Customer Information Policy Training for Contractors

The following training outlines the rules and guidelines contained within the Use of Customer Information Policy. WEC Energy Group takes protection of customer information very seriously. We expect those who do work on our behalf to protect the information in the same manner as our employees. This training defines customer information and the steps you are required to take to protect it. This training also provides guidance in the appropriate use of customer information systems. Please contact your supervisor if you have questions.

At the end of the training you will be asked to complete a Certification. Completion of this form serves to reaffirm your commitment to protect customer information while performing work on behalf of WEC Energy Group companies. Additional instructions are provided at the end of the training for completion of the Certification.

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

Excellent customer service and corporate reputation are built on trust and integrity. Doing what is right for customers – ethically, fairly and honestly – is key to our success. As an individual performing work on behalf of our companies, you need to understand what customer information is and the importance of protecting it. The decisions you make when using customer information are essential to ensure your actions are in compliance with the guidelines established in the Use of Customer Information Policy.

Customer Information Policy Training for Contractors

What is customer information?

Customer information is data or facts known about a person or company that receives energy service or products from WEC Energy Group companies.

Customer information resides in various customer information systems used throughout our companies. The information may also exist in paper format, electronically or viewable on the Internet. 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.
- CDs 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 such as Facebook, Twitter, YouTube, blogs and others.

Guidelines to protect customer information

Our companies strive 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 the information.
- 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.

Your role in protecting customer information

As a representative of WEC Energy Group company, you have access to confidential customer information in your day-to-day work. It is your responsibility to protect and maintain the privacy of customer information regardless of sensitivity level. You should protect this information to prevent inappropriate use. Confidential customer information should only be shared when appropriate and on a need-to-know basis.

Performing work on company facilities

- As utilities, our businesses requires field work on company facilities or equipment (electric or gas meters, service laterals, etc.). Based on the Performing Work on Facilities Policy, you are prohibited from working on company facilities located on your own property or account, and those of family members, or on their behalf. Additionally, you may not have close friends or family members perform work on your behalf on our facilities.
- If you receive a work order to perform work on our facilities for your own property or that of family members, you must call your supervisor.
- In smaller communities served by our companies, you may be acquainted with many customers. Performing work on our facilities 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 your own property or that of family members, you must call your 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.

CONFIDENTIAL

WEC Energy Group

Customer Information Policy Training for Contractors

Appropriate use and release of information

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

Appropriate releasing of customer information to third parties

Release customer information to a third party only is appropriate 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.

We honor requests for the release of customer information to third parties when we receive verbal or written authorization from the customer of record to discuss anything related to their account with a third party.

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.

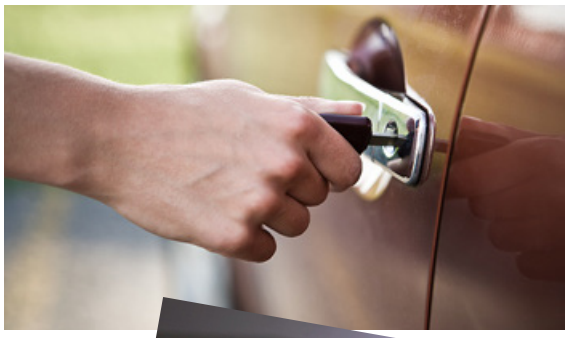
Safeguarding customer information

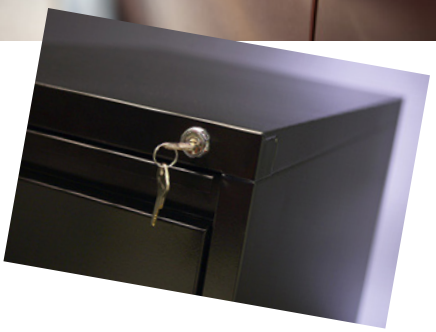
Information does not only reside in electronic systems. Sometimes customer information is printed from electronic systems or viewable on the Internet (e.g., Work Management Online). In everyday work, we may view or put together pictures, sketches, notes, reports, etc. It is critical that customers trust us to keep this information confidential. The appropriate handling of paper, files and orders (by office and field personnel) containing customer information is integral to maintaining customer information privacy.

WEC Energy Group

Customer Information Policy Training for Contractors

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 your PC (computer or laptop) every time you leave your 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 your password to others.
- Change your password frequently.
- Password protect electronic files containing customer information and only send to recipients authorized to view the information.

Safeguarding customer information (company responsibility)

We have a responsibility to inform and educate you on protecting customer information, but we also to have appropriate controls in place to ensure compliance. To secure company systems and ensure you are abiding by your work responsibilities, we perform a number of privacy and monitoring procedures. We monitor the use of our customer information systems on a regular basis and conduct random samplings. When there is a suspicion of inappropriate activity, we monitor this as well. Monitoring may include:

- Email
- Internet activity
- Phone calls

When violations occur, we take appropriate and consistent action.

WEC Energy Group

Customer Information Policy Training for Contractors

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. This includes protecting materials while in your possession, including an office or vehicle.
- 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 laptop or desktop 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 stolen, and is accessed only by those who need to use the locally stored restricted information. Note: This exception does not apply to PCs 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 your supervisor.
- If in doubt about who is authorized to receive data, ask your supervisor.

Accidental distribution of confidential data

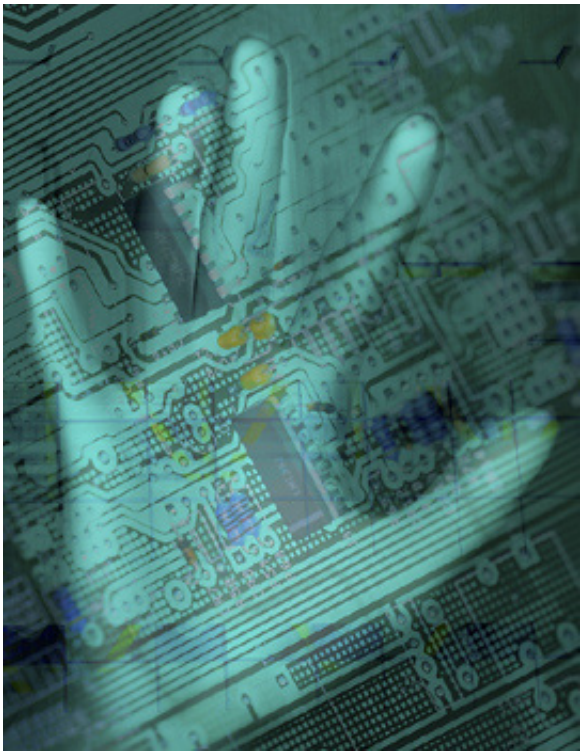
- If customer data has been misplaced or provided to an unauthorized recipient:
  - Attempt to retrieve the data immediately.
  - Notify your supervisor.

Compliance is important

Compliance with the guidelines governing the use of customer information is of the utmost importance. You should understand what constitutes a violation and the consequences for a violation. Misuse of customer information may lead to the revocation of user privileges which will result in either a discharge or reassignment by your employer. Each situation will be dealt with on an individual basis. Anyone viewing customer information for anything other than a business reason, such as out of curiosity or for some other nonbusiness-related purpose, is violating this policy.

If you have questions concerning your own account with one of our companies or need to make changes, please call the appropriate customer care center for assistance. Viewing information relating to your own account 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.



If you are aware that a breach of a customer's private information has occurred, you must report the matter to your supervisor. Failure to do so is considered a violation of the Use of Customer Information Policy. Violations are taken seriously and will be addressed accordingly.

If you are ever in doubt or have a question about the appropriate use or release of customer information or what can and cannot be shared when speaking and interacting with customers, consult your supervisor.

Consequences of violations

This training presents guidelines to follow. When a violation occurs, we take appropriate and consistent action. 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.

Losing your privileges and access to customer information, as a result of a violation, will make you unable to perform your work responsibilities for us. This will lead to either a reassignment or discharge by your employer.

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

Customer Information Policy Training for Contractors

Summary

Now that you have completed the Use of Customer Information Policy training, you:

- Have a clear definition of customer information.
- Can handle customer information appropriately.
- Know appropriate security measures that prevent unauthorized or unintended use of customer information.
- Recognize the consequences of customer information misuse.
- Can make smart decisions when handling customer information.
- Have the know-how to adhere to the guidelines of the Use of WEC Energy Group Customer Information Policy.

Certification instructions

You have completed the training portion of the Use of Customer Information Policy. The next step is to complete the Certification. Completion of the Certification reaffirms your commitment that you:

- Understand the importance and key points to protecting confidential customer information.
- Agree to fully comply with the rules, guidelines and procedures as defined in this training and are part of the Use of Customer Information Policy.
- Will seek advice when you encounter a doubtful situation and report any concerns regarding policy compliance to your immediate supervisor.

Completion of certification

Customer information policy training certification form >