CIMARRON CREATING A CLEANER ENVIRONMENT™	CYBER SECURITY POLICY			
PROCEDURE NUMBER: CIM0020	**REV:**	**ORIGINAL ISSUE DATE:** 04/20//22	**REVISION DATE:**	
PREPARED BY: INFORMATION TECHNOLOGY	**REVIEWED BY:** IT, HR, MANAGEMENT, AND LEGAL	**APPROVED BY:** VP INFORMATION TECHNOLOGY	**APPROVED BY:**	

1.0 PURPOSE

Our company Cyber Security Policy outlines our guidelines and provisions for preserving the security of 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 our company'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.

2.0 SCOPE

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

3.0 POLICY ELEMENTS

3.1 CONFIDENTIAL DATA

Confidential data is secret and valuable. Common examples are:

- Unpublished financial information
- Data of customers/partners/vendors
- Patents, formulas, or new technologies
- Customer lists (existing and prospective)

All employees are obliged to protect this data. In this policy, we will give our employees instructions on how to avoid security breaches.

3.2 PERSONAL AND COMPANY DEVICES

When employees use their digital devices to access company emails or accounts, they introduce security risk to our data. We advise our employees to keep both their personal and company-issued computer, tablet, and cell phone secure. They can do this if they use MFA (multi-factor authentication) to all Microsoft 365 resources as well as encourage MFA for other services where available. 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 company accounts and 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 hires receive company-issued equipment they will receive instructions for:

- Password management
- Antivirus/ anti-malware software

They should follow instructions to protect their devices and refer to our IT department if they have any questions.

3.3 EMAILS

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

- Each employee is enrolled and required to complete a comprehensive Security Awareness Training package from KnowBe4 which is followed up with bi-weekly individual penetration testing attempts.
- Avoid opening attachments and clicking on links when the content is not adequately explained.
- 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 is not sure that an email, they received is safe, they should click the KnowBe4 PAB (Phish Alert Button) which will refer it to our IT Helpdesk.

3.4 PASSWORDS

Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they will not 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 capital and lower-case letters, numbers, and symbols) and avoid information 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.
- Do not exchange credentials, unless with IT or HR department. When exchanging them in-person is not possible, employees should prefer the phone instead of email, and only if they personally recognize the person to whom they are talking.
- Change their passwords every two months.

Remembering many passwords can be daunting. We encourage users to use available apps for password management tool which stores passwords. Employees are obliged to create a secure password for the tool itself, following the above-mentioned advice.

3.5 DATA TRANSFER

Transferring data introduces security risk. Employees must:

- Avoid transferring sensitive data (e.g., customer information, employee records) to other devices or accounts unless necessary. When mass transfer of such data is needed, we request employees to ask our IT Helpdesk for help.
- Share confidential data over the company network/ system and not over public Wi- Fi or private connection.
- 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.

Our IT staff keeps up with 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 to our specialists. The IT department staff must investigate promptly, resolve the issue, and send a companywide alert when necessary.

IT department is responsible for advising employees on how to detect scam emails. We encourage our employees to reach out to them with any questions or concerns.

3.6 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 to [HR/ IT Department].
- 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.

We also expect our employees to comply with our social media and internet usage policy.

The IT department will:

- 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.

Our company will have necessary digital shields to protect information.

3.7 REMOTE EMPLOYEES

Remote employees must follow this policy's instructions too. Since they will be accessing our company's accounts and systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure.

4.0 DISCIPLINARY ACTION

All employees are expected to follow this policy and those who cause security breaches may face disciplinary action:

- First-time, unintentional, small-scale security breach: We may issue a verbal warning and train the employee on security.
- Intentional, repeated, or large-scale breaches (which cause severe financial or other damage): We will invoke more severe disciplinary action up to and including termination.
- We will examine each incident on a case-by-case basis.

Additionally, employees who are observed to disregard our security instructions will face progressive discipline, even if their behavior has not resulted in a security breach.

5.0 TRAINING

TAKE SECURITY SERIOUSLY

Everyone, from our customers and partners to our employees and contractors, should feel that their data is safe. The only way to gain their trust is to proactively protect our systems and databases. We can all contribute to this by being vigilant and keeping cyber security top of mind.

CYBER SECURITY AWARENESS AND TRAINING

Each employee is enrolled and required to complete a comprehensive Security Awareness Training package from KnowBe4 which is followed up with bi-weekly individual penetration testing attempts.

If an employee is not sure that an email, they received is safe, they should click the KnowBe4 PAB (Phish Alert Button) which will refer it to our IT Helpdesk.

CYBER SECURITY TRAINING REQUIREMENTS

Creation of a Cimarron email account carries a requirement for cybersecurity training & testing. Each new email account automatically creates a synchronized user account in the KnowBe4

Cybersecurity LMS (learning management system). Progress & status is reported automatically to the IT dashboard as well as each individual's direct supervisor.

KnowBe4's Enterprise Awareness Training Program is a comprehensive new-school approach that integrates baseline testing using mock attacks, engaging interactive web- based training, and continuous assessment through simulated phishing, vishing and smishing attacks to build a more resilient and secure organization.

a. Baseline Testing

We provide baseline testing to assess the Phish-prone percentage of our users through a simulated phishing, vishing or smishing attack.

b. Train our Users

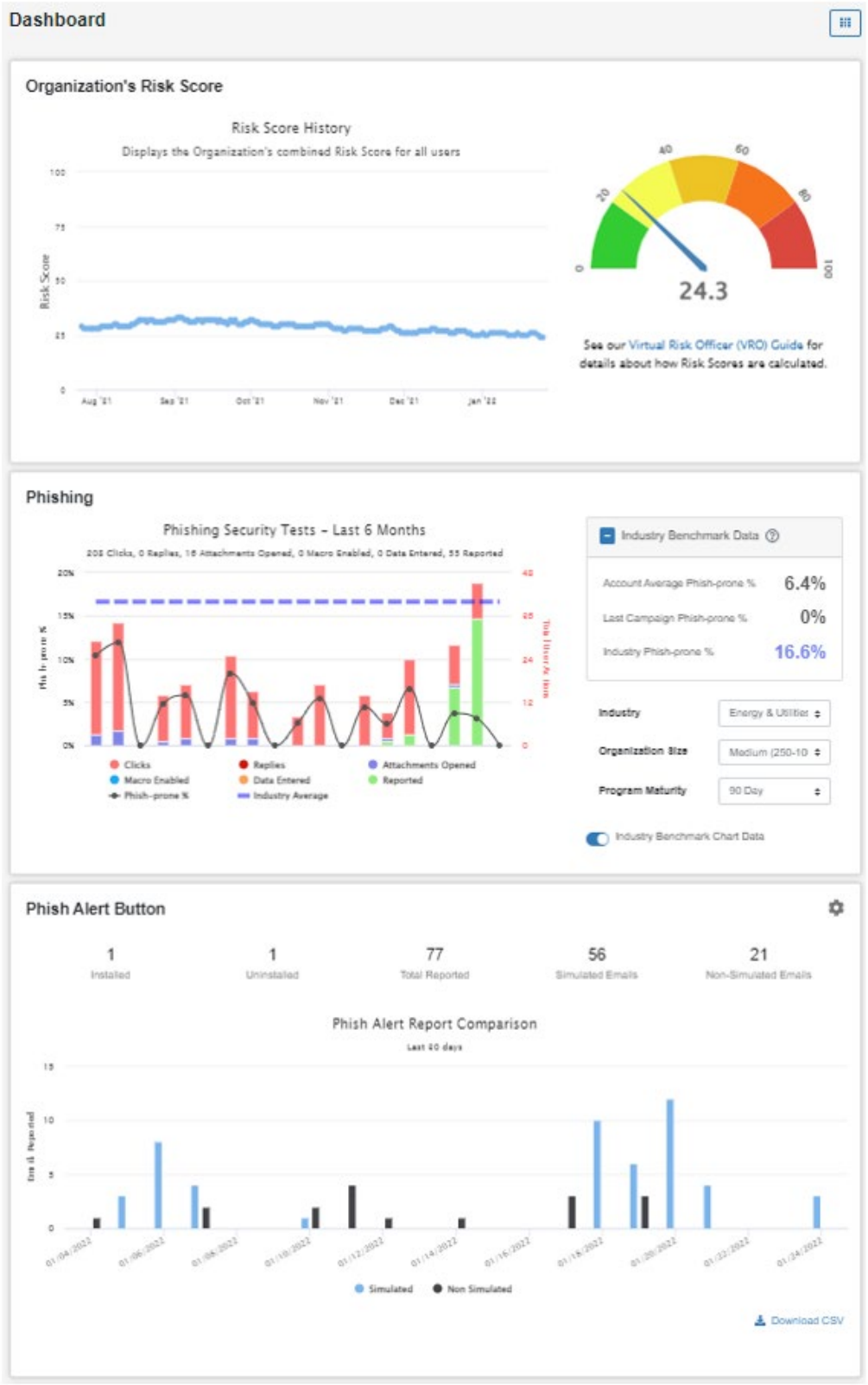
We employ the world's largest library of security awareness training content, including interactive modules, videos, games, posters, and newsletters. We create automated training campaigns with scheduled reminder emails and manager notifications.

c. Phish our Users

We also employ best-in-class, fully automated simulated phishing, vishing and smishing attacks, thousands of templates with unlimited usage, and community phishing templates.

d. Security Awareness Training

We can visualize the results in a real-time dashboard - see examples below:


Dashboard
Organization's Risk Score
Risk Score History
Displays the Organization's combined Risk Score for all users
Risk Score
24.3
See our Virtual Risk Officer (VRO) Guide for details about how Risk Scores are calculated.
Phishing
Phishing Security Tests – Last 6 Months
Clicks
Replies
Attachments Opened
Macro Enabled
Data Entered
Reported
Phish-prone %
Industry Average
Industry Benchmark Data
Account Average Phish-prone %
6.4%
Last Campaign Phish-prone %
0%
Industry Phish-prone %
16.6%
Industry
Energy & Utilities
Organization Size
Medium (250-10
Program Maturity
90 Day
Industry Benchmark Chart Data
Phish Alert Button
1
Installed
1
Uninstalled
77
Total Reported
56
Simulated Emails
21
Non-Simulated Emails
Phish Alert Report Comparison
Last 90 days
Simulated
Non Simulated
Download CSV

Both high-level and granular stats and graphs ready for management review:

This Policy supersedes all prior policies and statements, whether verbal or written, regarding the subject matter contained herein. The Company reserves the right to change, amend, modify, or terminate this Policy at any time.