The management of WOBCOM GmbH hereby adopts the following guideline on information security as part of its strategy:

1 Purpose of the Guideline

As a provider, WOBCOM relies on the availability of modern information and communication technology to fulfill its business processes in conjunction with the ability to be able to work with its customers and partners. In addition, there are obligations to ensure information security based on legal provisions and contractual obligations of WOBCOM, towards project partners, employees and customers.

The protection of WOBCOM's information and communication infrastructure against misuse, manipulation, interference, spying on confidential information, etc. – in short, information security – is therefore of crucial importance. Lack of information security can lead to disruptions in the performance of tasks, which can reduce the performance of WOBCOM and, in extreme cases, bring its business processes to a standstill.

Against this background, an adequate level of information security in the business processes of WOBCOM GmbH is organized as an information security management system (ISMS).

2 Scope

This Guideline and all related regulations apply to the entirety of WOBCOM. It also applies to all external workers, working on behalf of the company. The contents of the guideline and the resulting regulations and measures must be observed and complied with by all of WOBCOM employees and associates.

3 Objectives of Information Security

All activities aimed at maintaining and improving information security are aimed at ensuring the core values of confidentiality, integrity and availability of information, and in particular our customer data.

Confidentiality

Information must not be passed into the wrong hands. It must only be made available to the respective authorised persons.

Availability

Information must be available at all times; it must be protected against downtime or the risk of failure should be minimized.

Integrity

Information should not go unnoticed. Changes to information must always be plausible and comprehensible.

The specific security measures must be economically justifiable in relation to the need for protection of the information processed. As core activities to maintain and improve information security, information security risks are continuously identified, evaluated, and addressed. Information security is subject to various legal, regulatory, and contractual requirements, which are continuously identified and considered for information security.

4 Security Organizations

All information security responsibilities are clearly assigned.

The management assumes overall responsibility for information security at WOBCOM GmbH. It fully backs the information security objectives set out here and the concepts, policies and measures derived from them.

In order to achieve the information security objectives, an Information Security Officer (*Informationssicherheitsbeauftragter ISB*) has been appointed by the management. He advises the management in the planning and implementation of information security in the company. In his organisationally independent function, he reports regularly, and on a case-by-case basis directly to the management and is supported in his work by the information security coordinators (*Informationssicherheitskoordinatoren ISK*) of the individual departments. A Data Protection Officer (*Datenschutzbeauftragter DSB*) has also been appointed.

The management provides the ISB, ISK and DSB with the necessary time and financial resources to further their training and to achieve the established information security objectives.

The ISB is involved in all projects and measures at an early stage to take security-relevant aspects into account at the planning stage.

5 Security Measures

Responsible persons (asset managers) are designated for all procedures, information, IT applications and IT systems, who determine the respective protection requirements and assign the necessary access authorizations.

Representations must be set up for all responsible functions. It is necessary to ensure, through instruction and sufficient documentation, that representatives can carry out their duties.

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

All Internet access is secured by suitable firewall systems. All protection programs are configured and administered to provide effective protection and prevent tampering. In addition, IT users support these security measures by working in a security-conscious manner and inform the appropriately defined bodies in case of abnormalities.

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

In order to limit or prevent major damage in the event of emergencies, a rapid and consistent response to security incidents must be carried out. Emergency measures are put together in a separate emergency preparedness concept. Our goal is to maintain critical business processes even in the event of a system failure and to restore the availability of failed systems within a tolerable period of time.

If IT services are outsourced to external locations, we specify specific security requirements in the Service Level Agreements. The right to control is established. For large or complex outsourcing projects, we prepare a detailed security concept with concrete policy guidelines.

IT users regularly participate in training on the correct use of IT services and the security measures associated with them. The management supports the needs-based further education and training.

The regulations and regulations resulting from the security measures in the form of guidelines are known to all WOBCOM employees and must be complied with.

6 Improving Information Security

This Guideline and the ISMS are regularly or after major changes to be checked and adapted for timeliness and its effectiveness. In addition, the measures are regularly examined to see whether they are known to the employees concerned, implementable and can be integrated into the operation. The reviews and related changes to the information security guideline are influenced by management assessment results. The management supports the continuous improvement of the safety level. Employees are encouraged to pass on any improvements or vulnerabilities to the ISB.

The ISB shall provide appropriate information on the updates. On behalf of WOBCOM, - persons are informed by the responsible contact person.

All intentional, grossly negligent or negligent violations of safety procedures and regulations are prosecuted by WOBCOM on the basis of a formal disciplinary process. This is based on the information security policy and on all guidelines and safeguards to support it.

7 Obligation To Cooperate

The management is committed to its task of supporting the objectives of information security described in this guideline and calls on all employees to also contribute to the maintenance or improvement of information security.