PacifiCorp Security Training

This training comprises PacifiCorp's physical security, cybersecurity, Information Security Management Systems and NERC Critical Infrastructure Protection programs. These programs and this training demonstrate management's commitment to information security throughout the organization. It is important to become familiar with and comply with applicable information security rules and obligations, as defined in policies, standards, laws, regulations, contracts and agreements. This training provides information about how PacifiCorp complies with many of the CIP standard requirements and satisfies the CIP-004 training requirement. The components of the training that are related to CIP compliance are denoted by the following icon, which includes the sub requirement number from CIP-004.

PacifiCorp's Physical and Cybersecurity Programs

NERC CIP 2.1.5

Security Program Overview	PacifiCorp's physical and cybersecurity programs protect its human, physical and information assets. **PHYSICAL SECURITY** is often the first line of defense in protecting our personnel, facilities and assets. Physical assets include: • Generation plants • Substations • Distribution and transmission lines • Corporate offices • Control centers • Communications sites • Vehicles, equipment and tools **CYBERSECURITY** focuses on protection of computing resources and information. Electronic assets include computer hardware, software applications and communication networks **BOTH PROGRAMS** • Strive to prevent, delay or minimize attacks • Provide the foundation for sustaining compliance with regulatory and industry requirements • Collaborate with external agencies and sustain industry partnership to identify threats and benefit from best practices • Maintain security awareness and training programs

PacifiCorp ISMS and CIP Compliance

CIP Systems	PacifiCorp is required to comply with the North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection Standards (CIP). PacifiCorp's critical infrastructure includes its assets (locations) that are vital to operation of the Bulk Electric System (BES.) • The assets must be protected from malicious activities that could threaten the reliability of the BES • Failure to comply with the standards could expose the assets to malicious activity and result in fines of up to one million dollars per day, per violation • PacifiCorp's Compliance Office provides oversight to ensure the business remains compliant with the standards

Information Security Management Systems (ISMS)	PacifiCorp Information Management Systems (ISMS) focuses on a systematic process approach for the establishment, implementation, maintenance and continual improvement to managing sensitive operational and select employee and customer information so that it remains secure.
	• The standard for ISMS is ISO/IEC 27001:2013
	• In-scope ISMS physical and cybersecurity assets include:
	  ○ Generation Thermal and Renewable fleet distributed control systems real-time information
	  ○ Energy Management System real-time operations information
	  ○ Sensitive employee information (SEI) – defined as an individual with a P number's name and at least one of the following data elements:
	  ▪ SSN #(full number)
	  ▪ Drivers' License Number
	  ▪ Passport Number
	  ▪ State ID Number
	  ▪ Date of Birth
	  ▪ Personal health information as defined by the U.S. Health Insurance Portability and Accountability Act
	  ▪ Personal Credit Card Numbers, bank account numbers or bank routing numbers
	  ○ Residential customer information – which includes PPI (Personal Identifiable Information) defined as customer name and at least one of the following data elements:
	  ▪ SSN #(full number)
	  ▪ Drivers' License Number
	  ▪ Passport Number
	  ▪ State ID Number
	  ▪ Date of Birth
	  ▪ Acct Type, Routing Number, Account number (ACH)
	  ▪ Credit Card Number, Date of Expiry, security code
	
	PacifiCorp's Compliance Office provides oversight to ensure the business remains compliant with the standards.

Information Security Policies NERC CIP 2.1.1	The PacifiCorp Information Security Policies identify the guiding principles that govern protection of its facilities and cyber assets (systems/devices) subject to the ISMS and CIP Standards. The policies reference documents, processes and procedures that provide detailed information about how PacifiCorp adheres to the principles. In addition to policy topics contained within this training, specific ISMS policies cover: • Roles and responsibilities • information classification (and handling) and acceptable use of assets including decommissioning and disposal • physical and environmental security • information transfer • teleworking • backup • communications security • management of technical vulnerabilities • supplier relationships The policies can be accessed on the PacifiCorp Corporate and Information Security Management System intranet portals. As a newly hired person you must review these policies.

Controlling Access

Access Management NERC CIP 2.1.2/3	Access to PacifiCorp's physical and logical ISO and CIP Systems are managed through a variety of processes that are designed to: • **Restrict** unauthorized access to devices and locations • **Prevent** compromise or failure of infrastructure components Access management includes: • Approving who has access to specific devices and locations • Performing background checks and providing additional training to personnel with access to CIP Systems and/or ISMS in-scope devices or locations • Periodically reviewing access privileges to confirm an individual's ongoing business need for the access • Removing an individual's access when it is no longer needed, such as due to a job change or when the person leaves the company • Maintaining accurate records and program documentation
Electronic Access Controls NERC CIP 2.1.3	Below are PacifiCorp's key strategies related to controlling electronic access. **CONTROL AND MONITOR NETWORK TRAFFIC** • All communications to and from PacifiCorp networks are rigorously controlled and monitored • CIP Cyber Systems connected to a network via a routable protocol are required to reside in an Electronic Security Perimeter (ESP) that is enforced using firewalls • Inbound and outbound communications with CIP Cyber Systems within an ESP require documented access permissions, including the reason for granting access • Network traffic is managed through security zones that are enforced using firewalls • Since most jobs at PacifiCorp require you to access its corporate network, PacifiCorp uses passwords and remote access controls to authenticate a person's identity before allowing access to its network. This helps protect business assets from unauthorized access. **RESTRICT REMOTE ACCESS** • All remote access to CIP Cyber Assets and ISMS Cyber Assets require authentication when establishing Dial-up Connectivity or multi-factor authentication for all Interactive Remote Access sessions • Interactive Remote Access is required to utilize encryption that terminates at an Intermediate System such that the remote computing device does not directly access a BES Cyber Asset • PacifiCorp restricts access to its computing resources and information from remote hosts and non-company-controlled networks • This includes access from workstations, laptops, smart phones and other mobile devices that could be connected to the company network **REQUIRE SECURE PASSWORDS** PacifiCorp has established guidelines to ensure personnel create secure passwords, also known as strong passwords. Passwords must contain at least 15 characters and adhere to the following requirements: • Contain at least one uppercase and one lowercase letter • Cannot contain the same character three times in a row or sequential numbers • Cannot contain portions of your full name or user ID • Cannot contain words identified as common or guessable , regardless of their complexity – even those with substituted characters (e.g., w!nter, p@ssw0rd) • Cannot contain common number or keyboard patterns (e.g., 1234, 2468, 2015, qwerty, asdfg) • Passwords on CIP Cyber Assets must also contain at least one number or special character

	The best way to remember a password is to make it meaningful to you. Some people use phrases to help them remember. For example: • SprtBrndSprtBrnd (childhood dog and cat names without vowels • Gm20lkGm45lkGm16lk (gym locker combination mixed with letters) Your password will expire in 365 days. If you need to write down or electronically store your password, keep it separate from your employee ID and any information that could identify what the password is associated with. Make sure you store it in a secure location (e.g., locked drawer, wallet or purse). **DO NOT** share your passwords with others, use the same password on multiple Web sites, or allow your Web browser to automatically save your passwords. **INFORM PERSONNEL ABOUT PACIFICORP'S EXPECTATIONS** • A login banner is used to inform and remind employees, contractors and others who access PacifiCorp's computing resources and information about the company's expectations related to their use • The computing resources and information used and created by personnel are PacifiCorp property • Use of PacifiCorp's assets is construed as implied consent to established terms and conditions • Users should have **NO** expectation of privacy. At any time and for any lawful purpose, PacifiCorp may monitor, intercept, record and search any communications or data transiting or stored on its systems.
Physical Access Controls NERC CIP 2.1.2 NERC CIP 2.1.4	**SECURITY DEVICES AND SYSTEMS** Security devices and systems prevent or impede attackers from impacting business personnel, facilities, assets and information. PacifiCorp uses a five-tiered strategy to secure its physical assets. • Environmental design – placing an asset in a location that enhances its security • Mechanical and electronic access controls– restrict access by unauthorized personnel • Intrusion detection systems – alert security staff to an attack or unauthorized access attempt • Monitoring – video systems and observation and investigation by security personnel • Quality control – regular testing and review of physical security systems and procedures The following strategies are particularly important for compliance with CIP requirements to protect BES facilities and the cyber systems that support them • Monitoring access to control centers 24-hours a day/seven days a week • Use of two separate methods to verify a person's identity before permitting unescorted access to control centers • Implementation of procedures to authorize and manage unescorted access to all locations **VISITOR CONTROLS** A visitor is defined as anyone who has not been approved for unescorted access to a specific site or secured area, including employees from other locations, contractors and vendors • Processes to manage and monitor visitor access are different for corporate offices, control centers, generation plants and substations • Visitors who need access to a secured area must be escorted by authorized personnel at all times • Be sure to check the requirements for your location before admitting visitors

Information Protection

BES Cyber System Information NERC CIP 2.1.5	BES Cyber System Information (BCSI) • Includes information about a CIP Cyber System that is not publically available and could be used to gain unauthorized access or pose a security threat to the system • Excludes individual pieces of information that by themselves could not be used to allow unauthorized access and do not pose a threat to the security of the system

	Groups that often handle BCSI include IT, system operations, substation operations, and plant operations. Although most company personnel will not come in contact with BCSI, it important to understand that CIP-related information must be protected. The proper use and handling of BCSI is described in the BES Cyber System Information Program. Important things to know about BCSI include: • Access to BCSI is restricted • Documents identified as BCSI should be marked with the BCSI stamp or label • BCSI should be stored in a secure location, such as a restricted shared drive or in a desk drawer • If you come across unattended BCSI outside of a designated repository, move the documentation to a secured area and attempt to identify the owner or contact the compliance office • BCSI must be vigilantly managed when in transit. Detailed handling instructions are included in the BCSI Protection Procedure • A non-disclosure agreement must be in place if BCSI is shared with a third party • Encryption is required when sending BCSI to a third party. Encryption instructions are available on the PacifiCorp Corporate intranet portal The compliance office is available to answer questions about classifying, handling and storing BCSI.
Supplier Relationships	Individuals interacting with supplier personnel must be aware of appropriate rules of engagement and behavior based on the type of supplier and the level of supplier access to the organization's in-scope ISMS systems and information.
Labeling and Handling	Hard copy and electronic documents identified as SENSITIVE for sensitive employee information (SEI) may be subjected to a labeling scheme to identify it as to its need for appropriate handling.

Cybersecurity Incident Identification

Cybersecurity Incident Identification and Initial Notification and Reporting NERC CIP 2.1.6/8	PacifiCorp's Cybersecurity Incident Response Plan (CSIRP) describes its strategies to respond to suspected or confirmed cybersecurity incidents. The scope of the CSIRP includes analysis and response to suspected or confirmed unauthorized access by a person or device through circumventing or damaging its physical or logical access control measures, including those associated with CIP locations and systems. The CSIRP identifies: • Procedures that characterize and classify events as reportable cybersecurity incidents • Process for reporting a cybersecurity incident to the Electricity Sector Information Sharing and Analysis Center (E-ISAC) • Cybersecurity Incident Response Team (CSIRT) roles and responsibilities, response strategies, incident handling procedures, and communication plans The CSIRP is supported by business continuity and technology recovery plans that are developed and maintained by the responsible business units and functions. • Business continuity plans focus on keeping the business running • Technology recovery plans focus on sustaining systems and applications, and cyber system recovery Activities that may warrant activation of the CSIRP include: • Malicious code infection • Unauthorized access to a network, system, application, information or computing resource • Inappropriate use of information or computing resources • Identification of a condition that could cause a physical or cyber attack. • An incident involving two or more threatening activities If you suspect a cybersecurity incident is developing or has occurred, call the Enterprise Service Desk, which will notify the personnel and teams responsible for cybersecurity incident response and investigation.

	Corporate Services Line Portland 503-813-5555 Salt Lake City 801-220-5555 **Option 1: Security Operations Center** – Physical security incidents **Option 2: Enterprise Service Desk** – Computers, printers & and other IT issues, including cybersecurity incidents and customer data privacy issues

Recovery Plans

BES Cyber System Recovery Plans NERC CIP 2.1.7	PacifiCorp has developed and maintains Technology Recovery Plans for all its ISMS and CIP Systems. The plans identify prearranged activities for responders to engage in if the following incidents occur: • Loss of primary site • Loss of equipment • Cyber incident/malicious code • Database corruption, where applicable The plans are exercised at a minimum every 15 months. The exercises are conducted through: • Tabletop walkthroughs • Scenario-based exercises • Functional restoration of devices from backups • Site switches of redundant systems

Cybersecurity Risks

BES Cybersecurity Risks Associated with Electronic Interconnectivity NERC CIP 2.1.9	PacifiCorp and the industry must be constantly alert for risks that may impact the reliability of the Bulk Electric System. One risk is the increased electronic connectivity of BES Cyber Systems. • Modern operating systems and software applications are more susceptible to cybersecurity vulnerabilities and require patching to mitigate the risks • Physical ports and logical ports and services on CIP systems require management to restrict use to only what is needed for business purposes • Transient computing devices and removable media require cybersecurity protections, including malware scanning, and must be authorized prior to connecting to a CIP system • Never connect a computing device or removable media to any CIP system without first advising your manager

Situational Awareness

Employee and Customer Data Privacy	PacifiCorp is committed to protecting the privacy of its employees and customer's personal and financial data.
	
	TYPES OF SENSITIVE EMPLOYEE INFORMATION (SEI)
	• SSN #(full number)
	• Drivers' License Number
	• Passport Number
	• State ID Number
	• Date of Birth
	• Personal health information as defined by the U.S. Health Insurance Portability and Accountability Act
	• Personal Credit Card Numbers, bank account numbers or bank routing numbers
	
	TYPES OF SENSITIVE CUSTOMER DATA
	• PacifiCorp account number
	• Credit card number
	• Social security number
	• Customer birth date
	• Driver's license number
	• Telephone number
	• Tax ID number
	• Address
	• Bank account number
	
	PROTECTING EMPLOYEE AND CUSTOMER DATA
	• Never provide employee or customer information to:
	  ○ Another employee, unless there is a business need to know
	  ○ A party outside the company, unless authorized to do so by legal or management directive
	• Only share data with co-workers when necessary
	• If you obtain information from a co-worker indirectly through an email, conversation or phone call, you are responsible for maintaining the confidentiality and security of the information
	• Make sure your computer is password protected when you walk away from it
	• Secure documents that contain customer data when you are not using them
	• Store customer data on a secure network drive – not on your local C drive
	• Ensure documents that contain sensitive employee information are managed per the PacifiCorp Records Retention Schedule
	
	REPORTING POTENTIAL COMPROMISE
	If you suspect customer data has been lost, stolen or compromised, immediately call the Enterprise Service Desk, which will notify the personnel responsible for incident response and investigation.

Electronic Devices	Electronic devices may include computer workstations or laptops, tablets computers and smartphones. **ANTI-VIRUS SOFTWARE** • Anti-virus software is installed on all company-owned electronic devices to minimize malware exposure • Disabling the anti-virus software is strictly forbidden. In addition, the devices must regularly be connected to the corporate network to receive anti-virus and software updates. **GENERAL GUIDELINES** • Logoff your device when unattended or not in use • When at your desk, secure your laptop with a cable lock. Store the cable key in a safe location. • Avoid leaving your device unattended in common areas or conference rooms • Use a nondescript bag to transport your laptop or device • Place a distinctive sticker or cover on your device to make it easy to recognize in a stranger's possession • If traveling by car/truck, store the laptop or device in the trunk or under a seat before you reach your destination. Ensure the vehicle is locked • If a company-owned device is lost or stolen, immediately notify your manager and the Enterprise Service Desk
Portable Storage Devices NERC CIP 2.1.9	Portable storage devices are capable of storing and transmitting digital media files, such as documents, images, audio and video. Examples of portable storage devices include digital cameras, CDs/DVDs, smartphones, flash drives, tablet computers, MP3 players, SD cards and external hard drives. **Only company-owned or authorized devices may be connected to PacifiCorp's computing resources and networks.** Such devices should always be scanned for malware before and between uses. If unsure if something is allowed, contact the Enterprise Service Desk **BEFORE** connecting the device. **CARE OF PORTABLE STORAGE DEVICES** • Take precautions to store the portable storage device in a secure location when not in use • Do not share approved devices or passwords with others • Encrypt the data when possible • If the device is lost or stolen, immediately notify your manager and the Enterprise Service Desk. It will initiate a process to properly disable network connectivity and services.
Unauthorized Software	Downloading unauthorized software, shareware, games, screensavers, media players and copyrighted material on company-owned devices is prohibited. Installation of unauthorized software may result in introduction of malware vulnerabilities, monetary penalties due to noncompliance with licensing requirements, and increased risk of software misuse. All software installed on company-owned electronic devices must be approved and licensed. Installing company-authorized software on personal electronic devices without management approval and appropriate licensing is also prohibited. PacifiCorp periodically audits company-owned devices to ensure only authorized software has been installed on them. Rules for the development of software and systems are also established by Corporate Security.

Social Engineering	Social engineering involves the manipulation or deception of people to convince them to divulge sensitive information or break normal security procedures. It takes advantage of an individual's normal tendency to want to help someone out. It is typically associated with unauthorized access to information or electronic devices, but it also may be used to gain unauthorized access to facilities and assets. **TAILGATING** Tailgating is a common type of social engineering used to gain unauthorized access to a secured location. It involves quickly following an authorized user through an access door or catching a door or other access mechanism, such as a gate, before it closes. All staff entering a secured area must swipe their badge prior to entering, even if their badge was not used to open the door. Be watchful for people entering behind you who do not use their badge to register access. If they do not have a badge, direct or escort them to the Security Desk. **PHISHING** The phisher (attacker) typically sends an email, instant message, comment (think Facebook) or text message that appears to come from a legitimate source, such as a friend, co-worker, bank, school, business or institution. The phisher's goal is to get you to share sensitive personal, business or customer information or click on a link that will install malware on your device. **General Guidelines** • Be polite, but exercise caution. • Don't let pressure or intimidation stop you from confirming the identity of a person • Don't share sensitive personal, business or customer information until you have confirmed the identity of the requesting source • Never deviate from approved processes without appropriate internal authorization • Escalate questions or concerns to your manager or the Enterprise Service Desk **Email Phishing** • If you receive a suspicious email or message ignore and delete it • Email messages that come from an external domain are marked with red text that is generated by the IT department • When you are unfamiliar with the sender or the domain from which the email is coming, always validate the authenticity of the sender • Don't open links or attachments in emails or social media messages from unknown or suspicious senders • Hover your mouse over a link to see its true path • When you don't know where the link is going, always stop and check with the sender before doing anything
Weapons and Dangerous Materials	PacifiCorp strictly prohibits the possession of unauthorized weapons and/or dangerous materials while on its properties or in company-owned vehicles. **This prohibition is applicable to all PacifiCorp employees, contractors, vendors and visitors, even those with concealed carry gun permits.** **Unauthorized Weapons** includes, but is not limited to, archery equipment, handguns, shotguns, rifles, knives not designed for work or eating, and unauthorized projectiles of any kind **Dangerous Materials** includes, but is not limited to, combustible or flammable incendiary devices and explosives
	Individuals should consult with local law enforcement and PacifiCorp human resources to identify the circumstances that would allow a firearm to be brought onto company property. Violation of this policy will result in disciplinary action up to and including termination of employment or contractual relationship and may involve legal prosecution.

Active Shooter	An active shooter is an individual actively engaged in killing or harming people through the use of firearms. In most cases, there is no pattern or method to the selection of victims. It is important for individuals to be aware of this threat and be mentally and physically prepared to respond, if needed. The only resource that is guaranteed to be present if you are attacked is YOU! Preplanning and a calm demeanor will increase your odds of survival and may help others to respond appropriately. Be aware of your environment and any possible obstacles. • Note the location of the two exits near you • Note barriers between you and the exits • Be aware of potential places to hide or use as safe rooms • Visualize yourself safely leaving the area • Be aware that customers and clients are likely to follow the lead of employees during an incident Actions taken during an active shooter situation should be determined by the circumstances and the location of the shooter. It is important to assess the situation and do whatever it takes to survive!
Bomb Threats	Most bomb threats are received by telephone. If you receive a bomb threat: • Contact the Corporate Services Line as quickly as possible. If a coworker is nearby, get their attention and indicate that help is needed • Remain calm, be polite and listen carefully • Try to keep the caller engaged and write down as much information as possible to provide to emergency responders • Do not use an electronic device, as some bombs may be activated by radio waves. If you must use an electronic device, try to move away from the area. • Do not hang up the phone. You may be the only person who has an opportunity to obtain vital information from the caller. Every effort should be made to keep the line open for tracking purposes.
Workplace Violence	All employees share responsibility for helping to maintain a safe and secure workplace. Managers and co-workers are sometimes the first to notice the characteristics of potentially violent behavior in others. You should notify your manager of the potential for workplace violence if you: • Have direct knowledge or reasonable suspicion of a threat • Have observed warning signs, such as unusual or aggressive behavior or expressions of violence This includes threats made outside the workplace that could affect the workplace. Reporting concerns allows action to be taken before a situation escalates into violence. Employees who have reason to believe their personal safety is at risk should immediately alert their manager and employee relations so appropriate actions can be initiated.
Evacuation	Become familiar with your work location floor plan and evacuation procedures. Be sure to note the locations of fire extinguishers, fire alarms, medical supplies, emergency exits and alternate evacuation routes. If an evacuation is required: • **DO** remain calm, use handrails on stairways, listen for instructions and report to your safe area • **DO NOT** use the elevators, push or run, or re-enter the facility until instructed to do so by authorized personnel

Event Reporting

Suspicious Activities	PacifiCorp relies on its personnel to be alert to suspicious activities that could result in harm to its personnel, facilities or assets. Suspicious activities may include: • Vandalism or sabotage of PacifiCorp assets • Activities related to theft of business equipment or materials • Indications that your business computer account has been accessed or used by someone else • Someone walking around inside your business location who does not seem to belong there • Someone taking unauthorized pictures of a facility or equipment • The presence of a suspicious or abandoned vehicle inside or outside a business facility • Malfunctions or breaches of security controls (doors, locks, etc.) • Breaches of information integrity, confidentiality or availability • Lost or found security (keys, badges) or mobile devices (removable media, phones, laptops, etc.). • Encountering unescorted visitors or anyone not wearing visible identification • Observation of someone tailgating or other access violation
Event Reporting	Known or suspected acts of vandalism or sabotage and suspicious activities must be reported to corporate services immediately so an appropriate response can be initiated. In some instances, there are time-sensitive reporting requirements to government and regulatory agencies. **Corporate Services Line** Portland 503-813-5555 Salt Lake City 801-220-5555 **Option 1: Security Operations Center** – Physical security incidents **Option 2: Enterprise Service Desk** – Computers, printers & and other IT issues, including cybersecurity incidents and customer data privacy issues **Email:** pacificorpsecurity@pacificorp.com

Enforcement

Enforcement Policy	Failure to comply with PacifiCorp policies and procedures is subject to disciplinary action appropriate to the severity of the violation, up to and including termination of employment and possible criminal prosecution, so please use good security practices!

FERC Standards of Conduct Overview Training

Why am I receiving this training bulletin?	It is the policy of PacifiCorp to comply with all laws and regulations, and to conduct its business with honesty, integrity and fairness. One of the important regulatory requirements of PacifiCorp's business as an electric transmission provider regulated by the Federal Energy Regulatory Commission (FERC) is full compliance with the Standards of Conduct. This training is designed to acquaint you with the requirements of the Standards of Conduct and to advise you of your compliance obligations under these rules.
What are the FERC Standards of Conduct?	The Standards of Conduct, or SOC, are rules adopted by FERC that are intended to ensure that PacifiCorp's transmission function employees operate separately from and independently of its marketing function employees engaged in wholesale power sales transactions. The SOC are guided by four basic principles: • Non-discrimination. Transmission providers must treat all transmission customers, affiliated or non-affiliated, on a not unduly discriminatory basis and must not make or grant any undue preferences or advantages. • Independent functioning. PacifiCorp's transmission function employees must operate independently from marketing function employees and may not conduct marketing functions. • No conduit. No employees of PacifiCorp or its affiliates may be conduits of non-public transmission function information to marketing function employees. • Equal Access. All transmission customers are entitled to equal access to non-public transmission function information
What are transmission and marketing functions?	• Marketing functions are defined as the sale or making of offers to sell wholesale electric energy and capacity, demand response, virtual transactions, or financial or physical transmission rights, but excluding bundled retail sales. • Transmission functions are defined as the planning, directing, organizing or carrying out of day-to-day transmission operations, including the granting and denying of transmission service requests.
Who are PacifiCorp's marketing functions employees?	Certain PacifiCorp Energy Supply Management employees are marketing function employees. For a list of these employees, please refer to PacifiCorp's internet website or its Open Access Same-Time Information (OASIS) website: http://www.oasis.oati.com/PPW/PPWdocs/mfelist.pdf PacifiCorp's marketing function employees can also be identified by an email address designation of "{Mkt Function}" following each employee's name.
How can I comply with the FERC Standards of Conduct?	One of the most important rules from the SOC that employees must comply with is the "no conduit" rule. Employees must ensure that non- public transmission function information is not shared with marketing function employees, except through public communications. PacifiCorp maintains an internet site called its OASIS that is intended to be the main source of public communication of transmission function information on its electric transmission operations.
What are the "no conduit" rule and information-sharing restrictions?	The obligation not to be a "conduit" of non-public transmission function information is the most important rule with which employees should be familiar. The "no conduit" rule provides that if, in the course of their employment, any employee, contractor, consultant or agent of PacifiCorp or its affiliates receives non-public transmission function information, he or she cannot act as a "conduit" to pass that information to marketing function employees.

	This rule applies to all forms of communication during business and non- business hours, i.e. phone, e-mails, fax, in-person, etc. No employee should be a conduit for the improper sharing of non-public transmission function information. Note that the "no conduit" rule applies to contractors, consultants, agents and PacifiCorp employees. None of these individuals may share non- public transmission function information with marketing function personnel, regardless of the source of the information.
What are examples of non-public transmission function information?	Remember that transmission function information covers the planning directing, organizing or carrying out of day-to-day transmission system operations, including the granting and denying of transmission service requests, which includes information about available transmission capability, price, curtailments, storage, and balancing. Information about long-term transmission planning is generally not considered non-public transmission function information because it is available to all parties involved in the transmission planning process.
Does this mean I can't talk with marketing function employees?	No. The SOC rules do not prohibit you from talking to these employees, however if you are a transmission function employee, your interactions with marketing function employees should be limited to communications and interactions that do not include the improper disclosure of any non- public transmission function information. Employees who have non-public transmission function information must adhere to the "no conduit" rule and make sure that they do not inadvertently pass the information along to marketing function personnel
Why do I have to comply?	It is the policy of PacifiCorp that its officers, employees, contractors, consultants, and agents strictly adhere to the requirements of the SOC. FERC can impose substantial penalties for violations of the SOC. These include loss of market-based rates and significant civil (and even criminal) penalties. FERC can impose civil penalties of up to $1 million dollars per violation per day for violations of the SOC.
Who is PacifiCorp's compliance officer?	PacifiCorp has designated Mr. Colt Norrish, as the Chief Compliance Officer for SOC and other compliance issues. The Compliance department manages the company-wide Regulatory Hotline, which is used to report potential or actual SOC/Regulatory Compliance issues.
What if I am aware of non-compliance situations?	**Notify your supervisor and the Regulatory Compliance Hotline at 503-813-5555, option 6, or at 801-220-5555, option 6, immediately.**

Are communications with MidAmerican Energy Company, Northern Natural Gas Company and Kern River Gas Transmission Company restricted by this rule?	MidAmerican Energy Company is a related electric transmission provider. PacifiCorp can share information with MidAmerican Energy Company with one exception. MidAmerican Energy Company's electric trading group contains marketing function employees. Non-public transmission function information, either about MidAmerican Energy Company or PacifiCorp, may only be shared with MidAmerican employees who are not employed by that group. In the same fashion, no MidAmerican Energy Company non-public transmission function information should be shared with marketing function employees that may engage in transmission transactions on MidAmerican Energy Company's transmission system in PacifiCorp's Energy Supply Management division. Similarly, Northern Natural Gas and Kern River are affiliated gas transmission providers. Certain MidAmerican Energy Company and PacifiCorp gas supply and unregulated retail services employees engage in marketing functions on the Kern River system. No non-public transmission function information from Kern River should be shared with these employees.

Are there any other restrictions on sharing information that I should be aware of?	Yes. FERC's separate Market-Based Rates Affiliate Restrictions ensure that "market information" is not passed between PacifiCorp Energy Supply Management employees or its contractors and any employees of a market-regulated power sales affiliate such as Cordova Energy Company, directly or indirectly. "Market information" is broadly defined by FERC as a communication between a utility and its affiliated power marketer concerning the utility's, or the affiliated power marketer's power or transmission business, including:
	• Positive and negative information such as sales or purchases that will or will not be made
	• Present or future information
	• Concrete or potential information
	• Information of significant or slight value
	
	The Affiliate Restrictions also provide as follows:
	• PacifiCorp will not directly or indirectly provide to any affiliated power marketer personnel non-public information regarding transmission availability, terms or rates on PacifiCorp's transmission system unless such information:
	  ○ Is provided in response to a request by a power marketing affiliate for transmission service under PacifiCorp's open-access transmission tariff
	  ○ Pertains to the requested service
	  ○ Is comparable to the information provided to non-affiliated entities in the context of their requests for transmission service
	
	PacifiCorp will post on its OASIS the disposition of any request for transmission service by any power marketing affiliate in the same manner as it would post information for a request for service by any non-affiliated eligible entity.

Three-Part Communication Training

What is Three-Part Communication?	Three-part communication is a tool used to ensure instructions and information are understood correctly BEFORE actions are taken. Three-part communication is an important tool used in the field but can also be valuable in other situations that involve important phone communication. Examples include, giving operating instructions and communicating critical or emergency procedures. Three-Part Communication requires the following: • The person initiating the call issues the message. • The person receiving the call repeats back the details of the message to the issuer. • The person who issued the message confirms the details are correct or repeats the corrected message.
When should I use it?	Per the North American Electric Reliability Corporation's (NERC) COM-002-4 Standard, you **must** use three-part communication anytime you are communicating Operating Instructions* or directing operational tasks or information. It should also be used if • You are in a high noise area • There is a risk of miscommunication • There are critical processes or procedures • You are using radios, telephones and other communication devices You should use three-part communication when you are giving instructions in one location for a procedure to be performed in another location. You may or may not be responsible for issuing or receiving Operating Instructions as part of your job description. Please ask your supervisor or the Compliance Office if you are unsure. *NERC defines Operating Instruction as: A command by operating personnel responsible for the real-time operation of the interconnected Bulk Electric System to change or preserve the state, status, output, or input of an Element of the Bulk Electric System or Facility of the Bulk Electric System. (A discussion of general information and of potential options or alternatives to resolve Bulk Electric System operating concerns is not a command and is not considered an Operating Instruction.)
Guidelines	• Begin with the name/position of person being addressed • Only one person talks at a time • Be specific • Do not use slang or regional words • Avoid giving multiple instructions • Use approved phonetic alphabet if applicable • Do not act until issuer confirms a correct response

Three-part communication example