1. Aim and purpose of the document

This policy defines rules for handling **information** and **information security** that apply to suppliers, contractors, service providers, and other third parties (hereinafter referred to as contractors) who perform activities for **IT-HAUS GmbH** and come into contact with, process, or protect **IT-HAUS GmbH's** information assets.
The purpose of this policy is to establish the contractor's obligations regarding the handling and use of **IT-HAUS GmbH's** information assets, in order to ensure the protection of the confidentiality, integrity, and availability of information, as well as the rights and interests of **IT-HAUS GmbH**.

2. Responsibilities

The "Chief Information Security Officer" (CISO) is responsible for this policy in coordination with the management.

3. Scope of application

This policy is addressed to the contractor's management, their employees, as well as their agents and assistants performing tasks on their behalf.

4. IT and information security requirements

4.1st Maintaining the confidentiality of information/company secrets

IT-HAUS GmbH exclusively collaborates with contractors who have committed to maintaining the confidentiality of information and trade secrets through a confidentiality obligation or a non-disclosure agreement. In individual cases, where the transmitted information is subject to heightened security requirements, additional measures may be required from contractors to appropriately address these increased security needs.

4.2nd Technical and organizational measures for information and IT security

The confidentiality and integrity of sensitive data, as well as its availability and the continuity of operations and critical business processes, must also be ensured through effective and appropriate technical and organizational measures.

4.2.1 Information security management

IT and information security are of utmost importance to **IT-HAUS GmbH**. The client expects the contractor to establish appropriate processes within their organization to ensure IT and information security throughout the entire duration of service delivery. This can be achieved, for example, through a suitable Information Security Management System (ISMS) or through equivalent, appropriate processes that ensure information security during service provision. The contractor's information security processes must at minimum comply with the information security requirements described below and be aligned with ISO/IEC 27001 or an equivalent standard.

4.2.2 Consideration of relevant laws and standards for the provision of services

The Contractor shall comply with the relevant data protection regulations. Where applicable, **IT-HAUS GmbH** also expects compliance with requirements arising from other relevant laws and standards for the provision of services by the business partner, such as NIS2.

4.2.3 Contact persons for information security

The contractor must designate a qualified point of contact for all aspects related to information security (e.g., Information Security Officer, IT Security Manager), who is authorized and capable of providing information to **IT-HAUS GmbH** on all matters concerning information security management. Upon request, the contractor's point of contact shall provide information on the current status of IT and information security (e.g., by completing an information security questionnaire or by presenting proof of an ISO 27001-certified ISMS with a scope that includes the services provided to **IT-HAUS GmbH**).

4.2.4 Qualified personnel

The contractor assures that all employees involved in performing the work are familiarized with the relevant provisions and requirements regarding information security prior to commencing their activities. Furthermore, the contractor shall ensure that these employees are appropriately bound to confidentiality for the duration of their employment and beyond its termination. Upon request, the contractor shall provide **IT-HAUS GmbH** with evidence of such compliance.

4.2.5 Obligation of subcontractors

The contractor ensures that any subcontractors involved in service delivery—and, where agreed, their sub-subcontractors—comply with the requirements of this policy, which align with ISO/IEC 27001 or an equivalent standard. Upon request, the contractor shall provide **IT-HAUS GmbH** with appropriate evidence of such compliance.

4.2.6 General security requirements for access and access to IT systems

The contractor is obliged to have a procedure in place for the regular review of access rights to ensure that only authorized individuals can access IT systems of **IT-HAUS GmbH.** Whenever **IT-HAUS GmbH**'s IT systems are accessed, the contractor must comply with all security measures and conditions (and ensure that its personnel comply with them) that are necessary for the provision of the service. **IT-HAUS GmbH** shall only authorize the contractor to access the IT systems of **IT-HAUS GmbH** if this has been agreed and only to the extent necessary for the provision of the service.

The removal of work results or IT systems belonging to **IT-HAUS GmbH** from **IT-HAUS GmbH's** premises is permitted only within the scope of the agreed service delivery and requires the prior written approval of **IT-HAUS GmbH**.

The authentication credentials (usernames and passwords) stored on **IT-HAUS GmbH** data processing systems must be used in a manner that clearly identifies the individual user. Disclosure or sharing of these credentials with third parties is strictly prohibited.

The contractor must ensure that only those employees who are directly involved in the delivery of services have access to **IT-HAUS GmbH's** information. Access to and use of **IT-HAUS GmbH's** IT systems is permitted solely for the agreed purposes and tasks.

The contractor shall implement a secure login procedure for its own systems that process **IT-HAUS GmbH's** information, in accordance with current technological standards (e.g., multi-factor authentication or the use of strong passwords).

The contractor shall take all necessary precautions to prevent the introduction of computer viruses into **IT-HAUS GmbH's** software and IT systems, and shall take appropriate action upon detecting any such virus. The contractor commits to taking all precautions and measures that can reasonably be expected from a diligent business partner to ensure that no security incident is caused, facilitated, or triggered in

relation to its deliveries and/or services and/or within the **IT-HAUS GmbH** information systems to which the contractor has access.

4.3. Security incident report

In the event that the contractor becomes aware of or suspects, any unlawful or unauthorized access to and/or use of data and/or IT systems of **IT-HAUS GmbH** or the contractor, the contractor is obligated to report such (suspected) security incident to **IT-HAUS GmbH** in writing as soon as they become aware of it and/or are notified of it by a directly or indirectly responsible authority.

In such cases, the contractor shall take all appropriate measures that a diligent contractor would take to protect its own data and/or IT systems as well as the data and/or IT systems of **IT-HAUS GmbH**, including but not limited to disconnecting the connection and/or blocking access. Under no circumstances shall **IT-HAUS GmbH** be liable for any deterioration in the quality of deliveries and/or services resulting from the measures taken in such cases.

Furthermore, the contractor is obliged to report any unauthorized or unlawful access to and/or unauthorized use of the information systems / IT systems of IT-HAUS GmbH, as well as any suspicion of such an event or any other security incident, without undue delay, but no later than within one (1) calendar day after becoming aware of the (suspected) security incident.

The report shall be submitted via the **IT-HAUS** Security Incident portal at https://sir.ith-services.com.

The portal ensures immediate further processing, a complete and structured collection of all relevant information, as well as fast and transparent handling of the reported incident.
Reporters benefit from traceable documentation, reduced response times, and a clear, structured process for handling security incidents.