cenareo

Cybersecurity Policies at Cenareo

Last update: May 1, 2024

The objective of these IT Cybersecurity policies is to internally drive and get up to date our standards, ensuring the optimal safeguarding of our information systems, confidential data, and intellectual property from unauthorized access, intrusions, malware, ransomware, and other cyber threats.

Last but not least, we've made the decision to grant our customers access to Cenareo's public policies. Moreover our team is dedicated to collaborating with our Customers to provide more detailed information.

Topics	Description	Link
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.	Data & Cyber Security Risk Management
Access Management	This policy ensures that access to sensitive information and systems is granted based on the principle of least privilege and helps to mitigate the risk of unauthorized access.	Access Management Policy
Data Protection	This Data Protection Policy outlines the technical and organizational controls Cenareo implements to safeguard customers' data entrusted to us.	Data Protection Policy
Vulnerability Management	This policy outlines the formal procedures for vulnerability & patch management within Cenareo. It ensures timely identification, prioritization, and deployment of security	Vulnerability Management Policy

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

	patches for all applications and systems processing data.	
Incident Management	This policy outlines our formal process for detecting, identifying, analyzing, responding to, and recovering from security incidents or crises.	Incident & crisis Management Policy
Change and Release Management	This policy outlines the formal procedures for Change and Release Management within Cenareo. It ensures secure and controlled development, testing, deployment, and management of changes to our software applications, systems, and infrastructure.	Change and Release Management Policy