Information Security Policy

1. Purpose, scope and target audience of policy

This document defines the organisation's information security policy and thus the overarching objective of the Information Security Management System (ISMS). This document defines the purpose, orientation, principles and general regulations for the ISMS.

The information security policy defined in this document relates to the entire ISMS in accordance to the defined scope of the ISMS.

The users of this document are all employees of the organisation, relevant external third parties, and contractors who have an active role in or are affected by the ISMS.

2. Terms of information security

Term	Meaning
Confidentiality	The characteristic that information is not made accessible or disclosed to unauthorised persons, facilities or processes
Integrity	The accuracy and completeness of the information
Availability	The characteristic that information can be accessed and used by an authorised body if required
Information security	Maintaining the confidentiality, integrity and availability of information
Information Security Management System (ISMS)	Management procedure that deals with the planning, implementation, maintenance, review and improvement of information security
Risk	The effect of uncertainty on objectives, expressed as a combination of the likelihood of an event and its consequence (ISO 31000)
Information asset	Any item of information or information-processing facility that has value to the organisation, including data, systems, personnel, and physical items
Statement of Applicability (SOA)	Document listing all ISO 27001 Annex A controls, their applicability, implementation status, and justification for inclusion or exclusion

3. Importance of information security

3.1. Business objectives

Our business objective of "Fueling humanity with AI robotics" is only achievable when adhering to information security protocols in every aspect of our activities.

3.2. Relevant requirements and interested parties

The company is subject to the following requirements:

- Customer requirements,
- Contractual requirements,
- Legal requirements
- Regulatory requirements (including but not limited to GDPR, EU AI Act, NIS2 where applicable)

Interested parties include (not limiting to) the following groups:

- Employees,
- Customers,

- Investors,
- Stakeholders,
- Management Board,
- Suppliers,
- External partners,
- Regulators.
- Data subjects (individuals whose personal data is processed),
- Certification bodies.

3.3. Information security

Information security is a high priority in line with our business objectives. The objectives for the ISMS are derived from the organisation's business strategy described in section 3.1 and the relevant requirements and interested parties described in section 3.2.

Information Security is therefore of paramount importance to implementing our mission of fueling humanity with AI robotics.

3.4. ISMS objectives

The objectives of the information security management system are derived from the business objective described in section 3.1 and from the requirements of the interested parties described in section 3.2. Each objective acts on at least one of the protection goals of confidentiality, integrity and availability, and gives direction to the prioritisation of security measures and to the determination of protection needs in risk management.

ID	Objective	Protection goal	Responsible department
O1	Ensure the availability of the cloud-based production control, so that customer kitchen installations remain operable	Availability	Software Engineering & Platform
O2	Prevent unauthorised or erroneous changes to the control, recipe and order data that govern food preparation	Integrity	Software Product, Robotics & Automation
O3	Deliver CircusOS releases without unresolved critical security findings	Integrity, availability	Software Engineering & Platform
O4	Prevent the unauthorised disclosure of source code and intellectual property	Confidentiality	Software Engineering & Platform, Hardware & Manufacturing
O5	Prevent impermissible data flows out of the segregated China region environment	Confidentiality	Software Engineering & Platform, Operations
O6	Protect customer data and end-user personal data in accordance with the applicable legal, regulatory and contractual obligations	Confidentiality, integrity	Operations, Finance & Legal

Certification against ISO/IEC 27001, the delivery of training and awareness measures, and the continual improvement of the ISMS are means of achieving these objectives rather than objectives in their own right. Their fulfilment is monitored as ISMS performance indicators in accordance with clause 9.1 and reported in the management review.

For each objective, the measurable targets, the key performance indicators, the responsible role, the resources and the evaluation cycle are defined in the record "Information Security objectives" in accordance with the Procedures for Information Security Objectives & KPIs. The objectives are documented and their fulfilment is checked in accordance with section 3.5.

3.5. Planning and reviewing the objectives of the ISMS and their fulfillment

When planning how the objectives of the ISMS should be achieved, the planned measures, resources, responsibilities, time targets and the assessment method for the review must be defined. The points must be documented. The objectives of the ISMS and their fulfilment must be reviewed annually. The person responsible for carrying out the review, analysing the results of the review and preparing a review report for management is the Information Security Officer.

The review must include an evaluation of whether objectives remain aligned with the organisation’s risk landscape and business strategy. Any changes to objectives must be approved by the Management Board and communicated to all relevant parties.

3.6. Information security measures

The organisation commits to comply with the information security requirements as defined in the subject-specific information security policies and ISO/IEC 27001. Suitable information security controls are identified, defined and reviewed within the risk management framework in the risk assessment and risk treatment methodology.

The applicable information security measures, their implementation status and any exceptions are documented in the Statement of Applicability (SOA). Responsible for the SOA is the Information Security Officer. The SOA must be filed in accordance with the chapter "Management of records to this document".

Any exceptions or deviations from required controls documented in the SOA must include a formal risk acceptance signed by the relevant risk owner and approved by the Management Board. Exceptions must be time-limited and reviewed at least annually.

4. Responsibilities

The following responsibilities exist within the ISMS:

Responsible for	**Job title**
the correct implementation and maintenance of the ISMS in accordance with the information security guideline and ensuring that sufficient resources are available for this.	Management Board
coordinating the operation of the ISMS and reporting on its performance.	Information Security Officer
ensuring that annual reviews of the ISMS and any significant changes are carried out and recorded.	Information Security Officer
the information security awareness of all employees as well as their education and training on the subject of information security.	HR
ensuring the integrity, confidentiality and availability of the assets or information for which the person is responsible.	Asset owner
the reporting of information security incidents or vulnerabilities.	All employees
the handling of information security incidents and vulnerabilities.	Information Security Officer
the definition of the information that is communicated to interested parties in the context of information security.	Management Board
ensuring that third-party and vendor access to information assets complies with the organisation’s security requirements and contractual obligations.	Information Security Officer
ensuring that information security considerations are integrated into all projects from initiation through completion.	Project Managers / Information Security Officer

All key responsibilities and recurring tasks in the ISMS are managed and documented by the Task Manager in the Digital Compliance Office (DCO).

5. Policy

Information security is anchored at the highest management level of the organisation. The organisation's management is committed to the ISMS in accordance with the requirements of ISO/IEC 27001 and the requirements of risk management in order to adapt the system to constantly changing business conditions and to ensure that the necessary resources are provided. This should enable all relevant ISMS stakeholders to achieve the information security objectives and continuously improve the ISMS. The management is also responsible for implementing the company policy.

The Management Board demonstrates its commitment to the ISMS by: (a) ensuring the information security policy and objectives are compatible with the strategic direction of the organisation, (b) ensuring the integration of ISMS requirements into the organisation’s business processes, (c) ensuring the resources needed for the ISMS are available, (d) communicating the importance of effective information security management and conformance with ISMS requirements, and (e) directing and supporting persons to contribute to the effectiveness of the ISMS.

6. Obligations and responsibilities in the area of information security

All employees and relevant third parties must be familiar with the organisation's information security policy and the ISMS. All employees must act in accordance with the information security policy, the topic-specific information security policies and all requirements specified by the management. If company policies are violated, disciplinary action may be taken. The management is responsible for communicating the information security policy and emphasising the importance of the ISMS and the company-wide commitment to information security.

Employees and relevant third parties must acknowledge their understanding of and commitment to this policy in writing (or electronically) upon onboarding and annually thereafter. Records of acknowledgement must be maintained in accordance with the “Management of records to this document” section.

For disciplinary procedures related to policy violations, the requirements defined in the Compliance Policy (Section 8 - Disciplinary proceedings) apply.

7. Communication

The organisation must determine the need for internal and external communications relevant to the ISMS, including what shall be communicated, when, to whom, and by whom. A communication matrix must be maintained and reviewed annually. The communication matrix is referenced in Section 8 (Management of records to this document).

8. Referenced documents

The following documents are referenced:

- Scope of the Information Security Management System
- Procedure for Identifying Requirements
- Procedures for Information Security Objectives & KPIs
- Procedure for Corrective Actions
- Policy on Risk Management
- Statement of Applicability (SOA)
- Compliance Policy
- Policy for the Classification of Information and Assets
- Policy on Handling Information Security Incidents

9. Management of records to this document

The following records are kept for this document:

- Information Security objectives
- Report on ISMS objective achievement
- Management Review
- Appointment of the Information Security Officer
- Resource planning
- Overview of Legal, Statutory, Regulatory, Contractual and other Requirements
- Statement of Applicability (SOA)
- Communication matrix
- Risk acceptance records for SOA exceptions
- Policy acknowledgement records
- ISMS training and awareness records

The records must be kept in accordance with the procedure for the control of documents and records.

10. Document control

This document is valid from 17.10.2025.

The owner of this document is the Information Security Officer, who must review the document at least once a year and update it if necessary.

At least the following criteria must be taken into account when evaluating the document for effectiveness, appropriateness and possible need for adjustment:

- Results of internal and external audits
- Results of the KPI evaluation
- Results of the management reviews
- Adjustments resulting from risk management or corrective actions
- Changes in legal, regulatory, or contractual requirements
- Significant information security incidents or near-misses
- Changes to the organisation’s business objectives, risk environment, or technology landscape

Approvals

Approved by Jan Sorgenfrei on 13/11/2026 at 09:26