AMERICAN ELECTRIC POWER

Principles of Business Conduct

At AEP, we are committed to improving customers' lives with reliable, affordable power.

A Letter from our President & CEO

February 16, 2026

Dear Team Members,

At AEP, our vision is clear: to improve lives by delivering reliable, affordable power. That mission calls for more than simply showing up—it demands an unwavering commitment to our customers, our employees, and the environment. It requires integrity in every regulatory and legislative action, and a relentless focus on operational excellence, and financial strength in all we do.

Our Ways of Working—the "Winning Behaviors" we practice daily—define how we deliver on those principles: Be Customer Focused, Get Stuff Done, Be an Owner, and Be a Team Player.

This updated *Principles of Business Conduct* brings these two powerful concepts together—the "what" and the "how"—into one clear standard for decision making and behavior across AEP. It is not just a reference guide; it is a promise to each other and to our customers.

As your CEO, I commit—along with our entire leadership team—to uphold these standards without exception. We will reward results achieved the right way, address issues swiftly and fairly, and continually strengthen the training, tools, and processes that help you succeed. Our customers and communities deserve nothing less.

Thank you for living our values, practicing our ways of working, and making ethics and compliance a daily discipline. Together, we will continue to power a new and brighter future—reliably, affordably, and with integrity.

With appreciation,

Bill Fehrman
Chief Executive Officer

Speak Up

WHY SPEAK UP?

At AEP, we are committed to a culture of trust and transparency, ensuring the highest level of ethics and integrity. Employees should feel free to speak up or raise concerns without the fear of retaliation.

WHAT SPEAKING UP MEANS

"Speaking up" is not just about reporting misconduct.

It's about:

- Asking questions
- Sharing ideas
- Raising concerns
- Seeking clarity

Get more information on the Speak-Up Policy →

NO RETALIATION

AEP strictly prohibits retaliation against anyone who, in good faith, raises a concern, reports potential misconduct, or participates in an investigation. Retaliation can take many forms such as demotion, exclusion, or any adverse action and it will not be tolerated. Every report will be handled respectfully, confidentially to the extent possible, and investigated promptly. If you believe you have experienced retaliation, report it immediately through the same channels used for any other concerns.

WAYS OF WORKING

Be Customer Focused

- Put yourself in your customer's shoes
- Know your customer
- Respond to customer needs quickly

Get Stuff Done

- Measure success by impact, not effort
- Act with urgency
- Make things better

Be an Owner

- Manage the details
- Set high standards
- Be accountable

Be a Team Player

- Collaborate and share
- Get to "yes"
- Be open to diverse perspectives

Table of Contents

Customer Service

Industry-best customer experience

Contents

Customer Experience

Maintaining Customer Focus

To ensure that we continue to meet the needs of our customers and enhance their quality of life, it's essential to adopt a customer-centric approach.

HOW TO MAINTAIN CUSTOMER FOCUS

1. Listen to Our Customers

- Actively seek feedback through surveys, interviews, and direct communication
- Use customer insights to inform service improvements and new offerings

2. Deliver Value to Our Customers

- Ensure that services provided are efficient, reliable, and safe
- Promote products and services transparently, emphasizing their benefits and value

3. Consider the Customer Impact of Our Decisions

- Evaluate how decisions affect customers before implementation
- Maintain a balance between operational efficiency and customer satisfaction

Cultivating a reputation for honest, compassionate, and respectful communication is fundamental to this long-term approach.

Communications & Marketing

AEP is often featured in various media outlets, and it's important to handle media interactions appropriately.

Here are the key points to remember:

- If you receive a request from the news media for an interview or to address an issue on behalf of the company, please refer the request to the Communications & Marketing team.
- For situations requiring immediate comments related to public safety, employees may respond within their areas of expertise, but they should inform Communications & Marketing of the media contact as soon as possible.

Additional Information

By following these guidelines, we can ensure that our communications are consistent and aligned with the company's objectives.

WAYS OF WORKING

Be Customer Focused

- Put yourself in your customer's shoes
- Know your customer
- Respond to customer needs quickly

Social & Digital Media

Social & Digital Media Policy

AEP recognizes the significance of social and digital media in shaping perceptions about the company and its offerings. This policy applies to all employees and contractors regarding their social media communications, whether during work or non-working hours, and on both company-issued and personal devices.

Key Guidelines

1. Maintain Professionalism

- If you wouldn't say it directly to your supervisor or CEO, don't say it on social media.
- Treat everyone with respect, including past and present co-workers, customers, and suppliers.

2. Privacy Awareness

- Understand that private posts may not be private; anything you publish can be viewed by others.
- Consider your audience and the potential impact of your posts.

3. Authenticity

- Clearly express that the views you share are your own.
- Ensure your online profiles are consistent with how you present yourself in the workplace.

4. Authorized Representation

- Only approved spokespeople can speak on behalf of AEP. Do not portray yourself as an unofficial spokesperson.
- Only individuals granted permission as "Authorized Digital Spokespersons" may comment on behalf of AEP.

5. Content Caution

- Avoid demeaning, inflammatory, or offensive comments.
- Correct any mistakes promptly and responsibly.

6. Confidentiality & Copyrights

- Never disclose confidential AEP information or personal employee details.
- Respect copyrights and fair use; always credit sources properly.

7. Scams & Misinformation

- Remain vigilant about AI-generated and other types of scams, phishing attempts, or fraudulent content.
- These may appear as unsolicited messages, deepfake videos, fake social media accounts offering services or impersonating AEP personnel.
- Any suspicious activity must be reported immediately to the IT department or the Social Media Manager.

8. Use of Artificial Intelligence

- Any generation of content on behalf of AEP using Artificial Intelligence (AI) must comply with AEP's GenAI standards for safe and effective use and all other company policies and procedures governing the use of AI.

Additional Reminders

- You are responsible for the content you publish.
- Avoid discussing employment statuses, customer accounts, or vendor contracts on social media.
- Any official representation of AEP on social media must be approved by the Social Media Manager.

By adhering to these guidelines, you can contribute positively to AEP's reputation while protecting both your own and the company's interests.

Employee Commitment

Safe and secure workplace

Engaged, trained & developed employees

Contents

Workplace Safety & Health

Commitment to Zero Harm

- AEP prioritizes the health and safety of employees and customers, aiming for everyone to go home in the same or better condition than they arrived.
- Compliance with health and safety regulations is mandatory, and all personnel must adhere to safety instructions and procedures.

Reporting Unsafe Conditions

Employees can report unsafe conditions through:

- AEP Hazard Line: 1-888-AEP-ASAP (1-888-237-2727)
- Local Manager
- AEP Concerns Line: 1-800-750-5001 or online at aepconcernsline.com

Report an incident ⟶

COMMITMENT & APPROACH

AEP's commitment is to ensure everyone goes home safely, driving the implementation of protective measures.

Key strategies for achieving safety include:

1. Fostering a commitment to a safe and healthy workplace
2. Involving all employees in a trusting and respectful environment
3. Integrating safety into operations and work procedures
4. Engaging employees through leadership interactions
5. Leading with purpose to reinforce safe behaviors
6. Holding each other accountable for safety

Safety Measures

AEP is committed to embedding layers of protection, including:

- Preventing serious injuries and fatalities
- Strengthening pre-job briefings
- Learning from safety incidents
- Providing targeted training and education
- Enhancing proactive safety initiatives and data analysis

Safety & Health Philosophy

- Health and safety are central to AEP's operations, harmonizing customer needs with environmental protection

ACTIVE ENGAGEMENT

AEP encourages active participation and leadership from all employees to create a safe and secure workplace, supporting overall safety and health goals.

Physical Security

All employees share the responsibility for maintaining a safe and secure workplace

Employees should:

- Stay vigilant and report suspicious activities or security incidents.
- Follow security protocols, such as using access badges properly and securing sensitive areas.
- Adhere to visitor management procedures.
- Avoid tailgating and do not allow unauthorized access through secured doors.
- Report lost or stolen badges immediately.

Active participation in physical security helps protect people, property, and information, promoting a culture of safety, integrity, and accountability.

MANDATORY SELF REPORTING

Our Values

Employees must report certain events within 24 hours to their immediate supervisor or the Employee Service Center:

1. Any arrest, charge, indictment, or conviction of a felony or misdemeanor (excluding minor traffic offenses).
2. Service of a protection or restraining order when the employee is the subject.

Supervisors receiving such reports should contact the Employee Service Center for further guidance.

Report security incidents to AEP Security either online or by calling:

SECURITY HOTLINE
1-866-747-5845

AUDINET
8-200-1337

AVAILABLE
24/7

Culture & Inclusion

AEP'S COMMITMENT TO INCLUSION & RESPECT IN THE WORKPLACE

Our Values

- AEP is dedicated to creating a diverse and inclusive workplace where all employees feel respected, valued, and connected.
- We serve diverse communities and customers, and our workforce must reflect that diversity.

Zero Tolerance Policy

- Discrimination and harassment of any kind will not be tolerated.
- Employment decisions (hiring, training, promotions, etc.) are made without regard to:
  - Race, color, religion, sex (including pregnancy, gender identity, and sexual orientation)
  - National origin, age, veteran/military status, disability, genetic information
  - Any other basis prohibited by law

Employee Expectations

- Conduct yourself in a way that supports a healthy, safe, and productive work environment.
- Support AEP's inclusive culture and follows the Rules of Conduct in the Employee Handbook.

Inclusion at AEP

- We value the unique talents, perspectives, and experiences of every employee.
- Differences are a positive influence on our ability to serve stakeholders effectively.

DID YOU KNOW?

Discrimination is the denial of normal privileges or rights based on protected characteristics.

Employee Resource Groups (ERGs) are voluntary, employee-led collectives formed around shared identities, interests, or life experiences. These groups are open to all employees who are interested in connecting, learning, and contributing to a more inclusive workplace. To join an ERG, employees can express interest through the internal ERG page on AEPNow or reach out directly to ERG leaders.

Benefits of joining an ERG include:

- Fostering acceptance, camaraderie, and equity across diverse groups
- Boosting visibility and support for underrepresented communities
- Enhancing employee performance and sparking innovation
- Offering leadership and talent development opportunities
- Educating peers and leadership on relevant social and cultural issues
- Creating spaces to network, socialize, and raise awareness

TELL ME MORE

AEP has nine ERGs which include:

ADAPT
Abled and Differently-Abled Partnership

AAEP
Asian American Partnership

BERG
Black Employee Resource Group

EP|C
Empowered Parents and Caregivers

HOLA
Hispanic Origin Latin American

MVERG
Military Veteran Employee Resource Group

PRIDE ERG
LGBTQ+ Employees and Allies Group

Women @ Work ERG
All Employees Resource Group

Human Rights Policy

At AEP, our most important job is to deliver safe, reliable, and affordable electric service to our customers. We strive to do more than keep the lights on; our mission is to positively impact the lives of our employees, customers, and communities while strengthening local economies. This includes ensuring the dignity, wellbeing, and fair treatment of all people without discrimination.

AEP defines human rights as rights inherent to all human beings without distinction of any kind, including race, color, religion, sex (including pregnancy, gender identity, and sexual orientation), national origin, age, veteran or military status, disability, genetic information, or any other basis prohibited by applicable law.

DID YOU KNOW?

Human Rights Include

Discrimination & Harassment
Protection against unfair treatment

Freedom of Association & Collective Bargaining
Rights to organize and negotiate

Safe & Healthy Workplace
Commitment to employee safety and health

Workplace Security
Ensuring a secure work environment

Forced Labor, Child Labor & Human Trafficking
Prohibition of exploitative practices

Work Hours, Wages, & Benefits
Fair compensation and working conditions

Environmental Responsibility & Social Justice
Commitment to sustainability and equity

Community & Stakeholder Engagement
Involvement with local communities and stakeholders

Learn more on the Human Rights Policy →

Workplace Conduct

Zero Tolerance: Harassment of any kind is not tolerated

How to Maintain Integrity in the Workplace

1. **Do the Right Thing:** Make ethical choices consistently.
2. **Value Differences:** Appreciate diverse perspectives and contributions.
3. **Treat with Respect:** Avoid actions that may be perceived as intimidation or bullying.
4. **Be Mindful:** Recognize that humor or behavior acceptable to you may offend others.

WAYS OF WORKING

Be A Team Player

- Collaborate and share
- Get to "yes"
- Be open to diverse perspectives

UNDERSTANDING HARASSMENT

Harassment is defined as conduct that is intimidating, offensive, demeaning, or hostile, and that unreasonably interferes with work.

Examples include:

- Racial jokes or insults: Making fun of someone's race
- Unsolicited opinions on sexual orientation: Sharing inappropriate comments
- Teasing about religious beliefs: Making fun of someone's faith
- Unwelcome sexual advances: Any unsolicited sexual interaction
- Disparaging nationality remarks: Making negative comments based on nationality
- Sexually explicit gestures or posters: Displaying inappropriate materials

Workplace Bullying

- Repeated mistreatment causing harm or distress
- Includes verbal abuse, exclusion, intimidation, and sabotage
- Hurts morale, productivity, and mental health
- May violate harassment laws if targeting protected traits

Horseplay

- Rough or playful behavior not suited for work
- Examples: pranks, throwing objects, physical antics
- Creates safety risks and disrupts workflow
- Often violates conduct and safety policies
- Should be addressed immediately by supervisors

Report through proper channels; retaliation is prohibited

Workplace Professionalism

Workplace professionalism sets expectations for employee behavior, focusing on integrity, respect, and appropriate conduct to foster a positive and productive environment. Key aspects include respectful communication, adherence to dress codes, effective problem-solving, honesty, and responsible use of company resources.

DID YOU KNOW?

Benefits of Workplace Professionalism

Positive Work Environment
Cultivates a culture of respect, trust, and cooperation

Ethical Standards
Provides a framework for ethical decision-making

Enhanced Productivity
Clear expectations help employees focus on their work and goals

Fairness
Ensures consistent treatment and equal opportunities for all employees

Professional Business Attire

All AEP employees may wear casual business attire that is appropriate for their particular job.

- When employees are in contact with representatives of government agencies, community groups, other companies, customers of the company, and official guest, they should wear traditional business attire.
- If an employee has doubt regarding appropriate attire for their work environment, the employee should discuss it with their supervisor and/or work team.

Learn more about Professional Business Attire ⟶

Travel

GUIDELINES FOR TRAVEL

The AEP Travel Policy provides employees (authorized to travel on the company's behalf) with reasonable transportation, lodging, meals and other services necessary to conduct official business. This policy applies only to travel expenses. The company's policy is also to reimburse employees for all reasonable expenses they incur on business in a timely manner.

Good Judgment
- Employees should exercise good judgment and fiscal responsibility during travel.

Management Approval
- Obtain prior management approval for any expenditures not explicitly covered in the policy.
- Exceptions to the policy require prior approval from the immediate supervisor.

Manager's Responsibility
- Managers must ensure that traveling employees are aware of and comply with this policy.

Employee Definition
- The term "employee" includes both employees and contractors directed to travel on company business.

Employees must use the corporate credit card and the AEP travel department for all business travel arrangements.

CONDUCT EXPECTATIONS

Representation
Employees represent AEP while traveling, including after-work hours.

Conduct Standards
All expectations for appropriate conduct remain in effect during travel.

For any questions regarding business travel, employees should contact Workplace Services at 200-6840 or 614-716-6840

Regulatory & Legislative Integrity

Balanced regulatory outcomes

Trusted industry leadership

Contents

Regulatory & Legislative Integrity

FERC Standards of Conduct & Affiliate Restrictions

Purpose

To prevent the passing of nonpublic market information between AEP's franchised public utilities (serving captive customers) and its market-regulated power sales affiliates (competitive affiliates).

KEY PROVISIONS

1. Separation of Functions

- **Transmission and Marketing**
  Employees in transmission functions must operate independently from marketing function employees. This includes prohibiting the sharing of non-public transmission information.
- **Physical and Electronic Separation**
  Transmission and marketing personnel are physically separated and do not have access to each other's facilities or information. Market-regulated power sales affiliate personnel are also kept separate from employees of franchised public utilities.

2. No Conduit Rule

- Service Corporation employees providing services to both operating companies and competitive affiliates may come into contact with market information, provided they do not pass this information inappropriately.
- Similarly, employees serving both transmission and marketing functions must not share transmission function information with marketing function employees.

Definitions

Transmission Functions

Involves planning, directing, and managing day-to-day transmission operations, including service request management.

Marketing Functions

Involves the sale or resale of electric energy or capacity, demand response, and related transactions in interstate commerce.

Employees

"Marketing function employees" and "transmission function employees" are those actively engaged in these respective functions on a daily basis.

Market Regulated Power Sales Affiliates

Competitive affiliates of a franchised public utility that sell power for resale at market rates.

Compliance & Responsibility

AEP ensures compliance with these regulations through the coordinated efforts of all transmission, energy marketing, and shared services employees. Employees are expected to adhere to these guidelines strictly to maintain compliance with FERC regulations.

WAYS OF WORKING

Be An Owner

- Manage the details
- Set high standards
- Be accountable

Political Engagement

AEP promotes a respectful, lawful, and inclusive environment regarding political activities. Employees are expected to comply with these guidelines to maintain the integrity of the organization while participating in civic duties.

AEP Political Engagement Policy Overview

Purpose

To meet customer expectations by participating in the policy-making and political process with government officials and stakeholders.

Compliance

All corporate political activities must adhere to the AEP Political Engagement Policy, which exceeds basic legal requirements for transparency.

Key Components

Political Participation

AEP engages in lobbying at national, state, and local levels, where legally permitted. Corporate funds may be contributed to candidates, parties, and political organizations aligned with AEP's business interests, provided there is no expectation of official acts in return.

Contributions and Corporate Resources

All corporate political contributions must comply with the AEP Political Engagement Policy. Use of corporate resources for political activities must be reviewed and approved by the Chief Compliance Officer – Political Engagement before any event is planned. Non-AEP entities using AEP space for political events must pay for the space and associated services in advance.

Disclosure and Transparency

AEP discloses corporate political contributions in accordance with laws and regulations. Additional disclosures are made through the company website and the Corporate Sustainability Report to inform stakeholders of political participation.

Oversight

All corporate political contributions require approval from AEP Legal and executive management.

Compliance

AEP has established policies and compliance measures to ensure adherence to legal and regulatory requirements.

Employee Guidelines

Encouragement of Participation

Employees are encouraged to engage in political and civic duties, provided they fulfill their job responsibilities and avoid conflicts of interest.

Disclosure for Officeholders

Employees seeking political office must disclose their position in the annual Conflict of Interest Disclosure and ensure their political role does not interfere with their AEP responsibilities. They should differentiate personal opinions from the company's representation.

Political Attire

Employees should refrain from wearing attire or displaying materials that could be perceived as campaigning for any candidate or political party in the workplace.

TELL ME MORE

Definition of a Government Official Under the Political Engagement Policy

Government Employees

- Any official, officer, employee, or representative of a governmental entity, which includes federal, state, local, or municipal departments or agencies.
- This includes individuals who are elected, appointed, retained, or otherwise employed in a governmental capacity, particularly when their role involves oversight or influence over AEP's interests.

Entities Controlled by Government Officials

- Any company, business, enterprise, or other entity that is owned, in whole or in part, or controlled by a person described above.

Political Parties and Candidates

- Any political party, party official, or candidate running for political office.

SCENARIO

PLANT MANAGER AND THE SCHOOL LEVY SITUATION

The local school district has a levy on the ballot, and the plant manager wants to contribute company money to support it.

Response

- A school levy qualifies as a "ballot issue," making any contribution a Corporate Political Contribution.
- Therefore, the plant manager cannot make this contribution without prior approval.
- The contribution must receive approval from AEP Legal and executive management before any funds are allocated.

Summary

Adherence to the AEP Political Engagement Policy is essential to maintain compliance and avoid conflicts of interest.

Definition of Social Welfare Organization

A Social Welfare Organization is defined as an organization operating under section 501(c)(4) of the Internal Revenue Code.

Examples Include:

- Human Rights Campaign
- Economic Development Corporations
- Civic Organizations: Such as Rotary and Lions Clubs
- Volunteer Fire Departments
- AARP

Importance

Understanding the guidelines and requirements for contributing to these organizations is essential for compliance with AEP policies.

DID YOU KNOW?

AEP is committed to transparency regarding contributions to Social Welfare Organizations in accordance with the Political Engagement Policy.

Here are some key points:

Disclosure

AEP discloses contributions of corporate funds or in-kind services to Social Welfare Organizations.

Approval Process

All contributions must receive approval from both AEP Legal and executive management before they are made.

Antitrust

Antitrust Laws & Compliance

Antitrust laws are essential for maintaining a competitive and fair market. All employees must ensure that their business practices adhere to both state and federal antitrust laws.

Is it OK to discuss our safety culture and our strategy for expanding into new markets?

Sharing safety practices is encouraged as it helps enhance workplace safety across the industry.

However, discussing specific details about AEP's product and geographic strategy could violate antitrust laws.

General discussions about AEP's corporate strategy are permissible, but it's best to consult with AEP Legal if there are any uncertainties.

Topics to Avoid When Engaging with Competitors

To comply with antitrust laws, you should never engage in the following activities with competitors:

Price Discussions
Avoid any discussions about pricing, including fees, surcharges, or discounts.

Terms and Conditions
Do not discuss terms of sale or purchase agreements.

Cost Information
Do not share information regarding costs.

Profit Margins
Avoid discussing profit margins.

Employment Practices
Refrain from discussing hiring or employment practices.

Sales or Marketing Plans
Do not share specific sales or marketing strategies.

Bidding Plans
Avoid discussions about bidding amounts, strategies, or potential outcomes.

Destroying Competition
Do not engage in practices like below-cost pricing aimed at harming competitors.

Boycotting
Avoid discussions about boycotting customers, suppliers, or competitors.

Additional Precautions

Intermediaries
Never use customers or any third party to exchange sensitive company information with competitors.

Reporting Concerns
If you suspect that sensitive information is being shared improperly, contact AEP Legal immediately.

Maintaining compliance with antitrust laws is crucial for protecting both the company and its employees.

Environmental Respect

Creative sustainable solutions

AMERICAN ELECTRIC POWER

Contents

Protecting the Environment

At AEP, we recognize that our operations have a direct impact on the communities we serve and the natural resources we all depend on. Protecting the environment is not just a regulatory requirement—it is a core expectation of every employee and a reflection of our commitment to sustainability and responsible business practices.

What This Means for You

Comply with Environmental Laws and Policies

Follow all applicable environmental regulations and AEP's internal policies and processes designed to safeguard air, water, land, and wildlife.

Prevent Pollution and Minimize Waste

Take steps to reduce emissions, conserve energy, and properly manage waste in your daily work.

Report Environmental Concerns Promptly

If you see a spill, release, or any activity that could harm the environment, report it immediately.

Support Continuous Improvement

Look for opportunities to make processes more sustainable, whether through innovation, efficiency, or collaboration.

Why It Matters

Our customers, regulators, and communities trust us to deliver reliable power while protecting the environment for future generations. Every decision you make—large or small—contributes to that trust.

Operational Excellence

World-class asset performance

Contents

Confidential Information & Privacy

Confidential Information and Privacy Guidelines

Overview

AEP is committed to protecting confidential information and ensuring data privacy across all operations. Every employee plays a critical role in maintaining these standards.

CONFIDENTIAL INFORMATION

What It Is

Includes business strategies, financial data, proprietary systems, and any non-public information.

Your Role

- Protect access to AEP funds, property, and sensitive data.
- Prevent unauthorized disclosure or misuse of confidential information.
- Report any suspected breaches immediately.

Privacy Policy

- AEP complies with all applicable privacy and data protection laws.
- Personal information is collected and used only for legitimate business purposes.
- Use of personal data is limited to what is adequate, relevant, and necessary.

Employee Responsibilities

- Understand and follow AEP Internal Privacy Policy.
- Handle PII (e.g., names, SSNs, contact details) with care and discretion.
- Ensure data is stored, accessed, and shared securely.

Key Takeaways

Ethical handling of confidential and personal information protects AEP's reputation and legal standing. You are responsible for knowing and applying AEP's privacy and security policies in your daily work.

For further details on specific obligations and policies, please refer to the relevant documentation or contact your supervisor or AEP Legal.

TELL ME MORE

What is considered confidential information?

- Engineering and other technical data
- Financial data, including actual and projected earnings and sales figures
- Planned new services and products
- Advertising and marketing programs
- Actual and proposed business plans and strategies
- Customer and supplier lists and information, including contract provisions and pricing
- Capital investment plans
- Product configuration, component specifications, logic diagrams, and technical drawings
- Test data
- Trade secrets, including methods, programs, and processes
- Employee information, including personal information and organizational charts

What to Do: Guidelines for Handling Confidential Information

Know and Comply

Familiarize yourself with and adhere to all applicable privacy and data protection laws, policies, and procedures relevant to your role.

Maintain Confidentiality

Always respect and safeguard the confidentiality and security of personal information collected by or for the company.

Limit Data Access

Never collect or attempt to access personal information about employees, customers, or business partners unless it is necessary for your job responsibilities. Additionally, do not retain such information longer than required.

By following these guidelines, you contribute to the overall security and integrity of the company's data and privacy practices.

SCENARIO

Situation

A customer begins reading their full Social Security Number during a call. The representative repeats the full number back, violating policy that only the last four digits should be used.

Outcome

The call is reviewed, the rep receives coaching, and they are reminded to stop customers from sharing unnecessary sensitive information.

TELL ME MORE

Personally Identifiable Information (PII)

Definition

Personally Identifiable Information (PII) refers to any information that can identify an individual (the "Data Subject"). It does not include de-identified data, aggregated data, or public information. PII can exist in various formats, including electronic, paper, or other forms, and may also be referred to as personal information or personal data.

Examples of PII:

- Social Security Number
- Driver's License Number
- State or Federal Government Issued ID Number
- Passport Number
- Financial Information: This includes credit card numbers, bank account details, or any other financially sensitive information.

While these are considered "classic" examples of PII, it's important to note that in certain jurisdictions, additional types of information may also qualify as PII and should be treated accordingly.

For any questions or concerns regarding the classification of specific information as PII, consult AEP Legal for guidance.

Cybersecurity Intelligence & Defense

The Cybersecurity Intelligence and Defense team is tasked with safeguarding AEP from a variety of cybersecurity risks and threats.

Their responsibilities include:

Monitoring & Managing Cybersecurity Risks
Continuously observing and managing potential vulnerabilities and threats to AEP systems.

Mitigating & Investigating Cyber Threats
Responding to cyber incidents and investigating any potential breaches or attacks.

Responding to Cyberattacks
Taking immediate action to address and remediate any cyber incidents affecting the enterprise.

Reporting
Providing detailed reports on cybersecurity risks, threats, and incidents.

AEP Assets Come with the Following Legal Notice

This system is for AUTHORIZED USERS ONLY and only for uses permitted by AEP policies. By using this system, each user acknowledges and accepts the following:

All of the users activities on the system may be monitored and recorded.

This system and its contents are owned by AEP.

Because the system is monitored, users have no expectation of privacy with regard to use of the system.

Use of the system for personal matters that the user may otherwise consider confidential, such as Attorney/Client communications with the user's personal attorney, may result in a waiver of confidentiality and the Attorney/Client privilege.

At any time and any lawful purpose, AEP may monitor, intercept, record in real time, and search any communications or data transiting, traveling to or from, or stored on this information system, and may disclose such communications or data to the U.S. Government and its authorized representatives.

Any use of the system that violates any Company policy or any law may subject the user to discipline, up to an including termination, by the Company and/or prosecution by law enforcement officials.

KEY FUNCTIONS

Security Data Analytics
Analyzing security data to identify patterns and potential threats.

Insider Threat Detection & Response
Monitoring for and responding to threats originating from within the organization.

Threat Intelligence Analysis
Gathering and analyzing information about potential cyber threats.

Proactive Threat Hunting
Actively searching for vulnerabilities and threats before they can cause harm.

Collaboration
Working with industry peers and U.S. Government partners to share and gather threat intelligence.

Enterprise Security Technology Management
Overseeing security technologies to protect AEP infrastructure.

Multi-Factor Authentication Administration
Implementing and managing authentication technologies to enhance security.

Forensics & Electronic Discovery
Assisting Human Resources, Ethics & Compliance, and AEP Legal with investigations through forensic analysis.

SPECIALIZED PROGRAMS

Insider Protection & Prevention Program (IP3)
Focused on preventing and responding to insider threats.

24x7x365 Cybersecurity Desk:
A dedicated team that leads all cybersecurity and insider threat incident response activities for AEP.

This proactive and comprehensive approach ensures that AEP endpoints, users, and systems are well-protected against a wide array of cyber threats, both on-premise and in the cloud.

Phishing

Three Primary Phishing Threats

1. Malicious Links

These links direct you to imposter websites designed to steal your information and may also infect your device with malware.

2. Malicious Attachments

Attachments can compromise your computer when opened, potentially leading to data breaches or malware infections.

3. Requests for Sensitive Data

Phishing attempts often prompt you to provide sensitive information such as user IDs, passwords, financial information, etc., which can then be stolen by attackers.

Being aware of these threats is crucial for protecting your personal and organizational information from phishing attacks. Always verify the source of any communication before clicking links, opening attachments, or providing sensitive information.

Phishing Awareness Program

To enhance AEP's defenses against malicious cyber threats, participation in an ongoing Phishing Awareness program is mandatory for all staff, including employees and contractors.

Key Points to Note:

- **Phishing Awareness Program**
  All staff must engage in this program to improve their ability to recognize and respond to phishing attempts.
- **Email Phishing Accountability Policy**
  Employees are encouraged to review this policy to understand their responsibilities and the potential consequences of phishing incidents.

Email Phishing Accountability Policy →

Consequences of "Failing" the Phishing Awareness Test

Employees who click on embedded links, open attachments, or forward test emails outside of AEP during phishing tests will be considered to have "failed" the test.

Consequences for failing a phishing test are outlined in the phishing accountability policy.

Read & Think Before You Click

Watch For:

Misspellings and poor grammar
Many phishing emails contain errors that can be a red flag.

Messages that don't seem quite right
Trust your instincts; if something feels off, investigate further.

Unsolicited emails
Be cautious with emails from unknown senders or unexpected messages.

Ask Yourself:

Was I expecting this message? If you weren't expecting communication from the sender, be skeptical.

Does this email make sense? Consider whether the content aligns with your knowledge or expectations.

Am I being pushed to act quickly? Phishing attempts often create a sense of urgency to trick you into acting without thinking.

Does this seem too good to be true? If an offer appears too favorable, it could be a phishing attempt.

What if this is a phishing email? Always consider the possibility that the email may be malicious. If in doubt, do not click any links or open attachments.

HOW TO RECOGNIZE AND AVOID PHISHING

Treat External Emails as Potential Risks
Always consider emails from external sources containing attachments or links as potential phishing threats.

Look for Warning Indicators
External emails will include the word "External" in the subject line. Additionally, there is often a brightly colored banner at the top of the content area in most external emails.

Exercise Caution with Attachments and Links
DO NOT open attachments or click on links from untrusted or questionable sources. This is a common tactic used in phishing attacks.

Report Suspicious Emails
If you encounter an email that seems suspicious, click the Report to Incidents button in your Outlook Ribbon to forward the email to incidents@aep.com for review.

By following these guidelines, you can help protect yourself and the organization from phishing attempts and other cyber threats.

NERC Standards

YOUR ROLE IN SECURITY AT AEP

As an AEP employee or contractor, you play a vital role in protecting your colleagues and the company's assets.

Your responsibilities:

- Safeguard your computer credentials
- Stay alert to suspicious activity near AEP facilities
- Responsibly manage information you share—both personal and work-related

WHAT IS NERC CIP?

NERC - The North American Electric Reliability Corporation is a regulatory authority responsible for ensuring the reliability and security of the power grid in the U.S., Canada, and parts of Mexico.

CIP - Critical Infrastructure Protection standards focus on safeguarding the physical and cyber assets that are essential for the operation of the Bulk Electric System (BES).

Compliance with NERC Standards

AEP is subject to NERC Standards, which establish extensive requirements for securing utility infrastructure and implementing specific information management policies. It is essential to adhere to these standards to maintain operational integrity.

Reporting Suspicious Events

AEP is required to report any incidents of sabotage

- All employees and contractors must promptly report suspicious activity to the Security team.
- The Physical Security and Cybersecurity teams will investigate all reports of suspicious activity to determine whether sabotage has occurred.
- Visit the Security page where you can find more information on the NERC Reliability Standards.

Do Your Part

Secure Personal & Company Property

Ensure all personal items and AEP assets are properly secured. Lock your desk whenever it is unattended.

Practice Safe Travel Habits

When traveling, store laptops and other valuables out of sight within your vehicle to reduce the risk of theft.

Lock Vehicles When Unattended

Always lock your vehicle, even if stepping away briefly.

Lock Your Computer

Use password protection and lock your computer every time you leave your desk.

DID YOU KNOW?

If you work in or have access to a NERC CIP-designated location, you must comply with stringent security standards:

Unescorted Access
Enter a NERC CIP-restricted area only if you have approved unescorted access.

Logging In and Out
If entering with an escort, you must log in and out each time you enter or leave the location.

Escort Responsibilities
If you are escorting someone into a NERC CIP restricted area, understand your responsibilities.

Security Hotline
When in doubt, call the Security Hotline at 1-866-747-5845 (Audinet 8-200-1337).

SCENARIO

NERC CIP ESCORT REQUIREMENTS

Scenario
I have a new employee who has not yet received NERC CIP access. They are currently working on training and other non-CIP-related projects. I need to leave the restricted area for a meeting and would like them to remain and continue working until I return.

Clarification
This is not permitted. If you are escorting someone into a NERC CIP area, you must accompany them at all times and log them out when you leave. Leaving them unattended, even briefly, violates escorting requirements under NERC CIP standards.

Content Governance

Records Management and Retention at AEP

Laws, regulations, and AEP policies dictate the management of records, including which records must be retained, how they are to be managed, and the duration for which they must be kept. A consistent approach to content governance is essential for mitigating risk.

AEP Retention Schedule

The AEP Retention Schedule outlines how records are classified and handled in accordance with the AEP Security Data Classification Guidelines. It's crucial to follow this schedule to ensure compliance and proper management of records.

Important Note
A LEGAL HOLD takes precedence over any retention requirements specified in our record retention policies. If you have questions about the disposition of a particular document, please reach out to AEP Legal.

DID YOU KNOW?

When your employment at AEP ends—whether through retirement, resignation, or termination—keep the following in mind:

Monitoring of Data Transfers
Mass data transfers and the use of removable disks are monitored by IT Security.

Unauthorized Removable Disks
DO NOT use unauthorized removable disks or similar items to download contents from your workstation or server.

Personal Information
If you have personal information on your workstation (e.g., photos or documents), contact Ethics & Compliance before removal to obtain the necessary authorization.

Legal Hold

Information to Preserve Under a Legal Hold

If you are placed under a Legal Hold, you are required to preserve the following types of information:

Personal Devices
Any relevant information stored on personal devices such as cellphones, computers, tablets, and thumb drives.

Hard Copy Files
Physical documents that may be relevant to the case.

Company Devices
Information stored on company-issued devices, including cell phones and laptops.

Physical Evidence
Any tangible items that may serve as evidence, such as broken poles, tampered meters, or other physical evidence related to the case.

Importance of Compliance

It is crucial to adhere to a Legal Hold to ensure that all relevant information is available for legal proceedings. Failure to comply can lead to legal repercussions for both the individual and the organization.

TELL ME MORE

What is a Legal Hold?

A Legal Hold is a formal notification issued by an organization's legal team directing employees to preserve all relevant information, including electronically stored information and hard copy documents, that may be pertinent to a current or anticipated legal dispute or lawsuit.

Enterprise Policies

Understanding Enterprise Policies

Purpose of Policies
Policies serve as guiding principles or courses of action adopted by the organization. They establish general rules and shared values that help achieve company goals and objectives.

These *Principles* align with and reference key AEP corporate policies, which are available through AEP Policy Hub. AEP Policy Hub provides more detailed guidance than what is outlined in the *Principles* and may include additional policies not covered here. Employees should always consult the AEP Policy Hub for comprehensive information. The AEP Policy Hub can be accessed through ARCS.

Definition of an Enterprise Policy
A policy is considered an Enterprise Policy if it governs the activities of any employee or contractor outside the direct reporting structure of the policy owner.

Review and Approval Process

All enterprise policies must go through a formal review and approval process outlined in the AEP Enterprise Policy Development and Maintenance Policy.

Annual Review Requirement
Each enterprise policy must be reviewed annually by the policy owner to ensure it remains relevant, effective, and aligned with organizational goals.

Learn more about Enterprise Policy development →

AEP Policy Hub

AEP Policy Hub, an ARCS's centralized policy management platform, streamlines version control and the approval process in alignment with the Enterprise Policy Development and Maintenance Policy.

- One-stop shop for all policy-related needs
- Each business unit should have a policy liaison
- All policies should be reviewed annually by policy owner
- All employees can access via AEPNow

Financial Strength

Strong financial discipline

Contents

Financial Records & Reporting

We all share responsibility for accurate reporting and recordkeeping. The AEP Speak Up Policy requires you to immediately report any suspected fraud to an appropriate member of management, Audit Services, Ethics & Compliance, AEP Legal, or Human Resources. Suspected fraud can also be reported confidentially and anonymously through the AEP Concerns Line at 1-800-750-5001.

INTERCOMPANY TRANSACTIONS

The company's regulated subsidiaries are governed by laws and regulatory rules that are intended to prevent cross-subsidies and to avoid the misstatement of expenses and earnings. Contact AEP Accounting or AEP Legal for assistance with these laws and rules.

SEC REPORTING

All AEP employees participating in the preparation of reports or documents filed with or submitted to the Securities and Exchange Commission (SEC) or engaging in public communications made on behalf of AEP shall endeavor to ensure full, fair, accurate, timely and understandable disclosures.

What to Do

Accurate Record Keeping

Be sure that the information you prepare, process, and analyze:

  - Is accurate and thorough
  - Complies with applicable laws, accounting principles, and company policies

- Never falsify, try to hide, or mischaracterize an AEP record.
- Never attempt to bypass any company procedure or control, even if you think it would be harmless, or save time.
- Always cooperate with external and internal auditors, and investigators.
- Be familiar with and follow company policies and procedures regarding business records, including requirements to keep and delete or discard business records.
- Never destroy records to avoid disclosure in legal proceedings or investigations, and comply with any notice from AEP Legal that requires you to retain records.

WAYS OF WORKING

Get Stuff Done

- Measure success by impact, not effort
- Act with urgency
- Make things better

Insider Information & Trading Activities

Insider Trading at AEP

AEP stock is registered with the Securities and Exchange Commission (SEC), enabling public trading. This registration obligates the company to maintain the integrity of the market.

INSIDER TRADING AT AEP

Insider trading refers to the trading of company stock based on material non-public information. Such trading is strictly prohibited. Insider information includes any material non-public information that employees, agents, vendors, contractors, or consultants learn through their employment.

Trading Restrictions
Employees are prohibited from buying or selling company stock based on material non-public information until after that information has been publicly released and the market has had time to react.

Disclosure Prohibition
Employees must not disclose insider information to anyone, including family, friends, and acquaintances. Trading on insider information can lead to criminal and/or civil actions against both the trader and the employee who disclosed the information.

For more details, employees should refer to the AEP Insider Trading Policy.

Questions & Answers

Question
Due to my job responsibilities, I often have access to earnings information before it is released. If someone asks me how the numbers look before the SEC filing, is it OK to provide them a general indication of the earnings?

Answer
No, disclosing any material non-public information, including estimates or other types of tip-offs, is prohibited. Such information should only be discussed among employees who have a legitimate need to know and who understand the insider trading rules.

Question
My family and friends sometimes ask me how AEP is doing and if they should buy our stock. I feel the company is doing well, and I am proud to work for AEP, so I recommend that they buy it; is this a problem?

Answer
While it's great to be proud of AEP's accomplishments, to avoid potential issues, it's best to refer them to the Investors tab on AEP.com, where they can find presentations and other investor-related materials.

TELL ME MORE

Examples of Material Non-Public Information

- Judicial or regulatory decisions
- Dividend declarations
- Plans to issue or buy back securities
- Earnings announcements
- Pending acquisitions or mergers
- Joint venture and contract negotiations

What's In Bounds

- Protecting company insider information from those who do not need to know.
- Adhering to SEC regulations and company policies regarding buying or selling AEP stock.

What's Out of Bounds

- Discussing insider information in public places.
- Using or sharing insider information for personal gain.
- Trading in AEP securities while in possession of material non-public information that has not yet been released to the public.

Appropriate Use of Company Assets & Records

USE OF COMPANY ASSETS AT AEP

AEP provides you with the necessary tools and resources to perform your job effectively. While limited personal use of certain company-owned assets is permissible, it's important to adhere to specific guidelines to maintain professionalism and integrity.

Permissible Limited Personal Use

- Occasional personal phone calls and text messages
- Internet use that is not excessive and does not interfere with your job duties

Prohibited Personal Use

- Misuse of company resources: AEP-issued equipment, including computers and software, is intended solely for business-related activities. Using these resources for personal gain—such as operating a side business—violates company policy.
- Work Time Appropriation: Company time should be dedicated to AEP-related responsibilities. Engaging in personal business activities during work hours, regardless of workload status, is inappropriate and may be considered time theft.
- Conflict of Interest: Operating a side business using company resources could create a perceived or actual conflict of interest, especially if the business activities interfere with job performance or company reputation.

Engaging in personal business activities during work hours or using company resources for personal business purposes is strictly prohibited and will result in disciplinary action up to termination.

Examples of potential conflicts:

- **Shopping for personal business supplies or using your AEP computer to look for inventory for your personal business**
- **Corresponding with personal business customers**
- **Maintaining, working on, or storing personal business files on an AEP computer**
- **Using AEP cell phone numbers or email address for personal business contact information**
- **Collecting payments: Picking up payments related to personal rental properties**
- **Working on personal business during AEP work hours**
- **Designing personal business flyers, business cards, brochures, or webpages on AEP assets**

SCENARIO

Personal Business

Facts

An employee operates a side business as a birthday party planner, offering services such as designing invitations, creating party favors and décor, and coordinating site logistics. While the employee has been completing their assigned work ahead of schedule, they have also been using their AEP-issued computer to create flyers for their personal business during work hours.

Is This Acceptable?

No, employees should not engage in personal side businesses during company time or use company resources for such activities. Doing so is a misuse of company time and assets and a violation of company policy. If an employee finds they have additional capacity, they should consult their supervisor to ensure alignment with business priorities.

PUBLIC SERVICE OR CHARITABLE FUNCTIONS

Occasionally, you may be asked to use company tools, equipment, or time for public service or charitable activities.

Examples

- Installing lights at a Little League baseball field
- Using your company computer to present at a United Way meeting

Ensure you fully disclose such activities and obtain prior approval from your manager.

INAPPROPRIATE USE OF COMPANY ASSETS

It is inappropriate to use company assets or perform the following activities during company time:

- **Tax preparation:** Providing tax preparation services for others or for profit
- **Real estate transactions:** Engaging in real estate activities as a landlord or agent
- **Personal business communication:** Sending or receiving messages related to a personal business
- **Using company contact information:** Utilizing company email, phone, or address for personal business purposes

DID YOU KNOW?

Exchanging sexually explicit or profane language with a coworker on Microsoft Teams is a violation of the AEP Prohibition Against Pornography and Offensive Material Policy. Always maintain a respectful and professional environment in all communications.

Prohibition Against Offensive Material

You may never use AEP's assets or network to view, send, store, or print pornographic or other offensive materials.

DID YOU KNOW?

Forwarding a racial or sexist joke on AEP email or messaging systems is a violation of the AEP Prohibition Against Pornography and Offensive Material Policy.

Do not use the AEP system to view/share:

- Pornographic websites
- Websites with inappropriate material
- The Dark Web
- Extremist or Conspiracy websites
- Racist or sexist jokes
- Dating websites or apps
- Personal subscriptions
- Non-AEP personal businesses
- Offensive cartoons and anime
- Weapons or violent crime

AEP actively monitors activities on company-owned assets and networks.

Any of the following can trigger an alert to Cybersecurity which will start an investigation:

- Offensive keywords
- Racial or sexist content
- Sexually explicit imagery
- Pornographic videos, photos, or films
- Excessive use of bandwidth
- Threats of violence
- Sexual or violent content
- Conspiracy or paramilitary
- Illegal drug use
- Sale or construction of weapons or explosives
- Emails or text messages that contain any of the above

Anti-Corruption & Bribery

Anti-Corruption & Bribery Policy at AEP

AEP is dedicated to fostering strong and productive relationships with government officials. To uphold this commitment, AEP requires all employees and representatives to conduct business openly and honestly, exercising the utmost integrity at all times.

Prohibition of Corruption

The AEP Anti-Corruption Policy explicitly prohibits bribery and any forms of corruption.

Providing, offering, promising, or authorizing others—such as lobbyists or political consultants—to give anything of value, whether tangible or intangible, to any individual (including government officials) with the intent to gain an unfair business advantage or improperly influence decisions related to the company is strictly prohibited.

Reporting Requirements

If a government official performs or offers to perform an official act for AEP in exchange for the selection of a vendor or supplier:

- **The request must be reported immediately to AEP's Chief Compliance Officer.**
- **The vendor or supplier involved in the request shall be disqualified from consideration to provide any goods or services to AEP.**

All employees are required to review and understand the Anti-Corruption Policy.

A bribe is never an acceptable cost of doing business.

TELL ME MORE

What can be considered a bribe?

Cash
Gift cards, stocks, bonds, or other items with a monetary value

Gifts
Especially those that exceed a nominal value

Entertainment, Hospitality, and Travel
Any that go beyond reasonable business needs

Food and Beverage
Excessive or lavish meals can be considered a bribe

Personal Services
This includes favors or loans that may create a conflict of interest

Offers of Employment
Providing jobs to influence decisions

Charitable or Political Contributions
Contributions made to sway decisions or gain favor

Awarding of Contracts or Business
Giving contracts in exchange for favors

Payments or Benefits
Any services provided for family members or acquaintances, including job offers

Breakfast Reception

Question

The State Senate Chief of Staff asked you if he could use the company's suite for a staff appreciation event at the arena for the upcoming NCAA men's basketball tournament?

Answer

The value of the suite and associated tickets are likely beyond a nominal value and would not be a permissible gift.

Question

The company would like to sponsor a breakfast reception for Legislators during the State Legislative Session. Other companies will be sponsoring various other events during the session. The breakfast will provide networking and educational opportunities for employees and legislators.

Answer

You should check with AEP Legal and confirm that the sponsorship was approved and disclosed as required under the **Political Engagement Policy.**

WHAT TO DO TO AVOID BRIBERY & CORRUPTION

Know and Follow Policies
Familiarize yourself with AEP's anti-corruption policies and relevant anti-corruption laws. Remember that many anti-bribery laws have severe penalties and apply globally.

Never Ask for or Accept a Bribe
Maintain integrity by refusing any offers of bribery.

Supervise Third-Party Associates
Exercise caution and follow AEP policies and procedures when retaining third-party business associates, ensuring their activities are properly supervised.

Do Not Encourage Illegal Actions
Never ask others to do something that the law or AEP policies prohibit you from doing.

Accurate Record Keeping
Ensure that all payments, benefits, or favors are fully, honestly, and accurately reflected in the company's books and records. Avoid any attempts to conceal or misrepresent payments or expenditures.

Seek Guidance
If you have questions or concerns about bribery laws, AEP policies, or whether a gift or payment may be unlawful or inappropriate, contact AEP Legal for assistance.

Fraud

The false representation or concealment of a material fact with the intent of personal gain or to improve the company's image or standing. This includes intentionally preparing or submitting financial statements that misrepresent the company's status, even without direct benefits to the employee.

Examples of Fraudulent Activities:

Forgery
Altering any document or account belonging to the company, including checks and financial documents

False Representation
Misrepresenting facts to misappropriate funds, securities, supplies, or other assets

Improper Handling of Finances
Inappropriate handling or reporting of money or financial transactions

Profiting from Insider Knowledge
Gaining benefits from insider information or company activities

Disclosure of Confidential Information
Intentionally revealing confidential information

Misrepresentation of Accounting Records
Falsifying accounting records or journal entries that misrepresent financial statements

Time Fraud
Misrepresentation of hours worked, overtime, or sick time

DID YOU KNOW?

Common examples of fraud include:

- **Misrepresentation of Health Insurance Data**
  Misrepresenting your smoking status or other health details
- **Misuse of Corporate Cards**
  Unauthorized use of corporate credit or fuel cards
- **Theft of Company Assets**
  Unauthorized use of tools, supplies, and equipment
- **Falsification of Time Sheets**
  Misrepresenting overtime or sick time

Reporting Responsibilities

Any employee who witnesses suspected fraud is responsible for immediately reporting it to an appropriate member of management, Audit Services, Human Resources, or Ethics & Compliance.

Conflicts of Interest

Conflict of Interest Policy at AEP

A conflict of interest arises when an employee participates in activities or relationships that benefit them personally but may not align with the best interests of AEP. Such conflicts can adversely affect decision-making, job performance, and loyalty to the company.

Examples of Potential Conflicts of Interest:

Ownership Interests
An employee owning a portion of a business that AEP does business with

Referral for Personal Gain
Referring AEP's customers to another business in which the employee has a financial interest

Consulting Services
Providing consulting services to an AEP customer while employed by AEP

Personal Profit from AEP Assets
Using AEP's assets, such as information, technology, or supplies, for personal profit

Talking It Through: Assessing Conflicts of Interest

Conflicts of interest may not always be clear-cut. If you find yourself in a situation that could lead to a conflict of interest, consider the following questions:

1. **Decision Impact:** Would the situation or relationship affect my decisions at AEP?
2. **Personal vs. Company Interest:** Am I putting my personal interest, or the interest of someone close to me, ahead of AEP's interests?
3. **Embarrassment Factor:** Would I feel embarrassed if someone at AEP knew all the facts of the situation?
4. **Divided Loyalty:** Do I, or does someone close to me, gain anything from my potentially divided loyalty?
5. **Perception by Others:** Would others think that the situation or relationship might affect how I perform my job?
6. **Fair Treatment Concerns:** Would a customer or supplier question whether we treated them fairly?

Conclusion

Recognizing and addressing conflicts of interest is crucial for maintaining integrity and trust within AEP. If you suspect a conflict of interest may exist, it is important to disclose it to your manager or the appropriate compliance personnel to ensure transparency and uphold AEP's ethical standards.

ANNUAL CONFLICT OF INTEREST DISCLOSURE REQUIREMENT

Employees are required to complete an annual Conflict of Interest Disclosure. This disclosure serves as a means for employees to document any relationships they have with other individuals or businesses that could potentially impact their objectivity in performing job duties.

Purpose of the Disclosure

- **Safeguard Ethical Conduct:** The disclosure is a proactive measure that helps ensure ethical behavior in the workplace. It is not a negative action; rather, it is a safeguard that allows Ethics & Compliance to provide guidance tailored to each employee's situation.
- **Objective Review:** Ethics & Compliance will review each disclosure, and every employee will receive specific written guidance regarding their disclosure.

ADDITIONAL STEPS

In addition to completing the annual Conflict of Interest Disclosure:

- **Discuss Conflicts with Supervisors:** Employees are encouraged to have open discussions about any potential conflicts of interest with their supervisors. This dialogue helps foster a culture of transparency and accountability within the organization.

HOW TO AVOID A CONFLICT OF INTEREST

- Be transparent about your outside activities and watch for situations where they might interfere with your work or make it difficult for you to be objective.
- Do not use your position at AEP to benefit yourself, friends or family members.
- Never pursue (for yourself or others) business or corporate opportunities that you learned about in your work at AEP or through the use of company property or information.

EXAMPLES OF A POTENTIAL CONFLICT OF INTEREST

- A family member or friend works for an organization that does business or wants to do business with AEP or competes with AEP.
- You use company resources for your personal benefit or for the personal benefit of someone else.
- You supervise or are supervised (directly or indirectly) by a family member or friend.
- You are offered a gift or entertainment that is excessive or that might influence — or appear to influence — your business decisions.

Gifts & Entertainment

Gifts & Entertainment Policy at AEP

Exchanging gifts and entertainment between AEP employees and customers, suppliers, and business partners can be an acceptable practice that helps build goodwill. However, it is essential to adhere to specific guidelines to avoid any actual or perceived conflicts of interest.

Acceptable Situations for Gifts & Entertainment

- **Occasional Meals & Seasonal Gifts**: Providing or accepting occasional meals, seasonal gifts, and tickets to sporting events may be appropriate in certain circumstances.
- **Travel and Overnight Stays:** Under specific conditions, attending functions that involve travel or overnight stays can be beneficial for maintaining good working relationships with customers or vendors. AEP will, where practical, cover travel expenses for such vendor-sponsored trips, but attendance must be approved by your supervisor.

Required Criteria to Accept Gifts & Entertainment

Before accepting any gifts or entertainment, ensure that it meets the following criteria:

- **Consistency with Good Business Practices:**
  The offer aligns with standard business practices.
- **No Business Inducement:**
  The gift or entertainment cannot be interpreted as a business inducement.
- **Ability to Reciprocate:**
  You should be able to reciprocate the gesture.
- **Public Disclosure:**
  It would not be embarrassing to AEP if the offer were made public.
- **Adherence to Unit Policy:**
  It complies with the specific policies of your business unit.

Considerations

As a general rule, occasional gifts of promotional items or items with nominal value are usually acceptable.

Prohibited Gifts and Entertainment

AEP prohibits the offering or acceptance of gifts or entertainment that may be deemed:

Lacking Business Purpose
Entertainment, hospitality, or travel without a clear business purpose or that exceeds reasonable business needs

Personal Services
Favors, personal services, or loans

Family Benefits
Payments or benefits provided to an individual's family members

Quid Pro Quo
Gifts offered with the expectation of something in return

Lavish or Extravagant
Gifts that are overly lavish or extravagant in nature

Reputational Risk
Gifts likely to reflect negatively on AEP's reputation

Legal Violations
Gifts that violate applicable laws or the policies of either the giver or the recipient

Conclusion

Employees must exercise good judgment when accepting or providing gifts or entertainment. If in doubt about the appropriateness of a gift, consult with your manager or Ethics & Compliance. Gifts that do not meet the outlined criteria should be returned to the donor with an explanation. If the gift is perishable, it should be donated to a charitable organization, and the donor should be notified. By following these guidelines, employees contribute to maintaining AEP's integrity and reputation.

Be mindful, each business unit could have their own limit for accepting gifts and entertainment.

GIFTS FROM VENDORS

Q: The SME has been invited on a private plane to look at a manufacturing project with a vendor?

A: Consult with Ethics & Compliance as there may be multiple factors to consider in a situation like this.

Q: A vendor offers to provide lunch for all employees and contractors after safe completion of a project?

A: In most cases this would be acceptable with managerial approval. If you have questions please call Ethics & Compliance.

DID YOU KNOW?

A gift is considered nominal if it is:

- Infrequent
- Low-value
- Not cash or gift cards
- Too minor to track

Nominal Gift Value
Keep under $75 and consult your manager and Ethics & Compliance for anything over $100.

Examples
- Coffee, snacks, small holiday treats
- Flowers, fruit baskets, books for special occasions
- Promotional items (e.g. pens, shirts, bags, hats, mugs)

Intellectual Property

You must safeguard AEP's confidential and proprietary information, trade secrets, and other intellectual property, which includes copyrights, trademarks, and patents.

Employees must not disclose any information that might compromise proprietary technologies or trade secrets to any unauthorized persons. You also must take reasonable precautions against inadvertently disclosing this information to anyone not authorized to have it.

Just as we expect our intellectual property rights to be protected, we will respect the intellectual property rights of others. You may not intercept, duplicate or gain the intellectual property of others through any means, unless given permission by the intellectual property right holder. Additionally, confidential information provided from outside sources may not be shared until approved by AEP Legal.

DID YOU KNOW?

Ownership Rights

AEP has ownership rights to the inventions, knowledge, and employee work product—collectively known as intellectual property—developed in the course of employees' work, on company time and using AEP assets and facilities. AEP will establish and protect its right to such intellectual property.

Report Concerns

Contents

Ethics & Compliance

MISSION

Support AEP's strong ethical culture and raise awareness of compliance expectations.

Team Structure

- Led by the Chief Compliance Officer
- Includes specialists who conduct investigations, develop training, and engage with employees

Program Goals

- Promote a "Speak Up" culture
- Ensure understanding of policies and procedures
- Foster high ethical standards and legal compliance

Team Structure

- Regular communication with executive and board leadership
- Program adjustments made based on internal needs and external trends

CONCERNS LINE: A PILLAR OF OUR CULTURE

As we evolve through Ways of Working, the Concerns Line remains a key tool for integrity and accountability.

The Concerns Line is more than a reporting tool—it's a foundation for empowerment, inclusion, and shared responsibility.

What Speaking Up Means

Speaking up goes beyond reporting misconduct. This broader view fosters open dialogue and supports our culture of integrity, transparency, and psychological safety.

Leadership's Role

When employees see leaders respond in a supportive manner to concerns—whether raised through the Concerns Line, HR, or direct conversations—it builds trust.

DID YOU KNOW

How anonymity is maintained when you call the AEP Concerns Line?

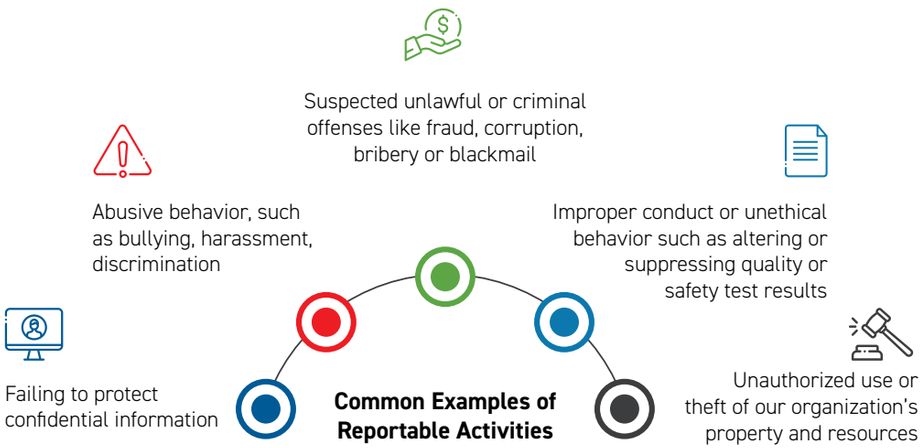
Speaking up goes beyond reporting misconduct. It includes:

- Asking questions
- Sharing ideas
- Raising concerns
- Seeking clarity

When to Report a Concern

Deciding whether to report a concern can be a difficult decision for anyone.

Employees should SPEAK UP when they observe wrongdoing, abusive behavior, illegal activity or policy violation.



How to Report a Concern

- Report to management or Human Resources
- Call the Concerns Line toll free, 24 hours a day at 1-800-750-5001
- **Contact Ethics & Compliance:**
  - 614-716-6226
  - 1 Riverside Plaza, Columbus, OH 43215
  - www.aepconcernsline.com
- **Contact Human Resources:**
  - 1-888-237-2363
  - hr@aep.com

THE CONCERNS LINE PROCESS

Confidential Reporting

- Calls are answered by an independent, 3rd party vendor
  - 1-800-750-5001
- Web intake forms are completed by the employee via Concerns Line portal.
  - www.aepconcernsline.com
- Anonymity is protected when requested.

Investigation

- Collaborate with Business Unit and relevant teams
- Gather background information
- Conduct interviews, review emails and forensic data

Resolution

- Recommend action to Manager, Human Resources, and Business Unit
- Follow up with reporter via phone or portal
- Notify participants when case is closed and address questions

Need Guidance Without Anonymity?

Contact Ethics & Compliance directly:

614-716-6226 or **Audinet 8-200-6226**

Employees, contractors, vendors, and suppliers help uphold a respectful workplace by reporting concerns. Retaliation is strictly prohibited against anyone who reports in good faith a suspected violation of policy, law, or regulation.

Retaliation can take many forms. Below are common examples to help employees recognize inappropriate behavior:

- Demotion or removal from key responsibilities after reporting a concern
- Unjustified negative performance reviews or disciplinary actions
- Termination or forced resignation
- Verbal harassment, intimidation, or exclusion from meetings
- Threats or pressure to withdraw a complaint
- Reassignment to undesirable tasks or shifts
- Attempts to uncover the identity of an anonymous reporter

For more information on retaliation and harassment see the Speak-Up policy. ⟶

If you experience or witness retaliation, report it immediately through the AEP Concerns Line or contact Ethics & Compliance.

To All Employees,

Thank you for taking the time to review AEP's *Principles of Business Conduct*. These standards are more than words on a page—they represent the foundation of our culture and the trust we share with our customers, communities, and each other.
Ethics and compliance are not optional. They are essential to our success and to the integrity of the energy grid we operate. Every decision you make—large or small—has an impact on safety, reliability, and reputation. That's why we expect every employee to act with honesty, fairness, and accountability, and to speak up when something doesn't seem right.

Our commitment to no retaliation is absolute. If you raise a concern in good faith or participate in an investigation, you are protected. We will investigate promptly and fairly, and we will take action to ensure that retaliation does not occur. Your voice matters, and your courage strengthens our company.

Together, we can uphold the highest standards of integrity and deliver on our promise to power a brighter future—safely, responsibly, and ethically.

Thank you for your commitment.

Associate General Counsel, Chief Compliance & Privacy Officer

Kate Krisher