Information Security Statement - iotspot B.V.

1. Commitment to Information Security

At iotspot we are committed to safeguarding information assets through robust security measures, continuous improvement, legal compliance, and ISO 27001 standards, ensuring the highest level of protection and trust for our stakeholders.

We recognize that information security is a shared responsibility. Therefore, we ensure that security measures are ingrained in every process, from system design and development to service delivery and customer interaction. Our goal is to minimize risk and maximize resilience in the face of evolving threats.

2. Objectives of Information Security

We aim to protect our customers' data, reduce security incidents, and ensure business continuity through systematic risk management and security controls, according to the established ISO 27001 standard. We actively promote security awareness, educating employees on information security best practices and their roles in maintaining the organization's security policies.

3. Scope of the ISMS

Our ISMS encompasses all operational areas where information is processed, stored, transmitted, or handled. This includes, but is not limited to:

- Software Development: ensuring security in the development, testing, and deployment of software solutions for IoT and other technological applications.
- Hardware Development: ensuring secure development and deployment of IoT devices.
- Cloud Hosting: protecting data stored within cloud, applying robust encryption and access control mechanisms.
- Internal Business Operations: this includes all aspects of our sales, customer relationship management (CRM), order to collection, and purchase to pay

processes. We handle sensitive information in our financial, HR, and operational processes with the utmost care.

- Third-Party Management: security controls are applied to all external vendors, suppliers, and business partners who have access to our data or systems, ensuring that their security measures align with our high standards.

4. Roles and Responsibilities

The leadership team of iotspot B.V. is ultimately accountable for the success and maintenance of the ISMS. The Security Officer is responsible for managing the ISMS, implementing security policies, and ensuring compliance with both internal and external standards.

Key responsibilities include:

- Leadership: Direct accountability for ensuring information security is maintained across all areas of the business.
- Security Officer: Ensures that security policies are properly implemented, oversees audits and assessments, and coordinates incident response efforts. The Security Officer is also tasked with driving security initiatives and reviewing the performance of security controls.
- Employees: Every employee is responsible for following security policies and procedures. Employees must comply with confidentiality agreements, report potential security incidents, and participate in regular security training and awareness programs.
- Third-Party Vendors: We carefully vet third-party service providers to ensure they comply with our information security standards, including regular reviews and audits of their security controls.

5. Risk Management Commitment

We are dedicated to proactive risk management. Our process involves:

- Risk Identification: we regularly identify security risks through threat intelligence, internal audits, and vulnerability assessments.

- Risk Assessment: all identified risks are assessed based on their potential impact on the organization and likelihood of occurrence.
- Risk Treatment: mitigation strategies are developed for identified risks, with risk treatment plans designed to reduce or eliminate risks. This may include technical controls, administrative controls, or physical security measures.
- Incident Response: should an incident occur, our team is trained and equipped to respond swiftly, investigate thoroughly, and mitigate any damage. Post-incident reviews are conducted to prevent reoccurrence and to refine our security posture.
- Documentation and Reporting: all risk management activities are documented, and regular reports are provided to senior leadership to ensure accountability and transparency.

6. Compliance with Standards

We maintain full compliance with ISO 27001, the international standard for information security management. In addition to ISO 27001, we adhere to relevant regulations such as the General Data Protection Regulation (GDPR) and industry-specific standards. Our ISMS is regularly audited, both internally and externally, to ensure compliance and identify areas for improvement.

7. Continuous Improvement

At iotspot, information security is an evolving process. We are committed to:

- Regular Audits and Management Reviews: both internal and external audits are conducted to assess the effectiveness of our ISMS.
- Learning from Incidents: we analyze any security incidents or near-misses to strengthen our systems and prevent future occurrences.
- Security Awareness: we continually monitor the information security landscape, staying up to date with new threats, technologies, and best practices. We proactively adopt new security measures to enhance our protection.
- Feedback Loops: feedback from stakeholders, including customers, employees, and partners, is used to continuously refine our security policies and practices.

8. Communication and Awareness

We recognize that information security is only as strong as the people who enforce it. To that end, we provide:

- Training Programs: regular and mandatory training for all employees, ensuring they are up to date on the latest security threats and best practices.
- Stakeholder Communication: regular communication to all stakeholders about their roles in maintaining security and how they can help protect our organization's data.
- Security Alerts: timely notifications of any emerging security risks or vulnerabilities, both internally and externally.

9. Review and Revision Schedule

This Information Security Statement will be formally reviewed at least once a year, or sooner if necessitated by significant changes to our business environment or security landscape. Any revisions will be documented, and stakeholders will be notified of the changes. We also reserve the right to modify or amend this statement in accordance with changes to applicable laws and regulations.