1. Aim and purpose of the document

This guideline defines rules for the handling of **information** and **information security** by suppliers, contractors and service providers as well as other third parties (hereinafter referred to as contractors) who carry out activities for **IT-HAUS GmbH** and come into contact with, process or protect information assets of **IT-HAUS GmbH**.
The aim of this guideline is therefore to regulate the obligations of the contractor for the handling and use of information assets of **IT-HAUS GmbH** in order to ensure the protection of 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 consultation with the management.

3. Scope of application

The guideline is aimed at the management of the contractor, their employees and their vicarious agents.

4. IT and information security requirements

4.1st Maintaining the confidentiality of information/company secrets

IT-HAUS GmbH works exclusively with contractors who have undertaken to maintain the confidentiality of information and trade secrets as part of a confidentiality obligation or a confidentiality agreement. In individual cases, if the information provided is subject to increased security requirements, contractors may also be required to take special measures to take account of the increased security requirements.

4.2ndTechnical and organizational measures for information and IT security

The confidentiality and integrity of sensitive data as well as its availability and the maintenance of operations and important business processes must also be ensured by effective and appropriate technical and organizational measures.

4.2.1 Information security management

IT and information security are very important to **IT-HAUS GmbH.** The client requires that the contractor establishes suitable processes in his company to ensure IT and information security as part of the provision of services and maintains these throughout the entire term. For example, this takes the form of an appropriate information security management system (ISMS) or equivalent, suitable processes to ensure information security as part of the provision of services. The Contractor's information security processes comply at least with the information security requirements described below and are based on ISO/IEC 27001 or an equivalent requirement.

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 appoint a competent contact person (e.g. information security officer, IT security manager) to **IT-HAUS GmbH** for all aspects relating to information security, who is able and authorized to provide information to the Client on all matters relating to the management of information security. Upon request, the Contractor's contact person shall provide information on the status of IT and information security (e.g. by means of an information security questionnaire or by providing evidence of an ISO 27001-certified ISMS with a scope that includes the services for the Client).

4.2.4 Qualified personnel

The Contractor warrants that it will familiarize the employees engaged in the performance of the work with the provisions and requirements on information security applicable to them before they commence their work and that it will impose an appropriate confidentiality obligation on them for the duration of their work and after termination of the employment relationship. The Contractor shall prove this to **IT-HAUS GmbH** on request.

4.2.5 Obligation of subcontractors

The Contractor warrants that its subcontractors and, if agreed, their subcontractors used for the provision of services fulfill the requirements of this guideline, ISO/IEC 27001 or those of a comparable standard. The Contractor shall provide corresponding evidence at the request of **IT-HAUS GmbH**.

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 persons 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 of **IT-HAUS GmbH** from the business premises of **IT-HAUS GmbH** is only permitted within the scope of the agreed service provision and requires the prior written approval of **IT-HAUS GmbH**.
The authentication information (identifiers and passwords) stored on **IT-HAUS GmbH** data processing systems must be used in a personalized manner. Passing on or disclosure to third parties is prohibited.
The Contractor shall ensure that only those employees are granted access to **IT-HAUS GmbH** information who are also involved in the delivery service. Access and access to the IT systems of **IT-HAUS GmbH** may only take place for the agreed purposes and tasks.
For its own systems on which **IT-HAUS GmbH** information is processed, the Contractor shall use a state-of-the-art secure login procedure (e.g. multi-factor authentication or use of strong passwords) for access to these systems and applications.
The Contractor shall take all necessary precautions to prevent the introduction of a computer virus into the software and/or IT systems of **IT-HAUS GmbH** and shall take appropriate measures if it becomes aware of the presence of such a virus. The contractor undertakes to take all precautions and measures to be expected of a diligent contractual partner to ensure that he does not or will not cause or facilitate a security incident in relation to his deliveries and/or services and/or in the information system of **IT-HAUS GmbH** to which the contractor has access.

4.3. Security incident report

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

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

In addition, in the event of unauthorized or unlawful access and/or use of the **IT-HAUS GmbH** information system/IT system and/or in the event of suspicion of such an event and/or in the event of any other security incident, the Contractor must notify the **IT-HAUS GmbH** Service Desk by e-mail servicedesk@it-haus.com or by telephone +49 6502 9208 110 as soon as it becomes aware of this, but no later than one (1) calendar day after a (suspected) security incident.