WESTAR

Western States Air Resources Council

Cybersecurity Policy
GA-00-03

Adopted February 9, 2022

Policy brief & purpose

This cyber security policy outlines WESTAR’s guidelines and provisions for preserving our data and technology infrastructure.

The more we rely on technology to collect, store, and manage information, the more vulnerable we become to severe security breaches. Human errors, hacker attacks and system malfunctions could cause great financial damage and may jeopardize WESTAR’s reputation.

For this reason, we have implemented a number of security measures. We have also prepared instructions that may help mitigate security risks. We have outlined both provisions in this policy.

Scope

This policy applies to all our employees, contractors and anyone who has permanent or temporary access to our systems and hardware.

Policy elements

Confidential data

Confidential data is secret and valuable. Common examples are:

- Unpublished financial information

- Personal Identifiable Information (PII) data for WESTAR employees

All employees are obliged to protect this data.

Protect personal and company devices

When employees access WESTAR emails or accounts, they introduce security risk to our data. We advise our employees all to be secure. They can do this if they:

- Keep all devices password protected.
- Choose and upgrade a complete antivirus software.
- Ensure they do not leave their devices exposed or unattended.
- Install security updates of browsers and systems monthly or as soon as updates are available.
- Log into WESTAR financial systems through secure and private networks only.

We also advise our employees to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

When new employees arrive at WESTAR, they will receive instructions for:

- Accessing their WESTAR email account.
- Creating an account for WESTAR's password management system; and
- Installing WESTAR's antivirus/malware software.

Keep emails safe

Emails often host scams and malicious software (e.g., worms.) To avoid virus infection or data theft, we instruct employees to:

- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g., "watch this video, it's amazing.")
- Be suspicious of clickbait titles (e.g., offering prizes, advice.)
- Check email and names of people they received a message from to ensure they are legitimate.
- Look for inconsistencies or giveaways (e.g., grammar mistakes, capital letters, excessive number of exclamation marks.)

If an employee isn't sure that an email they received is safe, they can ask the executive director or business manager.

Manage passwords properly

Password leaks are dangerous since they can compromise WESTAR operations. Not only should passwords be secure so they won't be easily hacked, but they should also remain secret. For this reason, we advise our employees to:

- Choose passwords with at least eight characters, including at least three of the four types of characters, as allowed by the account password rules: capital and lower-case letters, numbers, and symbols. Avoid passwords that can be easily guessed (e.g., birthdays.)
- Remember passwords instead of writing them down. If employees need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.
- Exchange credentials only when absolutely necessary. When exchanging them in-person isn't possible, employees should prefer the phone instead of email, and only if they personally recognize the person they are talking to.
- Change their passwords frequently.

Remembering a large number of passwords can be daunting. WESTAR purchases the services of a password management tool which generates and stores passwords. Employees are obliged to create a secure password for the tool itself, following the abovementioned advice.

Transfer data securely

Transferring data introduces security risk. Employees must:

- Avoid transferring sensitive data (e.g., employee records) to other devices or accounts unless absolutely necessary.
- Ensure that the recipients of the data are properly authorized people or organizations and have adequate security policies.
- Report scams, privacy breaches and hacking attempts

WESTAR's Business Manager and Executive Director need to know about scams, breaches, and malware so they can better protect our infrastructure. For this reason, we advise our employees to report perceived attacks, suspicious emails, or phishing attempts as soon as possible. WESTAR/s Business Manager and Executive Director must investigate promptly, resolve the issue, and send a companywide alert when necessary.

Additional measures

To reduce the likelihood of security breaches, we also instruct our employees to:

- Turn off their screens and lock their devices when leaving their desks.
- Report stolen or damaged equipment as soon as possible.
- Change all account passwords at once when a device is stolen.
- Report a perceived threat or possible security weakness in company systems.
- Refrain from downloading suspicious, unauthorized, or illegal software on their company equipment.
- Avoid accessing suspicious websites.

WESTAR should:

- Install firewalls, anti-malware software and access authentication systems.
- Arrange for security training to all employees.
- Inform employees regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly.
- Follow this policies provisions as other employees do.

WESTAR will have physical and digital shields to protect information.

Take security seriously

Everyone should feel that their data is safe. We can all contribute to a secure working environment by being vigilant and keeping cyber security top of mind.

Approval: _ ___ Marianne J Rossio ___________ Date: __February 9, 2022

Marianne Rossio
WESTAR President