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. According to the harmonized information classification levels of the German Association of the Automotive Industry (VDA), the following classifications and protection requirements apply. Our suppliers and service providers must protect the information received from IMS Gar in accordance with the classification and requirements.

Confidentiality level of information	**Protection level**	**Minimal requirements**
Public	No need for protection	No minimal requirements
Internal	Normal protection needs	Completion of the VDA ISA self-disclosure form with signature of the management or ISB
Confidential	High protection needs	TISAX according to VDA ISA in accordance with Assessment Level 2, or SOC 2 Type 2 Report (depending scope) or TPISR
Strictly confidential	Very high protection needs	TISAX according to VDA ISA in accordance with Assessment Level 3, or ISO/IEC 27001 (depending on the scope)
Strictly confidential and prototypes	Very high protection needs	TISAX according to VDA ISA in accordance with Assessment Level 3+

3. **Exchange of information**
   When exchanging information, special care must be taken to ensure that all necessary and appropriate security precautions are taken (e.g. encryption) to prevent unauthorized persons from viewing, modifying, or deleting the information. For all conversations that could contain information from IMS Gear, care must be taken to ensure that they cannot be overheard by unauthorized people.

4. **Remote maintenance**
   For remote maintenance access to the IT/OT system environment of IMS Gear, only a remote maintenance solution approved by IMS Gear must be used.
   Remote maintenance access is only permitted within the scope of the fulfilment of contractual obligations in relation to the provision of services for IMS Gear.
   All maintenance interfaces accessing IMS Gear's IT/OT system environment must be specified and documented in coordination with IMS Gear.
   Remote accesses must only be active in the context of maintenance. Permanent remote access is only permitted in cases authorized 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 media**
   Any media, data or data storage devices containing information from IMS Gear 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 information during transport. Data storage devices must be transported in a concealed manner. Data storage devices with confidential information must always be escorted by an employee of the supplier or service provider during any transport. Documents must be transported with visual protection, e.g. in a non-transparent folder.

6. **Physical transportation of laptops**
   Laptops on which information from IMS Gear 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.

7. **Handling of information security incidents and communication**
   Serious information security incidents (e.g. disruptions, loss of data, unlawful acts, cybercrime attacks) must be reported without undue delay to the contact person for information security using the e-mail address (Section 11). Any suspicion of loss of confidential information must also be reported to the contact person for information security without undue delay.

8. **Compliance with information security (supply chain)**
   When commissioning subcontractors or sub suppliers, the supplier or service provider must ensure that the requirements of IMS Gear for information security requirements in accordance with TISAX or ISO27001 are also met by the subcontractor or sub supplier. This also includes the conclusion of non-disclosure agreements with

subcontractors or sub suppliers. Proof of compliance is the responsibility of the supplier or service provider and must be provided at any time upon request.

9. **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.

10. **Confidentiality agreement between the supplier and its employees**
    Suppliers or service providers of IMS Gear shall conclude non-disclosure agreements (separately or as part of the employment contract) with all employees who receive or have access to information from IMS Gear during the collaboration. Proof must be provided at any time upon request.

11. **Subcontractors**
    The commissioning of subcontractors by the supplier or service provider requires the express written consent of IMS Gear. Consent may be revoked at any time. Consent shall be revoked if this is justified by serious breaches of duty or not insignificant misconduct on the part of the subcontractor or its agents in the context of the performance of contracts.

    The supplier or service provider is responsible for the subcontractor. If the subcontractor violates the requirements of IMS Gear, both the breach of duty and the fault of the subcontractor shall be attributed to the supplier or service provider.

12. **Contact address**
    Contact person for information security at IMS Gear:
    Mr. Heiko Watz (ISB/CISO), e-mail: isb@imsgear.com

    We hereby agree with fulfilling the above requirements.

_____

(Company in block letters)

_____	_____
(Place, Date)	(Place, Date)
_____	_____
(Signature)	(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. Gemäß der harmonisierten Informations-Klassifizierungsstufen des Verbands der deutschen Automobilindustrie (VDA) gelten folgende Klassifikationen und Anforderungen an den Schutzbedarf. Unsere Lieferanten und Dienstleister müssen die Informationen, die von IMS Gear empfangen werden gemäß der Klassifikation und den Anforderungen schützen.

Vertraulichkeitsstufe der Information	**Schutzbedarfslevel**	**Mindestanforderungen**
Öffentlich	Kein Schutzbedarf	-
Intern	Normaler Schutzbedarf	Befüllung der VDA ISA Selbstauskunft mit Unterschrift des Managements oder ISB
Vertraulich	Hoher Schutzbedarf	TISAX nach VDA ISA gemäß Assessment Level 2, oder SOC 2 Typ 2 Report (in Abhängigkeit des Scopes), oder TPISR
Streng vertraulich	Sehr hoher Schutzbedarf	TISAX nach VDA ISA gemäß Assessment Level 3, oder ISO/IEC 27001 (in Abhängigkeit des Scopes)
Streng vertraulich + Prototypen	Sehr hoher Schutzbedarf	TISAX nach VDA ISA gemäß Assessment Level 3+

3. **Austausch von Informationen**
   Beim Austausch von Informationen ist darauf zu achten, dass alle notwendigen und geeigneten 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**
   Bei Fernwartungszugriffen auf die IT-/OT-Systemumgebung der IMS Gear darf nur eine durch IMS Gear freigegebene Fernwartungslösung eingesetzt werden.
   Ein Fernwartungszugriff ist nur im Rahmen der Erfüllung vertraglicher Verpflichtungen in Bezug auf die Leistungserbringung für IMS Gear gestattet.
   Alle Wartungsschnittstellen, die auf die IT-/OT-Systemumgebung 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 Medien**
   Medien, die Informationen von IMS Gear beinhalten, 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. Datenträger sind verborgen zu transportieren. Datenträger mit vertraulichen Informationen werden grundsätzlich eskortiert durch einen Mitarbeiter des Lieferanten oder Dienstleisters transportiert. Dokumente müssen sichtgeschützt, also z.B. in einer Nicht-Klarsichtmappe transportiert werden.

6. **Physischer Transport von Notebooks**
   Notebooks 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.

7. **Umgang mit Informationssicherheitsvorfällen und Kommunikation**
   Schwerwiegende Informationssicherheitsereignisse (z. B. auftretende Störungen, Verlust von Daten, rechtswidriges Handeln, Cybercrime Angriffe) sind ohne schuldhaftes Zögern an den Ansprechpartner für Informationssicherheit unter Verwendung der E-Mail-Adresse (Ziffer 11) zu melden. Ein Verdacht auf Verlust von vertraulichen Informationen muss ebenfalls ohne schuldhaftes Zögern an den Ansprechpartner für Informationssicherheit gemeldet werden.

8. **Einhaltung der Informationssicherheit (Lieferkette)**
   Der Lieferant oder Dienstleister hat im Rahmen der Beauftragung von Unterauftragnehmern sicherzustellen, dass die Anforderungen von IMS Gear an die Einhaltung der Informationssicherheit gemäß TISAX beziehungsweise ISO27001 auch durch den Unterauftragnehmer eingehalten werden. Dies schließt auch den Abschluss von Geheimhaltungsvereinbarungen mit Unterauftragnehmern ein. Der Nachweis der Einhaltung obliegt dem Lieferanten oder Dienstleister und ist auf Verlangen jederzeit nachzuweisen.

9. **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.

10. **Geheimhaltungsvereinbarung zwischen dem Lieferanten / Auftragnehmer und seinen Mitarbeitern**
    Der Lieferant oder Dienstleister von IMS Gear verpflichtet sich dazu, mit all seinen Mitarbeitern, 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.

11. **Unterauftragnehmer**
    Die Beauftragung von Unterauftragnehmern durch den Lieferanten oder Dienstleister 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 beziehungsweise seiner Erfüllungsgehilfen im Rahmen der Leistungserbringung dies rechtfertigen.

    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.

12. **Ansprechpartner**
    Ansprechpartner zum Thema Informationssicherheit bei IMS Gear:
    Herr Heiko Watz (ISB/CISO), E-Mail: isb@imsgear.com

Hiermit verpflichten wir uns, die obenstehenden Anforderungen zu erfüllen.

_____

(Firma in Druckbuchstaben)

_____ _____

(Ort, Datum) (Ort, Datum)

_____ _____

(Unterschrift) (Unterschrift)