Supplier information security requirements

Classification: Public. Last Updated: January 2022

Supplier information security requirements

Introduction

At GKN Automotive, preserving the confidentiality, privacy, integrity and availability of our information and the information of our customers and other business partners is of the utmost importance. We have therefore adopted security frameworks (such as ISO/IEC 27001, TISAX and ISO/SAE 241434) that meet industry best practice, and we expect our suppliers to adopt similar frameworks in their own business. These requirements apply to all suppliers of GKN Automotive.

In these requirements: **"GKN Information"** means information or data (of any nature) provided directly or indirectly to you or your Affiliates by GKN Automotive, irrespective of whether that information relates to or originated from GKN Automotive or a third party; **"Information Security"** means measures (of any nature) which relate to maintaining the confidentiality, privacy, integrity and availability of GKN Information and Information Assets; and **"Information Assets"** means assets which contain (or which may be used to contain) GKN Information, including: (a) digital information in all formats including files, documents, drawings, engineering drawings, photographs, software, video and audio; (b) physical information including documents, handwritten notes, drawings, engineering drawings, photographs, IT hardware, vehicle parts, tools, components and cars; and (c) verbal information including recordings of phone calls and conference/video calls.

If you have any questions about these requirements, please speak to your usual GKN Automotive Procurement contact, or you can contact the GKN Automotive IT Security Team at: ITsecurity@gknautomotive.com

Scope of these requirements

You	These requirements apply to you, as a supplier to GKN Automotive. They apply throughout the duration of Your Contract and thereafter for so long as any GKN Information remains in your possession or control.
Your Affiliates	These requirements also apply to any other person or company which controls, is controlled by, or is under common control with you (an "Affiliate"). References in these requirements to you include your Affiliates.
Your Employees	You will ensure that your employees and other workers (and those of your Affiliates) comply with these requirements at all times and will adopt appropriate policies, procedures and other measures to achieve this.
Third Parties	You will ensure that all sub-suppliers and other third parties you engage from time to time, who (in accordance with these requirements and Your Contract) are provided with access to Information Assets, comply with these requirements at all times. References in these requirements to you include such third parties.
Your Contract	These requirements form part of your contract(s) with GKN Automotive from time to time ("Your Contract"). These requirements are in addition and without prejudice to the other terms of Your Contract. Nothing in these requirements operates as any waiver or release or variation under, or variation of, Your Contract.

Confidentiality & compliance

Respecting NDAs	You will comply with all confidentiality and non-disclosure agreements, contractual clauses and other obligations which we from time to time enter into with you, including those in Your Contract.
Compliance	You will comply with all applicable laws, regulations and related guidance relating to Information Security and data privacy that from time to time apply to your business. GKN Automotive may verify compliance with the security requirements, such as periodic audits or self-assessment reports
Handling of GKN Automotive Data	Suppliers must handle GKN Automotive's data in accordance with our Information, Classification, Marking and Handling policy. This includes ensuring that data is appropriately classified, stored, and protected based on its sensitivity level. Suppliers are required to implement measures to prevent unauthorised access, disclosure, alteration or destruction of GKN data. Additionally, suppliers must ensure that any transfer of GKN data is conducted securely and in compliance with applicable laws and regulations

Information security assessments & accreditations

Information Security Assessment

We may, whether before or during the term of Your Contract, require that you participate in an Information Security Assessment. The purpose of an Information Security Assessment is to assess the maturity level of your Information Security arrangements and to understand and manage the risks that they represent. This helps us establish a risk profile for you, which is a requirement for us to conduct business with you. This Information Security Assessment may include us providing you with a questionnaire which we ask you to complete. You will promptly complete all such questionnaires on request (and in any event within 30 days of receipt) and will ensure that all responses thereto (and all other information provided by you) are true, accurate and not misleading in all respects.

Disclosed Arrangements

Where, whether as part of an Information Security Assessment or otherwise, you disclose to us any policies, procedures, systems, controls or other measures which you have in place relating to Information Security ("Disclosed Arrangements"), you will maintain those Disclosed Arrangements and not allow them to expire or lapse without our prior agreement in writing.

Supplier-Specific Requirements & Corrective Actions

Based on the outcome of an Information Security Assessment, we may recommend that you implement additional Information Security measures, policies, procedures, systems or controls, or recommend that you implement corrective actions where you have failed to meet your own or our Information Security requirements (together "Supplier- Specific Requirements"). To the extent that such Supplier-Specific Requirements are reasonable and relevant to the goods or services you supply to GKN Automotive or your relationship with us, you will promptly implement those Supplier-Specific Requirements and (once implemented) will maintain those Supplier-Specific Requirements and not allow them to expire or lapse without our prior agreement in writing.

Independent Obligations

If the goods or services you provide involve inherent cybersecurity risks, you must maintain appropriate security certifications, such as ISO/IEC 27001, TISAX, SOC Type 2 and ISO/SAE 21434, or demonstrate compliance with equivalent standards if formal certification is not possible. These certifications must be always upheld, and you may not allow them to expire or lapse without obtaining our prior written consent. Upon request, you are required to promptly provide evidence of your certifications, including copies of relevant certificates, assessments, and audit reports. Failure to comply with these security requirements may affect your ongoing business relationship with GKN Automotive.

Incident response

Incident Response Testing

We may request that you take part in an Information Security incident response test. You will cooperate with any such reasonable request, provided that we give you reasonable notice.

Security Incidents

You must immediately (within 24 hours) notify us of any actual or potential breach, loss of or compromise to, any GKN Information or Information Asset or any of your policies, procedures, systems, controls or other measures relating to Information Security (including any cyber-attack or other data breach), or any other security incident which affects your ability to supply GKN. You must report breaches to ITsecurity@gknautomotive.com

Cooperation & Reporting

Following any such security incident, you will cooperate with us and provide such information as we may reasonably request to enable us to investigate such security incident, mitigate the risks of such security incident, or comply with our obligations to third parties or under any applicable law.

Training & awareness

Training

You will ensure that adequate training on Information Security is undertaken by all your employees, workers and other representatives in relevant roles, and that this training meets industry best practice. You will ensure mandatory training will be undertaken at least annually. You will provide us with evidence of such training upon request.

Awareness

You will promote, throughout your organisation, awareness of Information Security and its importance, so as to create a culture in which Information Security is taken seriously by your employees, workers and other representatives.

Monitoring, audit & assurance

Monitoring

You may be subjected to regular review and monitoring by us to ensure that information security risks are identified and mitigated. You will cooperate fully with such monitoring.

Audit

You will grant us (and third parties appointed by us) the right to enter any premises or location owned or occupied by you on reasonable notice during normal business hours (or in the event of an emergency at any time without notice) to audit, verify, assess and evaluate your compliance with these requirements, any Disclosed Arrangements, any Supplier-Specific Requirements and your Information Security resilience generally.

Assurance

You will, when requested by us, certify in writing compliance with these requirements, any Disclosed Arrangements, any Supplier-Specific Requirements and your Information Security resilience generally,
and provide such supporting evidence of compliance as we may reasonably request.

Transparency & cooperation

Transparency

You acknowledge that the purpose of these requirements is to ensure you maintain an adequate level of Information Security resilience and that we would always prefer that you bring any issues or concerns to our attention so that we can work with you to address them. You will be transparent and honest in your dealings with us relating to Information Security. You will promptly inform us of any material change in your business, operations, policies or procedures which may be reasonably likely to impact our assessment of your Information Security resilience. You will not conceal any information security concerns, risks or incidents.

Cooperation

You will cooperate with us and pay due regard to all recommendations we may make which exceed these requirements, any Disclosed Arrangements or any Supplier Specific Requirements. You will communicate and engage with us when requested, including participating in review meetings and telephone calls.

No Liability

You acknowledge that where we do give you advice, recommendations or support in order to improve your information security resilience, it
is your responsibility to verify that such advice, recommendations or support are suitable for your business needs, and we do so without any obligation or liability whatsoever on our part.

Following contract expiry or termination

Return or Destruction of GKN Information

The information security risks when Your Contract ends will vary depending on the circumstances and the value of the GKN Information concerned. Upon termination or expiry of Your Contract, you must return all GKN Information which you or your suppliers or third parties authorised by you have in your possession or control. Any GKN Information which takes the form of residual or metadata must be appropriately deleted or destroyed. Where return of GKN Information is not reasonably practicable, we may authorise you to destroy such GKN Information, in which case you will certify in writing that you have done so.

Discontinued Access

Where we have granted you access to any Information Asset and you no longer require such access for the purposes of performing your contract with GKN Automotive, we will revoke such access and you will promptly notify us if you become aware that such access has not been revoked, notwithstanding it is no longer required.