Information Security Policy

Introduction

At Threedy, we both *provide* Information Technology (IT) and *use* it: our customers entrust critical data to us and our products; we entrust our own data to the devices, applications, and services that we use.

Unfortunately, IT has become risky: criminals from all over the world readily exploit any weakness or error they find in the design, configuration, or usage of devices and applications. The consequences of being "hacked" can be dire: loss of time, money, reputation, and, ultimately, loss of business.

To avoid that, we all must take action to minimize the security risks in the IT products and services we use as well as in those we offer. This way we protect information - ours and our customers'!

This policy describes the most fundamental information security provisions at Threedy. It will be complemented over time by more specific policies as needed.

This policy has been reviewed and formally approved by Threedy's Managing Directors:

Page Approval Status	APPROVED
Date of Approval	Tuesday, 22 Jul 2025, 10:46 am UTC
Date of Expiry	N/A
Current Page Version	27
Approved Page Version	27

Approver	Status	Approval Date
Christian Stein	APPROVED	Tuesday, 22 Jul 2025, 10:46 am UTC
Markus Lindemann	APPROVED	Tuesday, 22 Jul 2025, 8:48 am UTC

Approver	Status	Approval Date
Maik Thöner	APPROVED	Tuesday, 22 Jul 2025, 8:21 am UTC

Scope

This policy is binding for all employees at Threedy (including working students and interns), and for all contractors and subcontractors acting in Threedy's name, and it applies to all work settings (both Threedy's office space and mobile working).

Basic Definitions

Information security means protecting three properties of information:

1. ***Confidentiality***: information must only be accessible to those authorized to access it.
2. ***Integrity***: information must only be modifiable by those authorized to modify it.
3. ***Availability***: information must be available whenever needed by those authorized to use it.

The exact level of protection required for each property varies and is determined by the type and value of information, and by what contracts, laws, and regulations dictate. For example: there is no requirement to keep confidential the information in a marketing post which has already been published on our website. On the other hand, we must always protect personal data in specific ways according to the GDPR, and customer data according to the NDAs we sign with them.

Protection requirements are met by selecting, implementing, and monitoring measures which support one or more of the above-mentioned properties. Such measures can be technical (e.g., using a particular type of firewall) or organizational (e.g., do a yearly training in cybersecurity) and are commonly called ***controls***.

Principles of Information Security at Threedy

The following are the guiding principles of information security at Threedy:

1. We commit to fulfill the information security requirements from our contracts with customers, suppliers, and partners.
2. We commit to fulfill the information security requirements from relevant laws and regulations, such as GDPR and NIS-2.
3. Our information security management is risk-based, that is, information security controls must be proportionate to the likelihood and the potential impact of security threats.
4. Our information security management is iterative, that is, information security controls are planned, implemented, and then regularly checked to identify issues or opportunities for

improvement.

Threedy's Information Security Management System

Threedy hereby establishes an ***Information Security Management System*** (ISMS), which consists of the policies, procedures, guidelines, and related resources and activities, managed by Threedy, with the overall goal of implementing the above-mentioned principles of information security.

ISMS Objectives

The ISMS will achieve that goal by pursuing, among others, the following objectives, each of which serves the interests of a particular group of stakeholders:

Stakeholders	Objectives
Management	• Enable governance in matters of information security. • Provide a factual and risk-based assessment of Threedy's information security posture. • Continuously improve Threedy's information security posture.
Employees	• Increase awareness for potential security threats. • Increase command of information security solutions and risk-mitigating behaviors. • Increase capacity to respond to information security incidents. • Minimize information security risks in all work setings.
Investors	• Minimize investment risks due to cybersecurity and non-compliance.
Customers	• Increase the trustworthiness of Threedy as supplier. • Increase the attractiveness of the offered products and services. • Increase awareness for contractual information security requirements. • Avoid non-compliance with known contractual information security requirements.

Suppliers & partners	• Increase the trustworthiness of Threedy as customer or partner. • Increase awareness for contractual information security requirements. • Avoid non-compliance with known contractual information security requirements.
Public authorities and regulators	• Increase awareness for statutory information security requirements. • Avoid non-compliance with known statutory information security requirements.

ISMS Roles and Responsibilities

The ISMS is designed and operated by an ISMS Management Team (currently: CTO and Head of Quality & Compliance) with full support from and under the regular supervision of the Managing Directors.

Every department and every employee is responsible to fully support and implement the information security controls, both organizational and technical, applicable to them.

Roles	**Responsibility**
ISMS Management Team **(CTO + Head of Quality & Compliance)**	Design and operate the ISMS. Select, implement, and operate organizational and technical controls.
Managing Directors	Periodically review the ISMS and Threedy's information security posture.
IT	Select, implement, and operate technical controls.
System owners/administrators outside of IT	Implement and operate the applicable technical controls.
Employees	Support and implement the applicable information security controls.

Violations

Violations of information security obligations set forth by this and related policies will not be tolerated and, depending on the nature and severity of the violation, disciplinary action may be taken.

In the event of a suspected information security violation, the following procedure applies:

1. **Investigation**	The suspected violation is investigated by the ISMS Management Team, the employee's line manager, and HR, respecting the employee's privacy rights under GDPR and BDSG.
2. **Hearing**	Before any disciplinary action, the affected employee is informed of the allegations and given an opportunity to respond.
3. **Sanctions**	Possible measures, depending on the severity and recurrence of the violation, include: • **Verbal warning** (mündliche Abmahnung) • **Written warning** (schriftliche Abmahnung) • **Temporary suspension** (bezahlte/unbezahlte Freistellung, only if legally justified) • **Termination** (Kündigung; only in severe or repeated cases and in compliance with Kündigungsschutzgesetz)

All steps will be documented in accordance with data protection laws.

In cases where a violation results in significant damage, harm, or constitutes a breach of applicable laws or regulations, the company reserves the right to initiate civil or criminal proceedings, in accordance with the applicable statutory provisions and after due consideration of all circumstances. Such measures will only be taken when legally justified and in compliance with employee rights and data protection regulations.