cenareo

# Cyber Security - Incident & Crisis Management Policy

Cenareo is committed to protecting customer data and maintaining the confidentiality, integrity, and availability of its information systems.

This policy outlines our formal process for detecting, identifying, analyzing, responding to, and recovering from security incidents or crises.

## Analysis and Investigation

### Detection and Identification

Cenareo utilizes various security tools and monitoring systems to detect potential security incidents or crises. This includes log analysis, intrusion detection systems, and endpoint security solutions. Upon detection of a potential incident or crisis, Cenareo will initiate an investigation to determine its nature, scope, and impact.

### Investigation Team

A dedicated incident response team consisting of IT security personnel, relevant business unit representatives, and legal counsel will be assembled to investigate the incident or crisis.

### Evidence Collection

The team will collect and preserve all relevant evidence, including system logs, network traffic data, and affected files. This will facilitate forensic analysis and root cause determination.

### Communication:

Throughout the investigation, Cenareo will maintain open communication with the customer, keeping them informed of the incident status and potential impact on their data.



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

**Notification Process**

Cenareo is committed to notifying customer promptly upon identifying a security incident that may impact their data or systems. The notification timeframe will be determined by the severity of the incident.

The notification will include details such as the nature of the incident, the potential impact on customer data, and the actions being taken to mitigate the incident and recover from it.

**Containment**

The primary objective is to contain the incident and prevent further damage or data loss. This may involve isolating compromised systems, suspending user accounts, or shutting down affected services.

**Eradication**

Cenareo will take steps to eradicate the root cause of the incident and prevent its recurrence. This may involve patching vulnerabilities, removing malware, or implementing additional security controls.

**Recovery**

Cenareo will restore affected systems and data to a functional state using backups and disaster recovery procedures. Data recovery capabilities for customer's data will be prioritized.

**Lessons Learned**

Following the incident, Cenareo will conduct a thorough review to identify lessons learned and improve our security posture. This includes updating our incident response plan and implementing additional security controls to prevent similar incidents in the future.



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

## Security Capabilities

### Digital Forensics

Cenareo can conduct digital forensics investigations to analyze evidence and determine the scope and nature of a security incident.

### Log Management

Cenareo captures and stores audit logs from relevant systems for analysis during investigations and post-incident review. customer's data within these logs will be anonymized where possible and protected with appropriate access controls.

### Log Security

Cenareo has controls in place to protect logs from unauthorized access or corruption. These controls may include encryption, access restrictions, and tamper detection mechanisms.

### Security Operations Center (SOC)

Cenareo maintain a Security Operations Center (SOC) or equivalent function that continuously monitors our information systems for suspicious activity. The SOC team is responsible for detecting, investigating, and responding to security incidents.

## Disaster Recovery Scenarios:

Cenareo has documented disaster recovery scenarios for critical systems, including Active Directory and Privileged Access Management (PAM) solutions. These scenarios outline the steps necessary to restore functionality and minimize downtime in case of a failure or compromise.



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

Cenareo can recover customer's data in case of a failure or data loss through backups and disaster recovery procedures. The recovery time objective (RTO) and recovery point objective (RPO) for customer's data will be clearly defined and documented.

## Incident History

Cenareo maintains a record of all security incidents, including successful attacks and those that Cenareore mitigated before causing disruption. This information is used to improve our security posture and ensure Cenareo is prepared to handle future incidents effectively.

## Communication with customer

Cenareo will maintain open communication with customers throughout the incident response process. This includes providing timely updates on the investigation, containment efforts, and recovery progress.

## Compliance

This incident management policy is aligned with relevant security frameworks and industry best practices. Cenareo will regularly review and update this policy to reflect changes in the threat landscape and regulatory requirements.



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