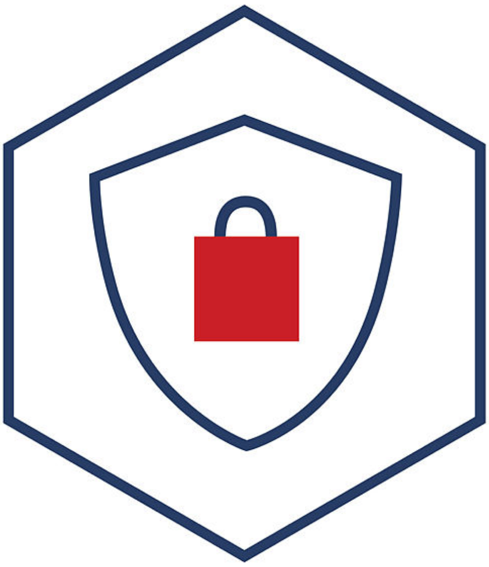
Public directive

Partner Information Security and Data Protection

Policy

DESCRIPTION:	Reference Document for Contractual Agreements with Third Parties. viastore GROUP
VERSION:	1.6
PROTECTION CLASS:	normal



Guaranteed Success.

Contents

Document information / modification status

Date	Version	Modification	Author
2025-04-10	1.0	Initial version.	Thorsten Sauter
2025-06-24	1.1	Updated version.	Thorsten Sauter
2025-06-25	1.2	Small fixes in language	Thorsten Sauter
2025-07-22	1.3	Partner Key Users	Thorsten Sauter
2025-07-27	1.4	EU Data Act, EU AI Act	Thorsten Sauter
2025-05-27	1.5	AI ownership	Thorsten Sauter
2025-08-07	1.6	Data handling	Thorsten Sauter

1. Purpose

This policy defines mandatory requirements for information security and data protection in contractual agreements with third-party partners, suppliers, vendors, and service providers (hereafter: “Partners”). This document, along with other measures, serves to implement corresponding legal obligations or aims to ensure their implementation, including NIS2 and the Cyber Resilience Act (CRA), and aims to minimize risk to viastore’s critical systems, data, and operations.

2. Scope

This policy applies to all Partners involved in the production, development, or delivery of products or software with digital components for **viastore** or any **viastore** customer. It also extends to Partners whose non-digital goods or services are critical to the overall delivery and performance framework, in order to ensure contractual fulfillment and to protect the integrity of **viastore**’s supply chain, operational stability, and customer obligations.

Furthermore, the policy applies to all Partners who process, transmit, store, or have access to viastore data, systems, or services - whether operating in on-premises, hybrid, or cloud-based environments.

This policy does not supersede or grant any additional permissions beyond those established by other company policies, regulations, or directives from management - especially GDPR related topics.

3. Partner NDA Requirement

All partners must sign a Non-Disclosure Agreement (NDA) before gaining access to any information or data. This ensures that sensitive materials are protected and that all external collaborators are contractually bound to maintain confidentiality.

4. Information Security Requirements

Partners falling within the defined scope must comply with all applicable information security and data protection laws as well as adhere to the controls and requirements set forth in this section.

4.1 Designation of Key and Backup Users for Account Management

If **viastore** or any of its customers provides user accounts for network access the partner must appoint an authorized key user and a backup user who will be responsible for informing **viastore** of any personnel changes. The designated users will serve as the primary and secondary points of contact for all account-related updates and security matters.

viastore will periodically request confirmation from the designated key user to verify that all user accounts remain assigned only to active employees. User accounts that are not confirmed will be automatically deactivated.

4.2 Information Security Requirements for Third Parties

Prior to entering into a business relationship, a Third-Party Information Security Classification (TPIS) must be conducted (see Appendix – Third-Party Information Security Classification (TPIS)). This assessment forms the basis for a risk-based approach that takes into account the core security principles of confidentiality, integrity, and availability. Based on the results of this risk analysis, minimum contractual security requirements must be defined to ensure an adequate level of protection is established in all agreements and contracts.

For Partners identified as high-risk, with a low information security maturity level, or with a recent cyber incident, this may include remote or on-site audits to verify the implementation of required controls.

These measures help reduce security and supply chain risks for **viastore** and its customers, ensuring greater resilience and trust in **viastore**'s partnerships.

4.3 Maintain an Information Security Management System (ISMS)

Demonstrate implementation of an ISMS aligned with ISO/IEC 27001 or equivalent.

This includes NIS2 compliance.

4.4 Background Checks and NDA

Ensure employees involved in service delivery are vetted and have signed confidentiality and security agreements.

The security agreement shall at minimum define confidentiality, proper use of IT resources, access responsibilities, incident reporting, data handling, policy compliance, and post-employment obligations.

4.5 Access Management

The requirements set out in this section 3.4 apply to any account involved in providing services to **viastore** or its customers.

- Ensure least-privilege and need-to-know access to systems and data.
- Use multifactor authentication (MFA) for access.
- Maintain up-to-date access logs and ensure timely revocation of access upon role changes or contract termination.
- No shared accounts are permitted.

4.6 Change and Configuration Management

- All changes to systems must follow a documented and approved change control process.
- All configurations must be version-controlled and auditable.
- Environment Separation:

- Development, testing, and production environments must be strictly separated.
- No real production data shall be used in test environments unless explicitly approved and protected.

4.7 Alignment with viastore Confidentiality Policy

Handling of confidential data must strictly follow the **viastore** confidentiality and labeling policy. This includes proper classification, labeling according to **viastore**'s data classification scheme, and access control measures to prevent unauthorized disclosure or misuse.

4.8 Secure Handling and Exchange of Confidential Data

Confidential data must be handled and exchanged in a manner that consistently secures both its confidentiality and integrity. Confidential material must only be transferred and stored in encrypted form. The CIA triad - Confidentiality, Integrity, and Availability - must be maintained at all times.

Encryption of confidential or personal data in transit and at rest must use current industry standards (e.g., AES-256, TLS 1.2+).

4.9 Vulnerability and Patch Management

- Monitor for CVEs affecting the product or its dependencies.
- Apply security patches within 14 days of release for critical vulnerabilities.
- Perform regular vulnerability assessments and provide reports upon request.

4.10 Secure Update Mechanism

- Ensure updates are authenticated, integrity-protected, and traceable.
- Ensure all used scripts, utilities and programs are authenticated, integrity-protected, and traceable.

4.11 Incident Detection and Response

- Maintain incident response capabilities.
- Notify viastore of any security and data breach incident within 24 hours (alert@viastore.com).
- Provide incident reports and participate in coordinated response when required.

5. Data Protection Requirements

Partners must:

5.1 Ensure GDPR

- Process personal data in accordance with the GDPR and relevant national data protection laws.
- Support rights of data subjects (access, rectification, erasure, etc.).

5.2 Data Minimization and Purpose Limitation

- Collect and process only the data necessary for the performance of the contract.

5.3 Sub-processing

- Obtain prior written consent before engaging sub-processors.
- Ensure sub-processors meet the same security and data protection obligations.

5.4 Data Location

- Inform viastore of data storage locations.
- Store and process data within the EU or in countries with an adequate level of protection.

5.5 Data Deletion and Return

- Return or securely delete all data upon contract termination, as per the organization’s retention policy.
- Delete all configuration files, scripts, API keys, credentials etc. after the end of project or engagement.

6. Audit and Compliance

- The organization reserves the right to audit partner compliance with this policy.
- Partners must cooperate with audits and provide evidence of compliance upon request. This includes **viastore**’s annual partner self-assessment questionnaire.
- Non-compliance may lead to contract termination or legal actions.
- Audit rights must be contractually established in the primary agreement.

7. Provision of Information and Communication Technology (ICT) and integrated services

If the Partner delivers Information and communications technology (ICT) products or services that are integrated into the **viastore**’s or customer’s environment:

7.1 Compliance with CRA/IEC62443 Obligations

- Meet CRA /IEC62443 requirements for secure product development, vulnerability handling, and supply chain transparency.
- Appropriate controls shall be based on the outcome of a detailed risk and threat evaluation. Final approval of risk acceptance lies with the viastore CISO.

7.2 Security by Design and Default

- Ensure products include secure configurations by default and provide documentation of security features.

7.3 Software Bill of Materials (SBOM)

- Provide a current and accurate SBOM upon request.
- Inform the organization of any known vulnerabilities in components used.

7.4 Support and Updates

- Commit to a defined support and update period. The vendor shall guarantee the availability of updates and security fixes for a duration of five years, at minimum.
- Notify viastore about end-of-life (EOL) in advance.

8. Software Development Requirements

Partners involved in code development must:

8.1 Apply Secure Development Lifecycle (SDLC)

- Implement a formal SDLC process that includes threat modeling, risk assessment, secure design, secure coding, and peer code reviews.

8.2 Secure Development Practices

- Follow secure coding standards (e.g., OWASP).
- Perform code reviews and security testing (SAST, DAST) prior to deployment of software components that will be integrated into the organization’s systems.

8.3 Comply with Secure Coding Standards

- Follow standards such as OWASP Top 10, CWE, and SANS guidelines.

- Avoid use of deprecated or insecure libraries or functions.

8.4 Code Testing

- Perform static and dynamic security testing (SAST & DAST).
- Provide test results and fix vulnerabilities before delivery.

8.5 Version Control and Traceability

- Use version control systems (e.g., Git) with proper commit documentation.
- Ensure full traceability between requirements, code changes, and deployments.

8.6 Software Bill of Materials (SBOM)

- Provide a complete and accurate SBOM for each deliverable.
- Declare known vulnerabilities and dependencies used in the software.

8.7 No Backdoors or Unapproved Logic

- Partners must not implement hidden logic, hardcoded credentials, or telemetry mechanisms unless explicitly approved.

9. Intellectual Property and Source Code Ownership

Unless otherwise provided in the main agreement, the following shall apply:

- All developed code, scripts, and configurations are the intellectual property of **viastore**, unless otherwise stated.
- Partner may not reuse code or configurations across customers unless open-source or explicitly permitted.

10. EU Data Act Compliance

All partner and suppliers must handle data on behalf of **viastore** or any **viastore** customer in full compliance with the EU Data Act, ensuring transparency, interoperability, and secure data sharing. This includes all products or services delivered as part of a customer project or installation.

10.1 Requirements

- **Data Access & Portability:** Partners and suppliers must enable secure, real-time access to data generated by products/services, in machine-readable formats, upon request by **viastore** or customer.
- **Data Sharing Governance:** Partners and suppliers must implement technical and organizational measures to ensure lawful, fair, and non-discriminatory data sharing.
- **Security & Confidentiality:** All shared data must be protected using encryption, access controls, and audit trails. Suppliers must comply with GDPR and NIS2 obligations.
- **Sub-Processor Disclosure:** Partners and suppliers must disclose all sub-processors and ensure they meet equivalent compliance standards.
- **Data Deletion & Return:** Upon contract termination, partners and suppliers must securely delete or return all company data.

11. EU AI Act Compliance

All partners and suppliers must develop, deploy, or integrate AI systems in full alignment with the EU AI Act and the **viastore**'s ethical standards. This includes all products or services delivered as part of a customer project or installation.

11.1 Requirements

- **Risk Classification:** Partners and suppliers must assess and document the risk level of any AI system (Prohibited, High-Risk, Limited, Minimal) per EU AI Act Article 6.
- **High-Risk AI Systems:** Must include CE marking, risk logs, human oversight mechanisms, and be registered in the EU database.
- **Transparency Obligations:** Partners and suppliers must clearly label synthetic content, disclose AI usage to users, and provide documentation on training data and model behavior.
- **Incident Logging:** Partners and suppliers must log and report serious incidents or malfunctions involving AI systems.
- **Ethical Use:** AI systems must not be used for social scoring, biometric categorization, or manipulative behavior unless explicitly authorized.
- **Security by Design:** AI systems must be developed with embedded security controls, traceability, and explainability.
- **Third-Party AI Tools:** Partners and suppliers using third-party AI must ensure those tools are compliant with EU AI Act and GDPR.

11.2 Policy on Ownership and Use of AI-Generated Models and Data

All AI models developed for **viastore** and **viastore**'s customers - including but not limited to large language models (LLMs) - as well as any data generated by these models (outputs, predictions, responses, etc.), are the exclusive intellectual property of **viastore**. The use of any internal or confidential data for the purpose of training, fine-tuning, or otherwise enhancing AI systems must be explicitly authorized in writing by the **viastore** Management Board or the CISO. Unauthorized use, sharing, or external disclosure of such models or their outputs is prohibited.

12. Training and Awareness

Partners shall ensure that all employees and contractors involved in the provision of services receive appropriate and regular training on cybersecurity and data protection.

This includes training on **viastore** procedures and policies. The content of the trainings will be selected by **viastore**.

13. Policy Acknowledgement

This policy shall be incorporated by reference into the main agreement. Partners must acknowledge and agree to its terms before initiating any data processing or service delivery.

Each Partner must sign the **viastore** "Agreement on the use of **viastore** IT facilities" (1.034).

Each employee with access must acknowledge the awareness by signing "Declaration on the use of **viastore** IT facilities for external user" (1.034-1).

14. Appendix - Third-Party Information Security Classification (TPIS)

14.1 Objective

The purpose of the TPIS process is to assess and classify Partners based on the information security risk they pose to **viastore** or **viastore** customers. This ensures proportionate and risk-aligned security controls throughout the lifecycle of the product or service.

14.2 Scope

Applies to all Partners that:

- Deliver products or services with digital components;
- Access, process, transmit, or store viastore or customer data or
- Are critical to the supply chain or fulfillment of contractual obligations.

14.3 Classification Levels

Level	Description	Examples	Typical Controls Required
High	Significant impact on operations, data, or compliance if compromised	Cloud providers, software integrators, hosting providers	Full security questionnaire, ISO 27001 or equivalent proof, audit rights, on-site audit
Medium	Moderate access to systems or data, or key operational dependencies	Remote service technicians, logistics software partners	Security self-assessment, confidentiality agreement, contract clauses
Low	Minimal or no digital access; limited operational dependency	Hardware suppliers without software, office equipment vendors	Basic NDA, security awareness confirmation

14.4 Risk Factors Considered

- Access to viastore or customer data (type, volume, sensitivity)
- Access to viastore systems or networks
- Criticality to operational continuity or supply chain
- Involvement of digital components (firmware, connectivity, APIs)
- Previous security incidents or maturity gaps
- Hosting model (on-premises, hybrid, cloud)

14.5 Classification Process

1. Initiation: Triggered before contract signature or onboarding.
2. Data Collection: Via cloud and supplier questionnaires and technical documentation.
3. Risk Assessment: Performed by Information Security and Procurement jointly.
4. Classification Assignment: Based on the predefined criteria above.
5. Documentation: Recorded in supplier risk register and ERP/sourcing tool.
6. Review Frequency: At least every 24 months or after significant changes.

14.6 Enforcement and Escalation

- High-risk suppliers may be subject to on-site audits, additional contract clauses, or onboarding delays until security gaps are resolved.
- Final classification decision and mitigation plan approval lies with the **viastore** CISO.

14.7 Benefits

- Aligns third-party controls with business risk.
- Enhances supply chain security and resilience.
- Supports compliance with ISO 27001, NIS2, any other information security and data protection laws and customer requirements.