ACDEON B.V.

Gasthuisplaats 1
2611 BN Delft
The Netherlands

Chamber of Commerce number: 97878421
VAT ID nr.: NL868271834B01
Bank Account [EUR]: NL09BUNQ2159258024
Bank Account [USD]: WISE 250768783669566

ACDEON - Security Baseline (NIS2-aligned, proportionate to ACDEON)

Executive summary

This document outlines ACDEON's baseline approach to information security. It is inspired by principles from the EU NIS2 Directive and ISO/IEC 27001, but tailored to the size and nature of ACDEON as a specialised representation
and consulting company. The focus is on practical, proportionate controls that protect business and customer information
without unnecessary complexity.

Scope of activities

ACDEON's activities, as registered in the Netherlands, include:

Het verlenen van advies en dienstverlening aan bedrijven in het Verenigd Koninkrijk en de Europese Unie, waaronder het optreden als vertegenwoordiger van een of meerdere ondernemingen. De activiteiten zijn gericht op de hightech industrie, waaronder de lucht- en ruimtevaart, defensiegerelateerde industrie, maritieme sector, agrarische industrie, de automobielindustrie en de semi-conductor industrie.

Security measures are therefore focused on protecting professional correspondence, contact details, technical and
commercial information related to projects in the high-tech sectors mentioned above.

1. Objectives

ACDEON's main security objectives are:
- Protect the confidentiality, integrity and availability of information needed to support customers and represented
manufacturers.
- Maintain trust with manufacturers, partners and customers.
- Keep the security approach pragmatic, manageable and proportionate to ACDEON's size.

2. Governance and responsibility
- Overall responsibility for information security rests with the director of ACDEON.
- Security is considered in decisions about tools, hosting, analytics and data processing.
- Where external IT suppliers are used, their security posture is taken into account in the selection process.

3. Access control

Key controls include:
- Strong, unique passwords for email, hosting, analytics and other critical systems.
- Two-factor authentication (2FA) wherever reasonably available, particularly for cloud and admin interfaces.
- Limiting access to systems and data to those accounts that are strictly necessary for ACDEON's operations.
- Regular review of active accounts and revoking access when no longer needed.

ACDEON B.V.

Gasthuisplaats 1
2611 BN Delft
The Netherlands

Chamber of Commerce number: 97878421
VAT ID nr.: NL868271834B01
Bank Account [EUR]: NL09BUNQ2159258024
Bank Account [USD]: WISE 250768783669566

4. Device security
- Work devices are kept up to date with operating system and security updates.
- Full-disk encryption is enabled where available to protect data at rest.
- Modern endpoint protection (such as antivirus/anti-malware) is used to reduce the risk of malware and phishing.
- Devices are locked when unattended.

5. Network and hosting
- The ACDEON website uses HTTPS to protect data in transit.
- Matomo analytics is hosted on EU-based infrastructure, with secure configuration and access control.
- Remote access to servers and administrative interfaces is restricted and protected by strong authentication.
- Default or weak credentials are not used on internet-facing services.

6. Backup and continuity
- Important business information (such as correspondence, documents and configuration data) is backed up regularly.
- Backups are stored separately from production systems to reduce the impact of hardware failures, ransomware or other
incidents.
- Basic restore procedures are tested periodically to ensure that data can be recovered when needed.

7. Incident detection and response
- Security-relevant events (such as suspicious login attempts, possible data leakage or malware alerts) are taken
seriously and investigated.
- If ACDEON becomes aware of a personal data breach affecting individuals, the incident will be assessed in line with
GDPR requirements, including whether notification to the Dutch Data Protection Authority (Autoriteit Persoonsgegevens)
and/or affected individuals is required.
- After incidents, appropriate corrective measures are implemented to reduce the likelihood of recurrence.

8. Supplier and service management
- Key IT suppliers (hosting, analytics, email, backup) are selected with attention to reliability, security features and
alignment with EU data protection rules.
- Where appropriate, contracts or terms of service include data protection and security clauses.
- Use of new external services is evaluated with a view to security and privacy impact before adoption.

9. Awareness and continuous improvement
- Security awareness is part of day-to-day work: phishing, social engineering and unsafe attachments are treated with

caution.
- Security practices are reviewed periodically and updated when there are relevant changes in technology, threats or
regulatory expectations (for example developments around NIS2).
- Feedback from manufacturers or partners regarding security is taken into account and may lead to refinements of the
baseline.

Document version and status
Document: ACDEON Security Baseline
This baseline is intended as a high-level description of ACDEON's security practices as of 9 December 2025. It is reviewed periodically and may be updated when systems, services or the regulatory environment change.