cenareo

Cyber Security - Data & Cyber Security Risk Management

This policy outlines Cenareo's approach to managing data security and cybersecurity risks, protecting our assets, and ensuring the confidentiality, integrity, and availability of customer's data throughout its lifecycle.

Risk Assessment

Cenareo conducts periodic risk assessments to identify potential threats, vulnerabilities, and their impact on data security and cybersecurity.

These assessments consider various factors, including:

- Data classification
- System and application security postures
- Network infrastructure vulnerabilities
- Internal and external threats (e.g., cyberattacks, human error)

The results of the risk assessments inform our security strategy, resource allocation, and implementation of appropriate controls.

Data Classification

Cenareo categorizes data based on its sensitivity and potential impact in case of a breach.

This helps prioritize security measures and allocate resources effectively as well as warranty:

- **Improved Security:** By identifying the most critical assets and prioritizing security controls for their protection.
- **Compliance:** By aligning with data privacy regulations that often mandate specific safeguards for certain types of data (e.g., GDPR).
- **Efficient Resource Allocation:** By understanding data sensitivity, organizations can allocate security resources more effectively and avoid over-protecting low-risk data.
- **Incident Response:** By simplifying incident response providing a clear understanding of the potential impact of a data breach.

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

Data classification is an ongoing process, Cenareo regularly reviews and updates classification schemes to reflect changes in business, regulations, and the threat landscape.

Cenareo Data is categorized with the following definitions:

Highly Confidential Data

This category includes data that is critical to the Cenareo operations, financial well-being, or reputation. A breach could result in severe financial losses, legal repercussions, or damage to public trust.

Examples:

- Customer financial information (credit card numbers, Social Security numbers)
- Proprietary trade secrets or intellectual property
- Personally identifiable information (PII) subject to strict regulations
- Executive communications and strategic plans

Confidential Data

This category encompasses sensitive data that, if compromised, could cause moderate financial harm, reputational damage, or operational disruptions.

Examples:

- Customer names, contact information, and purchase history
- Internal employee data (salary information, performance reviews)
- Confidential business documents (contracts, proposals)
- Marketing campaign data

Internal Data

This category includes sensitive information that is important for internal operations but doesn't necessarily have the same level of criticality as confidential data.

Examples:

- Employee training materials
- Internal communications and memos
- Non-public customer service records
- IT infrastructure information

Public Data

- Definition: This category refers to information that is publicly available or intended for public dissemination.
- Examples:
    - Company website content
    - Press releases and marketing materials
    - Public financial reports
    - Product manuals and brochures

Asset Management

Cenareo maintains a comprehensive inventory of all assets that store, process, or transmit customer data.

This includes:

- Hardware (servers, workstations, mobile devices)
- Software applications
- Network devices
- Data storage systems

Access to these assets is strictly controlled based on the principle of least privilege.

Supply Chain & Subcontracting

Cenareo recognizes the importance of cybersecurity within our supply chain and has established a risk management strategy agreed upon by relevant stakeholders.

This strategy includes conducting cyber supply chain risk assessments for:

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

- Information system vendors
- Third-party partners providing components or services
- Subcontractors entrusted with customer's data

These assessments evaluate the security practices and potential risks associated with these entities.

Third-Party Management

Cenareo conducts routine assessments of critical suppliers and third-party partners through:

- Security audits
- Penetration testing results
- Other forms of security risk evaluations

This ensures they meet their cybersecurity requirements and adequately protect customer's data.

Cenareo requires third parties to remediate identified vulnerabilities and security risks within a defined timeframe.

Contractual Safeguards

Cenareo only shares data with third-party vendors when absolutely necessary for operational purposes. All such data sharing is governed by strict information security clauses within the contracts.

These clauses address:

- Confidentiality obligations regarding customer's data
- Data integrity and availability requirements
- Security controls and incident reporting procedures

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

Non-Production Environments

Cenareo strictly minimizes the storage of customer data in non-production environments. This emphasizes the preference to avoid storing customer data in development, testing, and user acceptance testing (UAT) environments whenever possible.

When necessary, customer data must be stored in non-production environments, and the same or equivalent security measures used in production environments are applied.