Information Security Policy

Workpath takes special care in handling all sensitive data handed to us by Customers, Employees and Partners. To ensure even higher levels of security, Workpath has certified its Information Security Management System (ISMS) according to the ISO/IEC 27001:2022 standard.

Scope of the ISMS

The Workpath platform for outcome-focused strategy execution as well as the product and engineering departments. Included are respective infrastructure services and supporting processes that empower Workpath's customers to implement and accelerate outcome management within their organization.

The importance of information processing

Information processing plays a key role in the fulfillment of our tasks. All essential strategic and operative functions and tasks are significantly supported by information technology (IT). Overall, it must be possible to compensate for a failure of IT systems in the short term. Our business must not be allowed to collapse even in sub-areas.

Security objectives

All activities to maintain and improve information security are aimed at ensuring the basic values of confidentiality, integrity and availability of information and, in particular, our customer data.

The specific security measures must be economically proportional to the need for protection of the data processed. As a core activity for maintaining and improving information security, risks to information security are continuously identified, evaluated and dealt with. Various legal, official and contractual requirements are placed on information security, which are continuously identified and taken into account for information security.

Security organization

To achieve the information security objectives, an information security officer (ISO) has been appointed by management.

An information security management system (ISMS) has been introduced throughout the company and is regularly reviewed for its effectiveness.

Management is responsible for security organization. The information security officer advises management on the planning and implementation of information security within the company. In his/her function, he/she reports directly to management as required, but at least once a year in the management review.

Workpath GmbH • Ridlerstr. 39 • 80339 München • Amtsgericht München HRB 230902

The information security officer is provided by management with sufficient financial and time resources to receive regular training and information.

The information security officer is to be involved in all projects at an early stage in order to take security-relevant aspects into account as early as the planning phase.

A data protection officer has been appointed. The data protection officer has an adequate time budget for the fulfillment of his/her duties. The data protection officer is required to participate in continuous further training.

Security measures

For all procedures, information, IT applications and IT systems, a responsible person is appointed who determines the respective security requirements and grants access authorizations.

Substitutes must be set up for all responsible functions. It must be ensured by means of instructions and sufficient documentation that substitutes can fulfill their tasks.

Buildings and premises are protected by adequate access controls. Access to IT systems is protected by appropriate access controls and access to data by a restrictive authorization concept.

Anti-virus protection software is used wherever it makes sense, but especially on employee PCs. All Internet access is secured by a suitable firewall. All protection programs are configured and administered in such a way that they provide effective protection and prevent manipulation. In addition, IT users support these security measures by working in a security-conscious manner and, in the event of anomalies, inform the appropriately designated points.

Data loss can never be completely ruled out. Comprehensive data backup therefore ensures that IT operations can be resumed at short notice if parts of the operational data stock are lost or obviously incorrect. Information is uniformly marked and stored in such a way that it can be found quickly.

In order to limit or prevent major damage as a result of emergencies, security incidents must be responded to quickly and consistently. Measures for emergencies are compiled in a separate emergency prevention concept. It is our goal to maintain critical business processes even in the event of a system failure and to restore the availability of the failed systems within a tolerable period of time.

If any IT services are outsourced to external parties, we specify specific security requirements in the service level agreements. The right to control is defined. For extensive or complex outsourcing projects, we draw up a detailed security concept with concrete specification of measures.

IT users regularly take part in training courses on the correct use of IT services and the associated security measures. The company management supports necessary further education and training.

Security improvement

The information security management system is regularly reviewed for its accuracy and effectiveness. In addition, the measures are also regularly examined to determine whether they are known to the

employees concerned and whether they can be implemented and integrated into the operating process.

Management supports the continual improvement of the level of security. Employees are required to communicate possible improvements or weaknesses to the relevant departments.

The desired level of security and data protection is ensured by continual revision of the regulations and their compliance. Deviations are analyzed with the aim of improving the security situation and keeping it constantly up to date with the latest IT security technology.

Obligations to cooperate

Management is committed to its task of supporting the information security objectives described in this policy and calls on all employees to also contribute to maintaining or improving information security.

Munich, Oct 21, 2026

Stephanie Streitner
Managing Director
Workpath GmbH

Steffen Wenz
Information Security Officer
Workpath GmbH