ChannelEngine Security Overview

channelengine

Domains

ChannelEngine has defined and enacted an information security management system (ISMS) that consists of 5 security domains. The ISMS is guided by industry standards for identification of technical and procedural controls, and management of information security. The domains are essential in unifying technologies, people and budget.

The 5 domains are as follows:

- Security and risk management
- Security and engineering operations
- Software engineering security
- Data protection
- Legal and regulatory compliance

Policies

ChannelEngine has defined 38 policies that provide clear guidelines and standards for protecting the company's information assets. The policies are used to establish a baseline for information security practices, provide a consistent approach to risk management and ensure that everyone in the organization understands their responsibilities for protecting the company's information assets.

The information security policies are as follows:

- Information security policy
- Information security program
- Technical and organizational measures
- Acceptable use policy
- Clean desk policy
- Human resource security policy
- Security awareness blueprint
- Security audit and management review
- Risk management framework (CE))
- Supply chain and vendor risk management policy
- Password policy
- IT security policy
- Cloud security policy
- Cryptography policy
- Key management policy
- Security testing policy
- Data leakage prevention policy
- Configuration management policy
- Logging and monitoring policy
- Incident management policy
- System acquisition, development and maintenance policy
- Software change management policy
- Open source software usage policy
- Asset management policy
- Data classification, storage and exchange policy
- Access management policy
- Backup and recovery policy
- Data privacy, protection and retention policy
- Cyber insurance policy
- Security audit policy
- Mobile device management policy
- Business continuity plan

Controls & Capabilities (ISP)

ChannelEngine has defined and enacted an information security program (ISP) that defines an approach and all the activities required to implement preventive, detective, forensic and audit controls and sub-controls across the 5 domains identified in the information security management system (ISMS).

The controls reduce risks affecting confidentiality, integrity and availability by reducing probability, reducing impact, detecting occurrence of incidents and collecting evidence in support of incidence response. The controls and capabilities communicate the cybersecurity position of the company and are delivered by various technologies.

The controls are as follows:

- Server monitoring and alerting using site 24*7, Opserver, Solarwinds DPA for availability and performance
- Transaction log, differential and full backups taken every 15 mins, every 6 hours and daily respectively
- Wireless communication encrypted using WPA2 encryption standard
- Explicit deny rule implemented on firewalls to deny access unless explicitly allowed
- Use of secure protocols (sFTP, HTTPs) and disabling of insecure protocols
- Confidentiality agreements signed by employees and partners to minimize information disclosure
- Rules for acceptable use of IT systems and data are defined and implemented
- Security assessments and tests are performed annually including penetration tests and information security audits, code reviews and compliance attestation (ISO 27001)
- Passwords are encrypted and hashed using AES-256, SHA-256 respectively before being stored in a database
- Network segregation using firewalls and VLANS
- API keys and tokens are stored in a secure manner
- Monitoring and vulnerability management using Microsoft 365 defender for the platform, Elastic for the application and WIZ for the infrastructure, containers, micro-services and code repositories
- Centralized input validation is implemented to prevent XSS and SQLi attacks
- Establishment of secure communication to the application using TLS 1.3
- Endpoints are hardened and unnecessary services disabled
- Data anonymization after 24 months or as per customer request
- Secure authorization (SSO) using OAuth

Standards & Compliance

ChannelEngine is ISO/IEC 27001:2022 certified, having implemented an ISMS and ISP that demonstrated adherence to best practices, compliance to industry standards including GDPR, and commitment to continuous improvement.

CERTIFICATE

Certificate
K-0222690 / 1

kiwa

Issued on	2025-02-14	Page	1 of 1
First issue	2025-02-14	Valid until	2028-02-13

ISO 27001:2022

With this certificate Kiwa confirms that the management system implemented by

ChannelEngine.com B.V.

meets the requirements of ISO 27001:2022 for the scope:

Information security for the development, delivery, maintenance, and support of middleware and software connections for marketplaces.

ISMS includes statement of applicability version 2.0 2024-12-01

Ron Scheepers
Country manager Kiwa Nederland

Consult www.kiwa.com in order to ensure that this certificate is still valid.

Kiwa Nederland B.V.
Sir Winston Churchillaan 273
Postbus 70
NL-2280 AB RIJSWIJK

Tel. +31 88 998 44 00
Fax +31 88 998 44 20
info@kiwa.com
www.kiwa.com

Company details
ChannelEngine.com B.V.
Vondellaan 47
2332 AA LEIDEN
THE NETHERLANDS
COC 63350726

channelengine

Thank you

https://www.linkedin.com/company/channelengine

security@channelengine.com

ChannelEngine HQ Europe
Vondellaan 47, 2332 AA Leiden
The Netherlands

ChannelEngine Germany
Maximilianstraße 2
80539 München

ChannelEngine Inc HQ North America
228 E 45TH ST RM 9E
NEW YORK, NY 10017

ChannelEngine Canada
181 Bay Street, Suite 1800,
Toronto, Ontario, Canada, M5J 2T9

ChannelEngine Singapore
71 Robinson Rd
Singapore 068895

ChannelEngine Australia
Level 19, 15 William Street
Melbourne VIC, 3000

ChannelEngine Dubai
BCB2 402
Fourth Floor, Dubai CommerCity