cenareo

Cyber Security - Data Protection

Cenareo is committed to protecting the confidentiality, integrity, and availability of this data throughout its lifecycle.

This Data Protection Policy outlines the technical and organizational controls Cenareo implements to safeguard customers' data entrusted to us.

By implementing these data protection controls and fostering a culture of data security awareness, we strive to provide Cenareo customers with the highest level of assurance for the security and confidentiality of their entrusted data.

This policy will be reviewed and updated periodically to reflect changes in technology, security threats, and regulatory requirements.

Responsibilities

- **Management:** Provides resources and support for implementing and maintaining data protection controls.
- **IT Security Team:** Owns and manages technical controls, ensuring their effectiveness and regular updates.
- **All Employees:** Are responsible for adhering to data security policies and procedures, including data handling practices and reporting suspected security incidents.

Access Controls

- **Multi-Factor Authentication (MFA):** Cenareo enforces MFA for all user access to systems containing customer's data. This requires a combination of factors, such as passwords, security tokens, or biometrics, to verify user identity.
- **Least Privilege:** User access is granted based on the principle of least privilege, granting only the minimum permissions necessary for users to perform their assigned tasks.

Cenareo - SAS au capital de 22175 € R.C.S Toulouse 789 137 650 - APE: 6201Z TVA intra: FR 789 137 650

- **Access Logging and Monitoring:** All access attempts to customer's data are logged and monitored for suspicious activity.

Wi-Fi Network Access

- **Restricted Access:** Our Wi-Fi network is configured with access control mechanisms to restrict unauthorized access. This may involve the use of WPA2 encryption with strong passwords or pre-shared keys.
- **Guest Network:** For visitors or devices not requiring access to customers' data, a separate guest network may be offered. This guest network should be logically segregated from the network containing customers' data and have limited access to internal resources.

Device Registration:

- **Authorized Devices:** Only authorized devices pre-registered with the IT department can connect to the Wi-Fi network. This allows for monitoring and control over devices accessing the network.
- **Device Security Requirements:** Registered devices must meet minimum security requirements, such as having updated operating systems, antivirus software, and firewall protection.

Multi-Factor Authentication (MFA)

- **Mandatory MFA:** MFA is mandatory for all devices accessing resources containing customers' data, regardless of whether they are connected to the Wi-Fi network or the wired network. MFA adds an extra layer of security beyond passwords, requiring a secondary verification factor like a security token, one-time passcode, or biometrics.
- **MFA Enrollment:** All users authorized to access customers' data must enroll their devices in the MFA system and follow the established procedures for MFA authentication.

Security Protocols

Cenareo - SAS au capital de 22175 € R.C.S Toulouse 789 137 650 - APE: 6201Z TVA intra: FR 789 137 650

We enforce the use of secure protocols like HTTPS for web browsing, secure file transfer protocols (SFTP) for data transfers over the Wi-Fi network, and SSH (Secure Shell) for remote access. These protocols encrypt data in transit, protecting it from eavesdropping or tampering.

Approved Encryption Protocols:

- **AES (Advanced Encryption Standard)**: A widely adopted symmetric encryption algorithm considered secure for most applications. It comes in various key lengths (128-bit, 192-bit, 256-bit) with 256-bit being the strongest.
- **RSA (Rivest–Shamir–Adleman)**: An asymmetric encryption algorithm used for public-key cryptography. It's generally considered secure for key exchange and digital signatures when implemented with proper key lengths (at least 2048 bits).
- **TLS (Transport Layer Security)**: The successor to SSL, TLS secures communication between applications over a network. It uses a combination of symmetric and asymmetric encryption to ensure data confidentiality and integrity. Versions 1.2 and 1.3 are considered secure. (Note: Earlier versions of TLS (e.g., 1.0 and 1.1) are deprecated due to vulnerabilities)
- **SSH (Secure Shell)**: A secure protocol for remote access to computer systems. It uses strong encryption to protect user authentication and data transfer.

Deprecated Encryption Protocols:

- **DES (Data Encryption Standard)**: An older symmetric encryption algorithm that is no longer considered secure for most applications due to its short key length (56-bit).
- **RC4 (Rivest Cipher 4)**: A stream cipher that was once widely used but has known weaknesses. Its use is strongly discouraged due to security vulnerabilities.
- **MD5 (Message-Digest Algorithm 5)**: A cryptographic hash function used for data integrity verification. However, MD5 is no longer considered collision-resistant and should not be used for new security implementations.
- **SHA-1 (Secure Hash Algorithm 1)**: Another cryptographic hash function with vulnerabilities. While not completely broken, SHA-1 is no longer recommended for new applications and should be replaced with SHA-2 or SHA-3 variants.
- **SSL (Secure Sockets Layer)**: The predecessor to TLS, SSL has known vulnerabilities and is no longer considered secure.

Cenareo - SAS au capital de 22175 € R.C.S Toulouse 789 137 650 - APE: 6201Z TVA intra: FR 789 137 650

cenareo

Prohibited Activities

- **Unauthorized Access:** The use of the Wi-Fi network for unauthorized access attempts to customers' data or other restricted resources is strictly prohibited.
- **Malicious Activity:** Any activities on the Wi-Fi network that could compromise network security or introduce malware are strictly forbidden. This includes activities like unauthorized file sharing, peer-to-peer applications, or running network scanners.

Network Segmentation:

- **Firewalls:** We implement firewalls to segment our network and restrict unauthorized access to resources containing customers' data. Firewalls act as barriers, allowing only authorized traffic based on pre-defined security policies.
- **Demilitarized Zone (DMZ):** If applicable, we utilize a DMZ to isolate highly sensitive systems containing customers' data from the public internet. The DMZ acts as a controlled buffer zone, minimizing the attack surface for critical systems.
- **Virtual LANs (VLANs):** We may implement VLANs to further segment the network and logically separate traffic flows. This restricts communication between different network segments, enhancing data security.

Intrusion Detection and Prevention Systems (IDS/IPS):

Cenaroe plans to deploy IDS/IPS systems to monitor network traffic for suspicious activity and potential security threats. These systems can detect and block malicious attempts to access customers' data.

Network Access Control (NAC):

Cenareo plans to implement NAC to enforce security policies on devices attempting to connect to the network. NAC ensures devices meet specific security requirements (e.g., updated operating systems, and antivirus software) before granting network access. This helps prevent compromised devices from accessing customers' data.

Cenareo - SAS au capital de 22175 € R.C.S Toulouse 789 137 650 - APE: 6201Z TVA intra: FR 789 137 650

cenareo

Vulnerability Management:

Cenareo maintains a comprehensive vulnerability management program to identify, prioritize, and remediate vulnerabilities in network devices and software. This proactive approach minimizes the risk of attackers exploiting vulnerabilities to gain unauthorized access to customers' data.

Network Monitoring and Logging:

We continuously monitor network activity for suspicious behavior and security incidents. Network logs are collected and analyzed to identify potential threats and investigate unauthorized access attempts.

Data Segregation

- **Client Separation:** We implement logical and, where feasible, physical segregation of the customer's data processing environment from other client data. This separation minimizes the risk of unauthorized access or cross-contamination.
- **Production/Non-Production Segregation:** We logically segregate production environments where customer data is processed from non-production environments like development or testing. This ensures data integrity and prevents unauthorized access from non-production systems.

Encryption

- **Data Encryption at Rest:** All customer's data within our systems is encrypted at rest using industry-standard algorithms.
- **Data Encryption in Transit:** We utilize TLS/SSL encryption protocols to secure data transfers containing customer's data over public networks. This protects data from unauthorized interception during transmission.

Key Management

We maintain robust key management procedures and processes, including:

- Secure key generation and activation.

- Defined key rotation schedules and expiration policies.
- Secure storage of encryption keys with restricted access controls.
- Regular reviews and updates of key management practices.

Data Destruction

Cenareo enforces a standardized process for the secure destruction of old media containing customer's data. This process includes physical destruction or secure overwriting of data to ensure it is unrecoverable.

At the end of the contract term, we securely destroy the customer's data per a documented procedure. This may involve secure deletion, overwriting, or physical destruction of media.

Data Loss Prevention

Cenareo is implementing DLP solutions on endpoints, email servers, web proxies, and web services to detect and prevent potential leaks of customer data. DLP solutions scan for sensitive data patterns and enforce policies to restrict unauthorized data exfiltration.