



INFORMATION SECURITY MANAGEMENT SYSTEM

FYBU Digital Solution GmbH

Information Security Policy

CLASSIFICATION

Public

VERSION

1.0

DATED

15.09.2026



1 Purpose

FYBU Digital Solution GmbH develops and operates Fybu, a cloud-based digital accounting platform for businesses and tax professionals. Our customers entrust us with business-critical financial and personal data. This policy sets out the approach and objectives of our management for protecting that information, and communicates them to our employees, customers, partners and other interested parties.

Our Information Security Management System (ISMS) is designed to ensure the confidentiality, integrity and availability of all information assets, and to prevent any breach of legal, regulatory or contractual obligations. It is established in accordance with ISO/IEC 27001:2022 and operated as a process of continual improvement following the Plan-Do-Check-Act cycle.

Information security is not only a technical matter and not only the task of our IT team. It covers physical security, people, communication, software development and operations, and it can only succeed with the participation of every employee and partner. This policy is the top-level document of our ISMS; detailed rules are defined in supporting policies and procedures.

2 Information Security Principles

- **Confidentiality:** Information is accessible only to authorized persons, within the limits of their authorization.
- **Integrity:** Information is complete, accurate and protected against unauthorized modification.
- **Availability:** Information and systems are available and usable whenever authorized users need them.

Information is shared only when its owner permits it, when access has been authorized, or when the law requires it. Personal data is processed in compliance with the GDPR and protected with appropriate technical and organizational measures.

Information security risks are identified and assessed by the people responsible for the related assets, prioritized and treated with suitable controls. The security of the Fybu platform, its hosting environment and our customers' data is given the highest priority, so that customers can rely on secure and uninterrupted service. Our decisions are based on objective information and recognized good practice, and we invest continually in technology and know-how.

3 Information Assets

Information assets are everything that is important for FYBU Digital Solution GmbH to operate without interruption. This policy covers:

- All information and data in paper, electronic, visual or audio form
- The software and hardware used to access, process and store information, including the Fybu platform
- The networks and cloud services used to transfer and host information
- Our teams and employees
- Our offices and restricted areas
- Our solution and integration partners



- Services provided by third parties, such as hosting and data center providers

4 Use of Information Assets

Sharing knowledge is essential for our work, but it must always respect the sensitivity of the information. The effort and cost of protecting information are proportionate to its value and sensitivity. Using FYBU information resources for unethical or illegal purposes is not acceptable under any circumstances. In particular, the following are prohibited:

- Intentionally altering or falsifying data, or deliberately causing data errors or data loss
- Using information resources for activities that violate the law
- Violating or circumventing information security controls
- Stealing or destroying devices, software or other information resources
- Using information resources in a way that impairs the performance of our systems
- Damaging facilities, equipment or networks

Such actions are treated as disciplinary offences and may lead to legal action. Any security breach, attempted breach or weakness must be reported immediately to the Information Security Manager.

5 Organization and Responsibilities

5.1 Top Management

- Owns and sponsors the ISMS and its certification scope
- Provides the resources, authorities and responsibilities needed to establish and operate the ISMS
- Approves the ISMS scope and this policy
- Decides on issues that require management decisions, including the acceptable level of risk

5.2 Information Security Manager

- Coordinates the implementation, operation and continual improvement of the ISMS
- Ensures that appropriate controls are selected to treat information security risks
- Coordinates the asset inventory and risk assessment activities
- Reviews the effectiveness of the ISMS and the compliance of its processes
- Organizes awareness and training so that employees understand the risks relevant to their work
- Monitors and audits compliance with information security standards

5.3 Management Review

Top management and the Information Security Manager review the ISMS at regular intervals, at least once a year. These reviews cover, among other topics, this policy, the risk management methodology and current risks, security incidents, business continuity, awareness activities, internal audit results and significant changes affecting the organization.



5.4 Employees and Partners

All employees, including interns, as well as contractors and partners, are responsible for protecting the information they work with, for following the related policies and procedures, and for reporting security incidents without delay.

6 General Rules

- This policy applies to all employees, interns and business partners unless an exception is explicitly defined.
- Where a specific task requires an exception, the necessary security rules are defined in the relevant standards and instructions.
- The details of the requirements set out in this policy are regulated in the ISMS procedures, which employees and partners are required to know and follow.
- The rules apply to all information stored or processed on paper or electronically, and to the use of all information processing systems.
- All systems and infrastructure provided by FYBU Digital Solution GmbH, and all information and work products created with them, belong to FYBU Digital Solution GmbH unless laws or contracts provide otherwise.

7 Review and Approval

This policy is reviewed at least once a year and whenever significant changes occur. It has been reviewed and approved by the management of FYBU Digital Solution GmbH.