Information security requirements for suppliers and service providers

1. Purpose

Information and IT security is an essential part of IMS Gears' business processes and supply chain. Many companies work together along the entire value chain to enable the development and manufacturing of products. In the process, confidential information is passed on to suppliers and service providers. Consequently, the information and IT systems must be adequately protected so that the exchange of data and the availability of IT systems along the entire supply chain is not in danger. For this reason, our suppliers and service providers should set up and maintain a functioning information security management system (ISMS).

2. Protection requirements and evidence obligations

The implementation of information and IT security requirements depends on the information that is exchanged. The following classifications and protection requirements apply at IMS Gear.

The following minimum requirements must be met by the supplier or service provider in order to receive information worthy of protection from IMS Gear.

The minimum requirements result from the assigned confidentiality level of the information. IMS Gear assigns the confidentiality level to the information. Suppliers and service providers can only receive information of the confidentiality level whose minimum requirements they also fulfill.

Confidentiality level of information	Protection level	Minimal requirements
Public	No need for protection	-
Internal	Normal protection needs	Completed and approved self-declaration on information security.
Confidential	High protection needs	TISAX in accordance with VDA ISA as per Assessment Level 2, comparable standard (ISO 27001) or completed self-declaration on information security approved for high protection requirements.
Strictly confidential	Very high protection needs	TISAX according to VDA ISA in accordance with Assessment Level 3, or comparable standard (ISO 27001).
Strictly confidential and prototypes	Very high protection needs	TISAX according to VDA ISA in accordance with Assessment Level 3 + Prototype protection

3. **Exchange of information**
   When exchanging information, care must be taken to ensure that all security precautions corresponding to the above-mentioned protection requirements are taken (e.g. encryption) to protect against unauthorized access, modification and deletion of the information. For all conversations that could contain information from IMS Gear, care must be taken to ensure that they cannot be overheard without authorization.

4. **Remote maintenance**
   Remote maintenance access is only permitted within the scope of the fulfillment of contractual obligations in relation to the provision of services for IMS Gear.
   In case of remote maintenance access to the internal IT/OT system environment or cloud environment of IMS Gear, only a remote maintenance solution or access approved by IMS Gear may be used.
   All maintenance interfaces accessing the internal IT/OT system environment or cloud environment of IMS Gear must be specified and documented in coordination with IMS Gear.
   Remote accesses may only be active in the context of maintenance work. Permanent remote access is only permitted in cases approved by IMS Gear.
   For secure user authentication, remote access must be provided via personalized accounts with strong passwords and multi-factor authentication (either OTP, hardware token or biometric methods).
   IMS Gear reserves the right to prohibit or suspend remote maintenance access in justified cases without prior notice. Remote access ends upon termination of the contractual agreement with the supplier or service provider.

5. **Physical transportation of mobile data storage**
   Mobile data storage on which IMS Gear information is stored must be protected against unauthorized access, misuse or falsification during transport, even across organizational boundaries.
   Care must be taken to ensure that all necessary and appropriate precautions are taken (e.g. encryption) to protect against unauthorized access, modification and deletion of the information during transport.
   Mobile data storage on which IMS Gear information is stored must be transported in such a way that they are not visible from the outside. Furthermore, when used in public, care must be taken to ensure that no information on the screen can be read.
   Documents must be protected from view, e.g. transported in a non-transparent folder.

6. **Handling of information security incidents and communication**
   Information security incidents (e.g. occurring disruptions, loss of data, unlawful acts, cybercrime attacks) in which IMS Gear information could be affected must be reported without culpable hesitation to the contact person for information security using the e-mail address below.
   Any suspicion of loss of confidential information must also be reported to the contact person for information security without culpable hesitation.

7. **Compliance with information security (supply chain) / subcontractors**
   The commissioning of subcontractors by the Supplier or service providers who receive or process information from IMS Gear requires the express written consent of IMS Gear. The consent may be revoked subsequently. The consent shall be revoked

in particular if serious breaches of duty or not insignificant misconduct of the subcontractor in the context of the provision of services justify this.

Before passing on information of IMS Gear to subcontractors, the Supplier or service provider shall ensure that these subcontractors comply with an appropriate level of security in accordance with the above table (Clause 2). This includes the contractual conclusion of non-disclosure agreements with subcontractors. Proof of compliance is the responsibility of the supplier or service provider and must be provided at any time upon request.
The supplier or service provider is responsible for the subcontractor. If the subcontractor violates IMS Gear's requirements, both the breach of duty and the fault of the subcontractor shall be attributed to the Supplier or Service Provider.

8. **Right to audit in relation to information security**
The supplier or service provider grants IMS Gear the right, to be exercised at any time, to inspect and review all relevant data relating to information security between the supplier or service provider and IMS Gear after prior notification. This also includes the review of IT and data security measures. Employees of IMS Gear or third parties commissioned by IMS Gear may enter the premises of the supplier or service provider during normal business hours for this purpose. The cost of the inspection shall be borne by the supplier or service provider if violations of information security requirements or agreements of the respective order are identified unless such violations are not due to the fault of the supplier or service provider.

9. **Confidentiality agreement between the supplier or service providers and its employees**
The Supplier or service provider of IMS Gear undertakes to enter into a non-disclosure agreement (separately or as part of the employment contract) with all its employees, consultants and contractors who receive or have access to information from IMS Gear during the cooperation. Proof of compliance is incumbent on the Supplier or service provider and must be provided at any time upon request.

10. **Contact address**
The contact person for information security at IMS Gear is the Information Security Officer, who can be contacted at the following e-mail address: isb@imsgear.com

We hereby undertake to comply with the above requirements.

_____

(Company in block letters)

_____

(Place, Date)

_____

(Signature)

Informationssicherheitsanforderungen für Lieferanten und Dienstleister

1. Zweck

Informations- und IT-Sicherheit ist für IMS Gear ein wesentlicher Bestandteil der Geschäftsprozesse und der Lieferketten. In der gesamten Wertschöpfungskette arbeiten eine Vielzahl von Unternehmen zusammen, um die Entwicklung und Herstellung von Produkten zu ermöglichen. Dabei werden vertrauliche Informationen an Lieferanten und Dienstleister weitergegeben. Folglich müssen die Informationen und IT-Systeme angemessen geschützt werden, so dass der Austausch von Daten und die Verfügbarkeit der IT-Systeme entlang der gesamten Lieferkette nicht gefährdet ist.
Aus diesem Grund verpflichten sich unsere Lieferanten und Dienstleister dazu, ein funktionierendes Informationssicherheitsmanagementsystem (ISMS) einzurichten und aufrecht zu erhalten.

2. Schutzbedarf und Nachweispflicht

Die Umsetzung von Informations- und IT-Sicherheitsanforderungen ist abhängig von den Informationen, die ausgetauscht werden. Bei IMS Gear gelten folgende Klassifikationen und Anforderungen an den Schutzbedarf.
Um schutzwürdige Informationen von IMS Gear empfangen zu dürfen, müssen die folgenden Mindestanforderungen auf Seiten des Lieferanten oder Dienstleisters erfüllt sein.
Die Mindestanforderungen ergeben sich aus der zugewiesen Vertraulichkeitsstufe der Informationen. IMS Gear weist die Vertraulichkeitsstufe den Informationen zu. Lieferanten und Dienstleister können nur Informationen der Vertraulichkeitsstufe empfangen, deren Mindestanforderungen sie auch erfüllen.

Vertraulichkeitsstufe der Information	**Schutzbedarfslevel**	**Mindestanforderungen**
Öffentlich	Kein Schutzbedarf	-
Intern	Normaler Schutzbedarf	Ausgefüllte und freigegebene Selbstauskunft zur Informationssicherheit.
Vertraulich	Hoher Schutzbedarf	TISAX nach VDA ISA gemäß Assessment Level 2, vergleichbarer Standard (ISO 27001) oder ausgefüllte und für den hohen Schutzbedarf freigegebene Selbstauskunft zur Informationssicherheit.
Streng vertraulich	Sehr hoher Schutzbedarf	TISAX nach VDA ISA gemäß Assessment Level 3, oder vergleichbarer Standard (ISO 27001).
Streng vertraulich + Prototypen	Sehr hoher Schutzbedarf	TISAX nach VDA ISA gemäß Assessment Level 3 + Prototypenschutz.

3. Austausch von Informationen

Beim Austausch von Informationen ist darauf zu achten, dass alle dem o.g. Schutzbedarf entsprechenden Sicherheitsvorkehrungen getroffen werden (z. B. Verschlüsselung), die vor Einsichtnahme, Veränderung und Löschung der Informationen durch Unbefugte schützen. Bei allen Gesprächen, die Informationen von IMS Gear enthalten könnten, ist darauf zu achten, dass diese nicht unbefugt mitgehört werden können.

4. **Fernwartung**

Ein Fernwartungszugriff ist nur im Rahmen der Erfüllung vertraglicher Verpflichtungen in Bezug auf die Leistungserbringung für IMS Gear gestattet.
Bei einem Fernwartungszugriff auf die interne IT-/OT-Systemumgebung oder Cloudumgebung der IMS Gear darf nur eine durch IMS Gear freigegebene Fernwartungslösung oder Zugang eingesetzt werden.
Alle Wartungsschnittstellen, die auf die interne IT-/OT-Systemumgebung oder Cloudumgebung von IMS Gear zugreifen, müssen in Abstimmung mit IMS Gear spezifiziert und dokumentiert werden.
Fernzugänge dürfen ausschließlich im Rahmen der Wartungsdurchführung aktiv sein. Permanente Fernzugänge sind nur in von IMS Gear genehmigten Fällen zulässig.
Für eine sichere Benutzerauthentifizierung muss der Fernzugang über personalisierte Accounts mit starken Kennwörtern und über Multi-Faktor-Authentifizierung (wahlweise OTP, Hardware-Token oder biometrische Verfahren) erfolgen.
IMS Gear behält sich das Recht vor, den Fernwartungszugriff in begründeten Fällen ohne Vorankündigung zu untersagen oder auszusetzen. Der Fernzugang endet mit Beendigung der vertraglichen Vereinbarung mit dem Lieferanten oder Dienstleister.

5. **Physischer Transport von mobilen Datenträgern**

Mobile Datenträger auf denen Informationen von IMS Gear gespeichert sind, müssen vor unbefugten Zugriff, Missbrauch oder Verfälschung während des Transports, auch über Organisationsgrenzen hinweg, geschützt werden.
Es ist darauf zu achten, dass alle notwendigen und geeigneten Vorkehrungen getroffen werden (z.B. Verschlüsselung), die vor Einsichtnahme, Veränderung und Löschung der Informationen durch Unbefugte beim Transport schützen.
Mobile Datenträger auf denen Informationen von IMS Gear gespeichert sind, sind so zu transportieren, dass sie von außen nicht sichtbar sind. Darüber hinaus ist bei der Nutzung in der Öffentlichkeit darauf zu achten, dass keine Informationen am Bildschirm mitgelesen werden können.
Dokumente müssen sichtgeschützt, also z.B. in einer Nicht-Klarsichtmappe transportiert werden.

6. **Umgang mit Informationssicherheitsvorfällen und Kommunikation**

Informationssicherheitsereignisse (z. B. auftretende Störungen, Verlust von Daten, rechtswidriges Handeln, Cybercrime Angriffe) bei denen Informationen von IMS Gear betroffen sein könnten, sind ohne schuldhaftes Zögern an den Ansprechpartner für Informationssicherheit unter Verwendung der unten genannten E-Mail-Adresse zu melden.
Ein Verdacht auf Verlust von vertraulichen Informationen muss ebenfalls ohne schuldhaftes Zögern an den Ansprechpartner für Informationssicherheit gemeldet werden.

7. **Einhaltung der Informationssicherheit (Lieferkette) / Unterauftragnehmer**

Die Beauftragung von Unterauftragnehmern durch den Lieferanten oder Dienstleister, welche Informationen von IMS Gear erhalten bzw. verarbeiten, bedarf der ausdrücklichen schriftlichen Zustimmung von IMS Gear. Die Zustimmung kann nachträglich widerrufen werden. Die Zustimmung wird insbesondere widerrufen, wenn

schwerwiegende Pflichtverletzungen oder nicht unerhebliches Fehlverhalten des Unterauftragnehmers im Rahmen der Leistungserbringung dies rechtfertigen.

Vor der Weitergabe von Informationen der IMS Gear an Unterauftragnehmer, stellt der Lieferant oder Dienstleister sicher, dass diese Unterauftragnehmer ein angemessenes Sicherheitsniveau gemäß der o.g. Tabelle (Ziff. 2) einhalten. Dies schließt den vertraglichen Abschluss von Geheimhaltungsvereinbarungen mit Unterauftragnehmern ein. Der Nachweis der Einhaltung obliegt dem Lieferanten oder Dienstleister und ist auf Verlangen jederzeit nachzuweisen.

Der Lieferant oder Dienstleister ist für den Unterauftragnehmer verantwortlich. Sofern der Unterauftragnehmer gegen Anforderungen von IMS Gear verstößt, werden dem Lieferant oder Dienstleister sowohl die Pflichtverletzung als auch das Verschulden des Unterauftragnehmers zugerechnet.

8. **Auditrechte in Bezug auf Informationssicherheit**
   Der Lieferant oder Dienstleister räumt IMS Gear das jederzeit auszuübende Recht ein, nach vorheriger Anmeldung, sämtliche Daten zu Geschäftsvorfällen in Bezug auf die Informationssicherheit zwischen dem Lieferanten oder Dienstleister und IMS Gear einzusehen und zu überprüfen. Davon umfasst ist auch die Prüfung der Maßnahmen der IT- und Datensicherheit.
   Mitarbeiter von IMS Gear oder von IMS Gear beauftragte Dritte dürfen hierzu die Räume des Lieferanten oder Dienstleisters während der üblichen Geschäftszeiten betreten. Die Kosten der Überprüfung trägt der Lieferant oder Dienstleister, wenn hierbei Verstöße gegen die Informationssicherheit oder Vereinbarungen der jeweiligen Beauftragung festgestellt werden, es sei denn, solche Verstöße beruhen nicht auf einem Verschulden des Lieferanten oder Dienstleisters.

9. **Geheimhaltungsvereinbarung zwischen dem Lieferanten / Dienstleister und seinen Mitarbeitern**
   Der Lieferant oder Dienstleister von IMS Gear verpflichtet sich dazu, mit all seinen Mitarbeitern, Beratern und Auftragnehmern, die im Zuge der Zusammenarbeit Informationen von IMS Gear erhalten oder auf diese zugreifen können, eine Geheimhaltungsvereinbarung (separat oder als Teil des Arbeitsvertrages) abzuschließen. Der Nachweis der Einhaltung obliegt dem Lieferanten oder Dienstleister und ist auf Verlangen jederzeit nachzuweisen.

10. **Ansprechpartner**
    Ansprechpartner zum Thema Informationssicherheit bei IMS Gear ist der Informationssicherheitsbeauftragte, erreichbar unter der E-Mail-Adresse: isb@imsgear.com

Hiermit verpflichten wir uns, die obenstehenden Anforderungen zu erfüllen.

_____

(Firma in Druckbuchstaben)

_____ _____

(Ort, Datum) (Unterschrift)