Information Security Policy

Sigma Capital Jakub Jasiński

Document version	1.0	**Effective date**	2026-09-03
Policy owner	Owner / Managing Director	**Next review**	2027-09-03

---

1. Purpose and scope

This policy defines how Sigmapack protects the confidentiality, integrity and availability of the information it processes, including personal data of customers and data obtained through connected e-commerce platforms.

The policy applies to all systems, applications, devices and third-party services used to operate our online retail business, and to every person acting on our behalf, including owners, employees and contractors. It covers our internal order management application, the databases supporting it, connected marketplace and logistics integrations, and the workstations and devices used to access them.

2. Governance and responsibilities

Sigmapack is a small organization. Accountability for information security rests with the Owner / Managing Director, who approves this policy, allocates resources for security measures, and reviews the policy at planned intervals.

- The policy owner approves access rights and reviews them when roles change.
- Everyone who processes company or customer data is required to follow this policy.
- Suspected security incidents must be reported to the policy owner without delay.

3. Data classification and handling

We classify information into three levels and handle it accordingly:

- **Confidential** — customer personal data (name, address, phone, e-mail), order contents, API credentials, database credentials and access tokens. Accessible only to authorized personnel on a need-to-know basis.
- **Internal** — sales statistics, settlement and commission data, operational records. Restricted to the organization.
- **Public** — product listings, published policies such as this document.

We do not store payment card data. Payments are processed by the marketplace or payment provider; our systems never receive or retain full card numbers, CVV codes or

bank credentials.

4. Access control

- Access to internal applications requires authentication and is limited to authorized users.
- Access rights follow the principle of least privilege — users receive only the permissions required for their duties.
- Accounts are personal and must not be shared. Credentials are never transmitted through unsecured channels.
- Access is revoked promptly when a person no longer requires it, and reviewed when responsibilities change.
- Administrative interfaces of hosting, databases and connected platforms are protected by strong, unique passwords and, where the provider supports it, multi-factor authentication.

5. Credential and secret management

- API keys, application secrets and access tokens are stored in server-side configuration files outside of version control and are never embedded in client-side code.
- Web server rules deny direct HTTP access to configuration files containing secrets.
- Access tokens obtained from connected platforms are stored server-side, refreshed automatically before expiry, and are never exposed to end users.
- Secrets are rotated when a compromise is suspected, when a person with access leaves, or when required by the platform provider.

6. Encryption and network security

- Traffic between end users and our applications, and between our systems and third-party APIs, is protected using TLS (HTTPS).
- Requests to partner APIs are cryptographically signed where the provider requires it, using HMAC-SHA256 with a secret held only on the server.
- Database services are not exposed to the public internet and are reachable only from authorized hosts.
- Remote administrative access to servers and devices uses encrypted protocols.

7. System and application security

- Operating systems, runtimes, libraries and applications are kept up to date, with security updates applied promptly.
- User input is validated, and database access uses parameterized queries to prevent injection attacks.
- Output rendered in web pages is escaped to prevent cross-site scripting.
- Only the services required for business operations are enabled; unused accounts,

endpoints and services are removed or disabled.

- Devices used to access company systems run supported operating systems with anti-malware protection and disk encryption where available.

8. Logging and monitoring

- Application and server logs record authentication events, integration errors and significant operations such as document issuance and fulfilment actions.
- Logs are reviewed when investigating incidents or unexpected behaviour.
- Logs must not contain plaintext secrets, access tokens or payment data.

9. Backup and recovery

- Business-critical data, including the operational database, is backed up regularly.
- Backups are stored separately from the primary system.
- Restoration is verified periodically so that recovery is possible after data loss, hardware failure or a security incident.

10. Third-party and vendor management

We rely on external providers for hosting, payment processing, marketplace integration, fiscal document issuance and logistics. Before granting a provider access to our data we assess whether it offers adequate security and privacy safeguards.

- Providers receive only the data necessary to deliver their service.
- Integrations request the minimum set of API permissions required for the intended function.
- Access granted to a provider is revoked when the service is no longer used.
- Data obtained from connected platforms is used solely to operate our own sales, fulfilment, accounting and customer-service processes, and is not sold or shared for unrelated purposes.

11. Incident response

When a security incident is suspected or confirmed, we follow these steps:

- **Report** — anyone noticing a suspected incident informs the policy owner immediately.
- **Contain** — affected accounts are disabled, exposed credentials revoked and rotated.
- **Assess** — we determine what data was affected and the scope of the impact.
- **Notify** — where personal data is affected, we notify the competent supervisory authority within 72 hours of becoming aware, as required by the GDPR, and inform affected individuals when the incident is likely to result in a high risk to their rights and freedoms. Affected platform partners are notified in line with their terms.
- **Recover and learn** — services are restored from clean backups, and we record

the cause and the corrective actions taken.

12. Data retention and deletion

- Personal data is retained only as long as necessary for the purpose for which it was collected, or as required by applicable accounting and tax law.
- Transaction and fiscal records are retained for the statutory period required by Polish tax regulations.
- Data that is no longer required is deleted, and storage media are securely wiped or destroyed before disposal.

13. Privacy and data subject rights

We process personal data in accordance with Regulation (EU) 2016/679 (GDPR). Processing is limited to what is necessary for order fulfilment, customer service, accounting and legal compliance.

- We apply data minimisation — we collect only the data required for these purposes.
- Individuals may request access to their data, correction, deletion, restriction of processing, or portability, by contacting us at the address below.
- Requests are handled without undue delay and within the statutory time limits.

14. Awareness and training

- Everyone with access to company systems is made aware of this policy and their responsibilities under it.
- We maintain awareness of common threats, in particular phishing, credential theft and social engineering.
- Security expectations are communicated before access is granted.

15. Policy review

This policy is reviewed at least annually, and additionally after a significant security incident, a material change to our systems or integrations, or a change in applicable law. Updates are approved by the policy owner, and the version and effective date at the top of this document are updated accordingly.

16. Contact

Questions regarding this policy, security concerns, or requests relating to personal data should be directed to: jakub@sigmapack.pl.

Approved by Owner / Managing Director, Sigma Capital Jakub Jasiński. This document is published at the organization's website and is reviewed at least annually.