Rafael Cervantes

1/28/2025

Development of a Comprehensive security Policy

TABLE OF CONTENTS

Security Policy for OrangeTech Solutions

OrangeTech Solutions is a mid-sized company with approximately 400 employees. OrangeTech Solutions is based in Palo Alto, California. Established in 2020, OrangeTech has rapidly positioned itself as a leader in the cybersecurity and software development sectors. Focused on providing cutting edge cybersecurity solutions and software applications. We empowered businesses of all sizes by delivering cybersecurity services and our cutting edge software applications. As a growing company, OrangeTech Solutions is deeply committed to maintaining the highest standards of cybersecurity for both its clients and its own operations.

Purpose

The purpose of this security policy is to ensure the protection of OrangeTech Solutions information assets, client data, software, employees data, and other sensitive information. The policy aims to safeguard the company's infrastructure from potential cybersecurity threats, such as data breaches, phishing attacks, ransomware, and insider threats. It also sets clear guidelines on compliance with industry best practices and regulatory requirements for information security. The security policy will mitigate the risks to the company's reputation, financial stability and operations. Employees and third party vendors would automatically follow the security policy implemented by the company. Ultimately, this policy is not just a set of guidelines but a critical framework for ensuring the long term sustainability and resilience of OrangeTech Solutions. Employees are expected to comply with these protocols as part of their daily responsibilities, while third party vendors are required to adhere to the same stringent security standards.

Scope

The security policy applies to all employees, and third party vendors who have access to OrangeTech Solutions' systems. Devices or systems that access, store, or transmit data must comply with this policy. This includes laptops, smartphones, tablets, desktops computers and any other devices that are connected to the company's network. Devices must use AES-256 encryption, VPNs and comply with NIST security standards.

OrangeTech Solution adheres to CCPA, GDPR, NIST, and ISO 27001 compliance, creating a flexible and comprehensive security and privacy framework. California Consumer Privacy Act (CCPA) provides California's residents rights over their personal data, the right to know what data is being collected and the right to request deletion of data. General Data Protection Regulation (GDPR) requires robust security practices to collect, process and store personal data of EU citizens. National Institute of Standards and Technology (NIST) is a U.S. government standards, guidelines and best practices for the technology sector. ISO 27001 is an international standard for information security management systems.

Policy

A. Acceptable Use

Employees are permitted to use OrangeTech Solutions' IT System for work related activities only. IT systems include computers, networks, and mobile devices. Prohibited activities include accessing, downloading, or distributing unauthorized files or media, as these actions can introduce malware, viruses, or other malicious software. All devices and applications used to access company resources must be configured in compliance

with the company's security standards. Access to certain sensitive systems or data may be restricted based on the employee's role and responsibilities.

B. Password Policy

Employees must create strong passwords with at least 12 characters, using a combination of letters, numbers, and symbols. Multi-factor authentication (MFA) must be implemented for all systems. Including methods such fingerprint scanners, facial recognition, email verification codes and push notifications. Employees should use a password manager for secure storage. Multi-factor authentication (MFA) must be enabled for accessing the company's systems and cloud services. Employees are prohibited from sharing passwords. If the employees passwords are forgotten, employees must use the official password reset procedure. If employees cannot reset their own passwords, the IT support team can help. Default passwords provided by vendors must be changed before any system is deployed.

C. Data Classification

AT OrangeTech Solutions, data is categorized into different levels based on its sensitivity and potential impact that unauthorized access could have on the company. Public data can be freely shared with the public.This type of data is generally nonsensitive and does not contain any private or confidential information that could harm the company. Public data required minimal protection. Internal data is non sensitive data that is used for daily operations and is only accessible by employees. Internal data still requires protection to prevent unauthorized access. This category includes internal

reports, meeting notes, operational procedures and other business documents. Internal data requires protection to prevent unauthorized access.

Confidential data is sensitive business data or customer information that must be protected. Confidential data includes sensitive business or customer information that requires protection but is accessible to authorized personnel within the organization. Confidential data should be encrypted and only accessible to employees who need it to perform their roles. Restricted data is highly sensitive data that requires strict protection and limited access. Restricted data is the most sensitive category, requiring strict access controls and encryption, and should only be accessible to specifically authorized personnel. Restricted data must be stored in secure environments with multiple layers of protection. Encryption, access controls, and strict monitoring are the layers used to protect restricted data.

D. Mobile Device Security

All mobile devices, including smartphones, laptops and tablets that access OrangeTech Solutions System must be secured with password protection or biometrics authentication to ensure that only authorized users can access company resources. Biometric authentication is encouraged since it provides a secure method of verification. Personal devices (BYOD) are permitted only if enrolled in the company's MDM system or an approved containerization solution. Unenrolled personal devices cannot access sensitive company data. The MDM system is essential for managing, securing and monitoring all devices that access the company network. All IoT devices connected to the

company network must be secured with strong passwords and firmware updates must be applied regularly.

E. Incident Response

The Incident Response Plan (IRP) is a critical component of OrangeTech Solutions; it must be activated immediately once a security incident is detected. The IRP is designed to ensure that the organization responds to security threats efficiently and in an organized manner to minimize the impact of the incident. It outlines the step by step procedures that must be followed when an incident is identified. Potential threats can be phishing emails, unusual login activity, unauthorized access, fake payment requests or unfamiliar devices connecting to the company network. Phishing emails are among the most common forms of cyberattacks. Unusual login activity such as multiple failed logins, unfamiliar locations, or logins outside of business hours should be reported.

Employees must report any suspicious security incident to the IT or cybersecurity team immediately. Incidents such as phishing emails, unauthorized access, or unusual system activity must be escalated within one hour to mitigate potential threats. Once an incident is reported, the It team will take the lead in investigating the situation. Incidents must be documented by the IT or cybersecurity team for future analysis and to develop preventative measures. Communication during a security incident must be managed by the Incident Response Coordinator (IRC), ensuring only authorized individuals are informed. The Company will notify the regulatory bodies in case of a data breach. After neutralizing the incident, the IT team will restore affected systems to their secure and functional state.

Roles and Responsibilities

A. Chief Information Security Officer (CISO)

The CISO has the overall responsibility for verifying the implementation and compliance with the security policy. The CISO supervises any new cybersecurity trends and verifies the company's security measures remain efficient. The CISO is responsible for regularly evaluating and testing the company's existing security measures to ensure they remain effective and efficient. The CISO is responsible for creating the security policies.

B. IT Team

The It team at OrangeTech Solutions plays a critical role in the implementation, maintenance and continuous improvement of the company's security infrastructure. The IT team implements and maintains security infrastructure, including firewalls, encryption, and access control. Additionally, they provide guidance on security best practices to employees. IT is also responsible for policy compliance checks, making sure that employees are following the password rules, data handling and reporting any suspicious activity. The IT team is responsible for log preservation to support forensic investigation. The IT team is responsible for providing ongoing guidance and training to employees regarding security best practice.The IT Team is responsible for data protection and privacy compliance. The IT team regularly conducts vulnerability assessments and penetration tests to identify weaknesses in the system and address them before they can be exploited by threat actors. The IT team collaborates with the CISO and others to create

the security policies. Using Security Information and Event Management (SIEM) will help monitor network traffic, login attempts that will prevent incidents from evolving.

C. Employees

Employees at OrangeTech Solutions are expected to fully comply with all aspects of the security policy to help protect the company;s digital assets, sensitive information, and overall security infrastructure. Employees need to secure handling of data, updating devices, using strong passwords and report any suspicious activity. Passwords must contain a mixture of numbers, special characters, uppercase and lowercase letters. MFA should be enabled wherever possible to add an extra layer of security when accessing company systems. Employees need to complete mandatory security awareness training. Employees need to know how to identify potential risks and report them to IT.

Enforcement and Penalties

Violations of this security policy will be addressed through a progressive disciplinary process, ranging from formal warnings and mandatory retraining to access restrictions, suspension, or termination for severe or repeated violations. Intentional security breaches, such as data theft or malicious activity, may result in legal action. Employees found to be in violation of the security policy may face various forms of corrective actions, depending on the nature and severity of the infraction. Minor violations such as failing to follow the password management protocols or neglecting to update security software may result in a formal warning. Employees found violating security policies may be subject to mandatory retraining on security best practices.

Severe violation of the security can lead to financial damage, loss of sensitive data, harm to the company or its clients. Any violations should be reported immediately to the CISO or HR for investigation. HR and the Chief Information Security Officer (CISO) will determine the appropriate disciplinary action. Employees using unauthorized devices will be restricted from network access.

Review and Revision

The Security Policy at OrangeTech Solutions is considered a living document which means that it is continuously involved to stay aligned with new threats, changes to technologies, regulatory updates and shifts in business needs. As laws and regulations around data privacy and cybersecurity continue to evolve, such as updates to the General Data Protection Regulation(GDPR) or the California Consumers Privacy Act (CCPA) the policy will be updated to ensure compliance with the latest legal requirements. The CISO is responsible for the ongoing review and refinement of the security policy. Once the security policy changes, all employees would be verified. The changes of the security policy will reflect on the future security training and employee handbook.

Auditing Procedure

Regular audits will be conducted on the company's IT systems, network infrastructure and security controls. Audits will include reviews of users access logs, system configurations, passwords compliance and security patches on devices and software. The IT team will perform internal audits quarterly. External audits performed by a certified third party security auditor will occur annually to verify impartiality and compliance with industry standards. Any vulnerabilities found during audits will be

addressed promptly, with corrective actions. Auditors will be reviewing how employees handle different categories of information and identifying areas of improvement. The audit findings will be reported to the CISO, and correctional action will be taken to rectify any gaps in security.

References

Developing a Security Policy for IBM I." *Www.ibm.com*, www.ibm.com/docs/en/i/7.4?topic=strategy-developing-security-policy.

Grimmick, Robert. "What Is a Security Policy? Definition, Elements, and Examples." *Www.varonis.com*, 6 Apr. 2023, www.varonis.com/blog/what-is-a-security-policy

"Building Information Security Policies with Ease." *Www.nsf.org*, www.nsf.org/knowledge-library/building-information-security-policies-with-ease.

Kirvan, Paul. "How to Write an Information Security Policy, plus Templates." *SearchSecurity*, Mar. 2022, www.techtarget.com/searchsecurity/tip/How-to-write-an-information-security-policy-plus-templates.

Buckbee, Michael. "How to Create a Good Security Policy." *Www.varonis.com*, 2 June 2023, www.varonis.com/blog/how-to-create-a-good-security-policy.

.