SEG Automotive Germany GmbH

Security Best Practices for Third Parties

SEG Automotive is fully committed to meeting all legal and regulatory obligations. This commitment extends to all relationships with clients, suppliers, contractors, and business partners, and outlines information Security requirements for Third Parties working with SEG Automotive.

These requirements help protect the availability, integrity, and confidentiality of SEG's information and technology assets when:

- You provide technological products (hardware, software) or services to SEG Automotive.
- Have access to SEG Automotive's Information & Technology Assets. Information Security Standards:

1. Third Party Assessment

To ensure Information Security and Data Protection compliance, SEG Automotive conducts a Third-Party evaluation Risk process before granting access to information or technology assets. This assessment includes:

- Reviewing your security policies and practices.
- Evaluating the alignment between your security measures and SEG Automotive's requirements.
- Qualifying Third Parties for potential services or continued collaboration.

SEG Automotive reserves the right to reassess Third Parties periodically to ensure ongoing compliance and security improvements.

2. Key Definitions

Audit: Independent review to assess compliance, identify risks, and suggest improvements.

Business Owner: Person accountable for overseeing a process or application system.

Confidential Information: Data restricted to authorized personnel, requiring explicit approval for release.

SEG Automotive Germany GmbH

SEG Automotive Policies:

Information Security Central Directives
Data Protection Central Directive
Statement on Information Security & Data Protection
Supplier Code of Conduct
Handling of Information Security Incidents

Security Incident: Unauthorized access, modification, disclosure, destruction of data, or disruption of IT operations.

Subcontractor: Third parties engaged by vendors to assist in service delivery.

3. Information Security Controls

Third parties must adopt industry best practices (ISO/IEC 27001, NIST Cybersecurity Framework, TISAX), including:

Change Management: Robust and documented processes, including structured release cycles (ITIL or equivalent).

Vulnerability Management: Security patches, updates, and IT asset changes must follow standard change management. Approved operational change windows may be agreed upon between SEG Automotive and Third Parties.

Environment Separation: Development, test, production, and backup environments should be physically and logically isolated to reduce security risks.

Backup & Retention Policies: Defined backup frequency and retention cycles aligned with contractual agreements.

Intrusion Detection & Prevention: Active malware protection with regularly updated antivirus software.

Download Restrictions: Tools must block unauthorized internet downloads or use of removable media on Third Party IT Assets.

Network & Physical Security: Secure perimeter protection and controlled access.

SEG Automotive Germany GmbH

Password Standards: Enforce password complexity requirements and Multifactor Authentication to mitigate weak credential risks.

Software Development Security: Adopt secure software development practices (S-SDLC).

Security Reviews: Technical audits of data centers and IT operations.

Forensic Investigations: Procedures for handling cybersecurity incidents.

4. Human Resource Security

Third parties must enforce employee security awareness before granting access to SEG Automotive's assets, including:

- Codes of conduct, ethics policies, and confidentiality agreements.
- Information Security and Data Protection Policies.
- Mandatory Information security and Data protection training with employee acknowledgment.

Employees must not:

- Monitor, intercept, or interfere with SEG Automotive communications.
- Use IT assets for personal or unauthorized activities (e.g., running a personal business).
- Modify, encrypt, or destroy SEG Automotive Confidential Information without consent, within SEG Automotive environment.

SEG Automotive reserves the right to revoke access at its discretion for policy violations.

5. Secure Information Exchange

Third parties must ensure secure data exchange using:

- Managed file transfer services or encrypted email tools.
- Compliance with SEG Automotive's security protocols when sharing Confidential Information.

SEG Automotive Germany GmbH

6. **Information Classification & Disposal**

Third parties must implement data handling standards addressing:

- Information classification, secure storage, encryption, and retention policies.
- Secure data disposal practices, including encrypted backup management and controlled access mechanisms.

7. **Consequences of Non-Compliance**

Any Third Party that fails to comply with SEG Automotive's information security policies shall be considered in breach of contract. Such violations may result in immediate corrective action, including suspension or termination of the contractual relationship between SEG Automotive and the Third Party.

Additionally, if the Third Party's actions constitute a violation of applicable laws or regulations, SEG Automotive reserves the right to take further legal measures, which may include:

Regulatory penalties imposed by authorities for failure to meet security and compliance standards.

Civil liability, including financial compensation for damages resulting from non-compliance.

Law enforcement intervention, which could lead to criminal prosecution or other legal consequences for the responsible parties.

SEG Automotive expects all Third Parties to adhere to the highest standards of cybersecurity and regulatory compliance. Failure to do so may result in severe legal and business repercussions, for which the Third Party shall be held fully accountable.