy Training
for external providers

The following training outlines the rules and guidelines contained within the Use of Customer Information Policy. WEC Energy Group (the company) takes protection of customer information very seriously and expects those who do work on the company's behalf to protect the information in the same manner as employees. This training defines customer information and the steps required to protect it. This training also provides guidance in the appropriate use of customer information systems.

Objectives

- Define and recognize various types of customer information.
- Understand how to use customer information appropriately.
- Learn safeguards to prevent misuse of customer information.
- Recognize policy violations related to misuse of customer information and the potential consequences of violations.

Introduction to customer information

Customer service and corporate reputation are built on trust and integrity. Doing what is right for customers – ethically, fairly and honestly – is key to the company's success. As an individual performing work on behalf of the company, understanding what customer information is and the importance of protecting it is necessary. The decisions made when using customer information are essential to ensure compliance with the guidelines established in the Use of Customer Information Policy.

Customer Information Policy Training
external providers

What is customer information?

Customer information is data or facts known about a person or organization that receives energy service or products from the company.

Customer information resides in various systems used throughout the company. The information may also exist in paper form or electronically . This information, whether paper, stored within a system or viewable on the internet, is confidential and should be used solely for business purposes and not viewed or shared with others for any nonbusiness-related reason.

Examples

- Name, address, city, state, ZIP code, phone number and email address.
- Social Security number.
- Employment information.
- Other examples:
  - Billing or payment information.
  - Credit or medical information.
  - Interactions with customers on the phone or in the field.
  - Printed or electronic material or systems.
  - Customer contact information.

Typical sources of customer information

- Various customer information systems.
- Electronic or paper work or service orders.
- Sketches, reports, work orders, forms, etc.
- Crew location information.
- Flash drives, CDs or other data storage device containing mapping information or construction standards.
- Conversations or interactions with customers occurring in person, on the phone or through other channels, including social media sites.

Guidelines to protect customer information

The company strives to deliver excellent customer service, and customer information helps achieve that goal.

Customer information:

- Must be protected as restricted and confidential.
- Is a valuable asset; it is not to be traded or sold.

- Should be kept confidential and secure, whether paper or electronic.
- Should be used solely for business purposes and not viewed or shared with others for any other reason. Do not forward confidential information to those not authorized to have it.
- Should be safely stored and properly handled in the office or in a vehicle.
- Should be placed in confidential bins where available or shredded if disposed.

Protecting customer information

Representatives of the company with access to confidential customer information as part of day-to-day work are responsibile for protecting and maintaining the privacy of customer information regardless of sensitivity level and for preventing inappropriate use. Confidential customer information should only be shared when appropriate and on a need-to-know basis.

Performing work on company facilities

- Utilities require field work on company facilities or equipment (electric or gas meters, service laterals, etc.). Based on the Performing Work on Facilities Policy, users are prohibited from working on company facilities located on the user's own property or account, and those of family members, or on their behalf; this includes close friends or family members who perform work on company facilities on the user's behalf.
- Performing work for those friends and acquaintances is not a policy violation provided the work order is generated through formal channels for issuing work orders. Again, if it is a work order for a user's own property or that of a family member or friend, the user must call their immediate supervisor.

Examples of formal channels include work orders or requests, typically provided by a work management system, or verbal orders dispatched by authorized personnel ensuring a proper record of the activity.

The only authorized exceptions to this policy are situations where the safety of the public or property is a concern, or at the specific request of public safety officials such as police or fire.

Customer Information Policy Training
external providers

Appropriate use and release of information

- Assisting customers with questions concerning their energy services account or work performed on their property.
- Managing services provided to customers.
- Interacting with customers or other external providers performing work at the premises.
- Maintaining records to accurately bill accounts.
- Releasing customer information only when the customer authorizes the request to make said information public.

Appropriate releasing of customer information to external providers

Releasing customer information to an external provider is appropriate only when it is in response to a request from a regulatory or government agency, a subpoena or when a written confidentiality agreement is in place.

Requests for the release of customer information to external providers require verbal or written authorization from the customer of record to discuss anything related to the account..

Inappropriate use of customer information

Using customer information improperly or for personal use directly violates the policy.

Some examples include:

- Looking at records of co-workers, neighbors or prominent community members out of curiosity.
- Searching for the phone number or address of a friend, relative or acquaintance.
- Sharing personal customer information you encounter while performing your day-to-day responsibilities with friends, family, neighbors or relatives.
- Viewing information about properties you own, but where service is in the tenant's name.

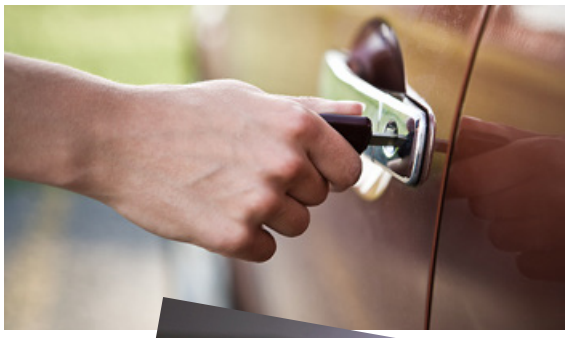
Safeguarding customer information

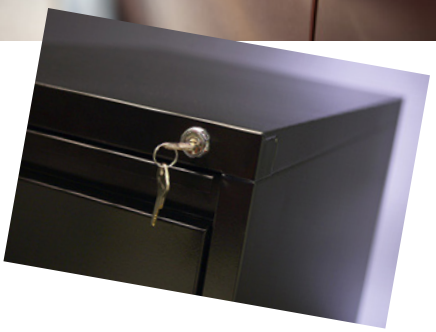
The company has the responsibility to inform and educate users on protecting customer information. In addition to training, the company has multiple controls in place to ensure compliance. Monitoring the use of customer information systems is performed on a regular basis and random samplings are conducted. Identified suspicion of inappropriate activity is monitored. Monitoring may include:

WEC Energy Group

Customer Information Policy Training
external providers

Safeguarding customer information on paper





- Protect confidential information printed from customer information systems or created independently, such as work orders, sketches, spreadsheets, letters, forms, memos, reports, notes, etc.
- Do not leave customer information unattended and available for inappropriate disclosure.
- Properly store customer information in a secure location.
  - In the office this may include a desk drawer, file cabinets, overhead cabinets, file folders and binders. Lock drawers or cabinets, if possible.
  - In the field, this may include placing information out of view — in a locked trunk of a vehicle, for example. Lock the vehicle and keep information off the dashboard, seats and floor, where it could be seen.
- Do not disclose internal information without proper authorization.
- When information is shared or mailed, ensure data is secured in a sealed package or envelope.

Safeguarding customer information on your computer

- Lock computers whenever leaving a workstation or work area. This prevents unauthorized entry of transactions that would be processed using your ID.
- Never use an authorization (ID or log in name) belonging to someone else, or lend passwords to others.
- Change passwords frequently.
- Password protect electronic files containing customer information and only send to recipients authorized to view the information.

Safeguarding customer information (company responsibility)

The company has a responsibility to inform and educate providers on protecting customer information, and has appropriate controls in place to ensure compliance. To secure company systems and ensure others are abiding by their work responsibilities, the company performs a number of privacy and monitoring procedures. It monitors the use of customer information systems on a regular basis and conducts random samplings. When there is a suspicion of inappropriate activity, it monitors that as well. Monitoring may include:

- Email
- Internet activity
- Phone calls

When violations occur, the company takes appropriate and consistent action.

Safeguarding customer information that is electronic data

- If files are saved in a shared network drive:
  - Determine who will have access for business purposes.
  - Establish a password for the file and provide it only to those authorized.
- Do not save restricted data on removable USB or flash drives.
- Protect customer information wherever the materials are used or reside, including those in offices or vehicles.
- When customer information is sent to a printer, retrieve it immediately or use the Private Print option available on multifunction printers.
- Do not save restricted data to the local hard drive of portable computers.
  - Exception: Saving restricted data to the local hard drive is acceptable for laptops that are not connected to the corporate computing network when in use. The laptop should have local hard drive encryption, which protects customer information if the laptop is stolen, and is accessed only by those who need to use the locally stored restricted information.

  Note: This exception does not apply to computers that normally are connected to the corporate computing network.
- Do not forward confidential data via e-mail as attachments unless it is password protected or encrypted. If this is needed, consult a supervisor.
- If in doubt about who is authorized to receive data, ask a supervisor.

Accidental distribution of confidential data

If customer data has been misplaced or provided to an unauthorized recipient:

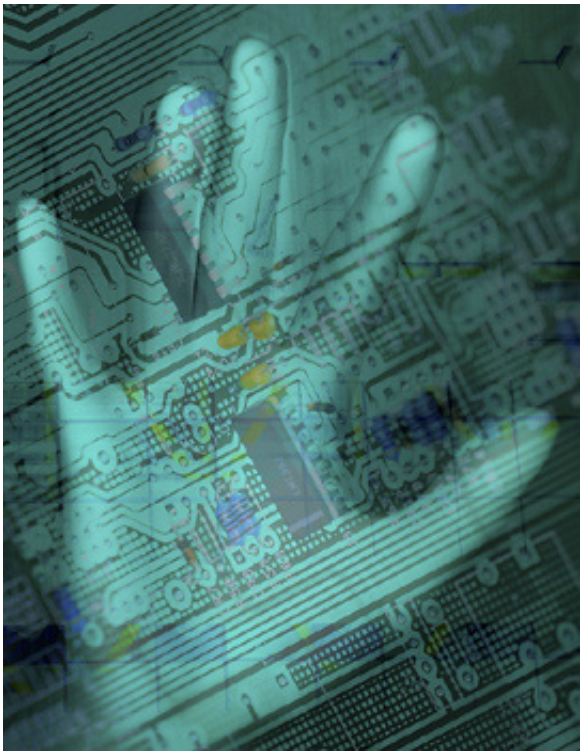
- Attempt to retrieve the data immediately.
- Notify a supervisor.

Compliance is important

Compliance with guidelines governing the use of customer information is of the utmost importance. Misuse of customer information may lead to the revocation of user privileges, which will result in either a discharge or reassignment. Each situation will be dealt with on an individual basis. Anyone viewing customer information for anything other than a business reason is violating this policy.

Questions concerning personal accounts with one of the companies, including account changes, should be directed to the appropriate customer care center. Viewing one's own account information is considered a violation of the Use of Customer

Information Policy. It is never appropriate or acceptable to make adjustments to your own account or to a premises you own, such as rental properties.



Known breaches of a customer's private information must be reported. Failure to do so is considered a violation of the Use of Customer Information Policy. Violations are taken seriously and will be addressed accordingly.

For questions about appropriate use or release of customer information or what can and cannot be shared when speaking and interacting with customers, consult a supervisor.

Consequences of violations

This training presents guidelines to follow. When a violation occurs, appropriate and consistent action is taken. Use of these resources in violation of, or inconsistent with, this policy may result in the following action:

- Revocation of user privileges and/or access to customer information systems.
- Surrender of all passwords, files and/or other resources.

Removed access to customer information, as a result of a violation, may prevent a user from completing job responsibilities, which can lead to either a reassignment or discharge by their employer.

- Certain violations are likely to result in immediate user revocation privileges that may include:
  - Manipulating one's own account for personal gain.
  - Using customer information to a customer's detriment.
  - Viewing or surfing accounts for no business reason.
  - Releasing customer information inappropriately to an external provider.
  - Accessing or transmitting customer and company proprietary information other than in the course of company business.

Summary

Completion of the Use of Customer Information Policy training provides a clear definition of customer information.

- Appropriate customer information handling.
- Appropriate security measures that prevent unauthorized or unintended use of customer information.
- Recognizing the consequences of customer information misuse.
- Smart decision making when handling customer information.
- Know-how to adhere to the guidelines of the Use of WEC Energy Group Customer Information Policy.