ADIENT VENDOR SECURITY STANDARD

Contents

ADIENT VENDOR SECURITY STANDARD

1. Scope and General Considerations

This Security Standard sets forth security requirements (security measures and procedures) with respect to Adient Information Assets (ADIENT IA) created, collected, received, transferred or otherwise obtained or disclosed by Adient to Vendor in connection to the Services.

In the event of any conflict between the provisions of this Standard and other contractual provisions, the provisions that are more protective of ADIENT IA shall prevail.

In order to fulfill Adient's high security and compliance standards, Vendor shall implement adequate and appropriate technical and organizational security measures designed and necessary to secure ADIENT IA against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access - in particular where the Processing involves the transmission of data over a network - in light of the relevant risks presented by the Processing. These measures shall ensure a level of security appropriate to the risks presented by the Processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation.

Vendor shall periodically review and update such measures and maintain the same in accordance with no less than industry-standard methods of protection. Without limiting its obligations otherwise set forth herein, Vendor shall comply with all applicable laws relating to its Processing of ADIENT IA.

Vendor warrants and represents to have implemented security measures that meet or exceed the requirements laid down in this Security Addendum. Vendor needs to provide Adient with sufficient documented evidence to demonstrate adherence to this Security Standard.

Failure to maintain these obligations constitutes a material breach of this Security Standard and, in addition to Adient's other rights, Adient may choose to terminate the Agreement.

To the extent Adient IA is Personal Data, Vendor additionally shall abide by applicable privacy regulations and agree to specific Data Processing Terms with Adient where necessary.

2. Definitions

“Adient”	Shall mean the same Adient entities as listed in the Agreement.
“Adient Information Assets” (ADIENT IA)	Shall include any body of Adient information or knowledge that is defined, organized, and managed as a single unit and has a recognizable and manageable value, risk, content, and lifecycle. It includes Adient’s information computing systems and data, including specifically Personal Data.
“Agreement”	Shall include any kind of MSA, Statement of Work (“SOW”) or any other kind of agreement between Adient and Vendor with regards to the Services.
“Security Event”	a) indicates that the security of an information system, service, or network **may have been** breached or compromised; b) indicates that an information security policy **may have been** violated or a safeguard may have failed; c) Means a Log Entry with a negative consequence or potentially negative consequence, such as system crashes, network packet floods, unauthorized use of system privileges, and unauthorized access to sensitive data or execution of malicious code that destroys data hasoccurred.
“Security Breach“	Means a Security Event leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to ADIENT IA, including Personal Data, transmitted, stored or otherwise processed in connection with the provisioning of the Services;
“Personal Data“	Means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
“Processing“	Means any operation or set of operations which is performed on Adient IA, including Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
“Security Rules“	Means rules applicable to the Vendor with regards to information security, including regulatory rules and state of the art standards on information security and rules that derive from applicable laws (e.g., privacy laws)
“Services“	Mean services as described in the Agreement, or other mutually agreed upon written description of services that has been executed by the parties
“Sub-Contractor“	Means any service contractor or service provider engaged by Vendor or by any other Sub-Contractor that directly, or indirectly, impact ADIENT IA. This includes any kind of services involving Processing, accessing, communicating, hosting or managing the ADIENT IA, or adding or terminating services or products to existing information by a person engaged or included to the service by the Vendor.
“Vendor“	Any party other than Adient that processes, stores or transports ADIENT IA, including Vendor cloud service providers.

3. Governance

3.1 Personnel

Prior to granting individuals physical or logical access to facilities, systems or data which involve ADIENT IA, Vendor shall take reasonable steps to ensure that its employees, other persons acting under its authority and other persons at the place of work concerned (including third party users, tenants and/or customers) are bound to legally binding obligations that meet or exceed the security measures mentioned in this Security Standard, measures enacted or to be enacted by relevant authorities or as provided by applicable Security Rules (for Sub-Contractors see section 3.2 below).

Pursuant to local laws, regulations, ethics and contractual constraints all Vendor’s employment candidates and third parties shall be subject to background verification proportional to the data classification to be accessed, the business requirements and acceptable risk. Vendor shall ensure that their staff that has access to ADIENT IA is adequately informed and skilled to ensure the protection of ADIENT IA.

3.2 Sub-Contractors

Whenever Vendor subcontracts work that relates to ADIENT IA to Sub-Contractors the applicable requirements set forth under this Security Standard need to be complied with at all times. Vendor shall provide the list of Sub-Contractors and applicable certifications upon request. Adient may object to the use of a new Sub-Contractor in writing if the new Sub-Contractor represents an unacceptable risk to the security of the ADIENT IA.

Pursuant to local laws, regulations, ethics and contractual constraints all Vendor’s Sub-Contractors shall be subject to background verification proportional to the data classification to be accessed, the business requirements and acceptable risk. Vendor shall ensure that all the Vendor’s sub-contractors that touch ADIENT IA holds applicable security certifications and adheres to security best practices.
Vendor shall ensure that all Sub-Contractors have been bound by an agreement including explicit coverage of all relevant security requirements compatible with this Standard and pursuant to applicable Security Rules. Sub-Contractors specifically need to be obliged to bind its personnel to substantially similar obligations as laid down in Section 3.1 above.

Vendor shall demonstrate compliance with information security and confidentiality, service definitions and delivery level agreements included in such third-party contracts. Third party reports, records and services shall undergo audit and review, at planned intervals, to govern and maintain compliance with the service delivery agreements.

Vendor remains responsible to Adient for any and all performance by its Sub-Contractors in relation to the protection of ADIENT IA.

Vendor must provide a non-disclosure agreement for each Sub-Contractor that relates to ADIENT IA.

3.3. Development of Applications

Vendor applications shall be designed in accordance with industry accepted security standards (i.e., OWASP for web applications) and shall comply with applicable regulatory and businessrequirements.

Vendor shall establish a program for the systematic monitoring and evaluation to ensure that standards of quality are met, including but not limited to all outsourced software development. Vendor shall supervise and monitor the development of all software and shall include security requirements, independent security review of the environment by a certified individual, certified security training for software developers, and code reviews. Certification for the purposes of this control shall be defined as either an ISO/IEC 17024 accredited certification or a legally recognized license or certification in the applicable legislative jurisdiction.

At a minimum, for Adient specific applications, the Vendor shall provide a bug list and code analysis at time of release and is fully responsible for defects, including vulnerabilities that are discovered in the application.

4. Technical and Organizational Measures

Vendor shall implement the following technical and organizational measures to secure the confidentiality, integrity, availability, resilience, of ADIENT IA:

4.1 Confidentiality

4.1.1 Physical access control

Vendor shall implement suitable measures to prevent unauthorized persons from gaining physical access to the data Processing equipment where ADIENT IA are Processed, transferred, or used in any manner. This shall be accomplished by, e.g. providing that entries to data Processing facilities (the rooms housing the application servers, computer hardware, database and related equipment etc.) are capable of being locked.

4.1.2 Admission control

Vendor shall implement suitable measures to prevent its data Processing systems from being used by unauthorized persons.

4.1.3 Virtual access control

Vendor shall implement suitable measures, including provisioning and de-provisioning processes, to ensure that those persons authorized to use a Processing system are only able to access ADIENT IA within the scope of their need to access (authorization) and in accordance with business, security, compliance and service level agreement (SLA) requirements, and that ADIENT IA cannot be read, copied, modified or deleted without appropriate authorization during Processing and after logging.

Vendor shall implement timely de-provisioning, revocation or modification of user access upon any change in status of employees, contractors, customers, business partners or third parties, including termination of employment, contract or agreement, change of employment or transfer within the organization.

Prior to the Vendor granting access to ADIENT IA's and systems, all identified security, contractual and regulatory requirements shall be remediated where applicable.

4.1.4 Separation control

Vendor shall ensure a clear separation of ADIENT IA from other customers' data. The separation must be ensured at the logical level which includes the application and preferably at the physical level.

Vendor shall ensure that data collected for different purposes can be processed separately

4.1.5 Encryption

4.1.5.2 Transport Encryption

All Adient IA transported on any untrusted network (such as the internet) requires encryption (e.g. https).

4.1.5.1 Storage Encryption

The Vendor must implement strict measures to ensure that Adient IA, specifically the data associated with Adient customers is encrypted at rest / in storage. Only for other than Adient customer data parties may agree on a deviation to this storage encryption requirement.

4.1.5.2 Encryption Key Management

Adient must manage the encryption keys for storage encryption, not the Vendor, specifically where data is associated with Adient customers. Only for other than Adient customer data parties may agree on a deviation to this key management requirement.

4.1.6 Job / Assignment Control

Vendor shall implement suitable measures to ensure that, in the case of commissioned Processing of ADIENT IA, ADIENT IA are Processed strictly in accordance with the instructions of Adient.

4.2 Integrity of the Data

4.2.1 Input Control and Logging

Vendor shall retain audit logs recording user access activities, modification or deletion of any data, authorized and unauthorized access attempts, system exceptions, and information Security Events, complying with applicable policies and regulations. Vendor shall review audit logs at least daily and file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents.

4.2.2 Transmission control

Vendor shall implement suitable measures to ensure that, during electronic transfer, transportation or when being saved to data carriers, ADIENT IA cannot be read, copied, modified or deleted without authorization, and that it is possible to check and establish to which bodies the transfer of ADIENT IA by means of data transmission facilities is envisaged.

Applicable for Vendors providing network services

Vendor network environments shall be designed and configured to restrict connections between trusted and un-trusted networks and reviewed at planned intervals, documenting the business justification for use of all services, protocols, and ports allowed, including rationale or compensating controls for those protocols considered to be insecure. Network architecture diagrams must clearly identify high-risk environments and data flows that may have regulatory compliance impacts.

4.3 Capacity & Resource Planning / Business Continuity / Availability Control

4.3.1 Capacity & Resource Planning

Vendor shall plan, prepare and measure its systems availability, quality, and adequate current and preventive capacity and resources to deliver the required system performance in accordance with regulatory, contractual and business requirements. Vendor shall provide a copy of the Capacity / Resource Planning Metrics and applicable assessments to Adient upon request.

4.3.2 Business Continuity

Vendor shall implement and maintain a Business Continuity Program; ensuring continuity of vendor services (i.e. customer service, technical support, incident management). Vendor shall conduct a business continuity exercise annually and shall provide Adient evidence of business continuity exercise within 30 days of Adient's request. Evidence shall include Date and time of exercise, Scope of exercise, Summary and finding.

4.3.3 Availability Control

Vendor shall implement suitable measures to ensure that ADIENT IA are protected from accidental destruction or loss and from denial of service attacks.

Additional Back-up / Disaster Recovery requirements for Vendors providing hosting services for ADIENT IA:
Vendor shall ensure that all ADIENT IA are regularly backed up to facilitate quick recovery in case of disasters.

Application and System architecture(s) shall support Adient's Disaster Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

Vendor shall implement and maintain a Disaster Recovery Program; ensuring a continuity of technologies, application and software services provided to Adient by this agreement. Vendor shall conduct a disaster recovery exercise annually and shall provide Adient evidence of disaster recovery exercise within 30 days of Adient's request. Evidence shall include:

- Date and time of exercise
- Scope of exercise
- Summary and Findings
- Achieved Recovery Time Objective
- Achieved Recovery Point Objective
- Method used to validate RPO

Specifically, Vendor shall implement measures to ensure that:

- a back-up is performed at least daily;
- backups are stored off-site and available for restore in case of failure of SAN infrastructure for database server;
- only Adient may authorize the recovery of backups (if any) or the movement of data outside the location where the physical database is held, and security measures will be adopted to avoid loss or unauthorized access to data, when moved;
- backups are only re-used if information previously contained is not intelligible and cannot be re-constructed by any technical means; other removable media is destroyed or made unusable if not used; and
- testing the recovery of backups is carried out at planned intervals

4.4. Resilience

4.4.1 Vulnerability / Patch Management

Vendor shall establish policies and procedures and implement mechanism for Vendor vulnerability and patch management, ensuring that application, system, and network device vulnerabilities are evaluated, and vendor-supplied security patches applied in a timely manner taking a risk-based approach for prioritizing critical patches.

4.4.2 Anti-Virus / Malicious Software

Service providers who will use their own (i.e. not Adient controlled) computing devices at an Adient or non-Adient location must have an Adient approved personal firewall and Adient approved anti-virus software with up to date definition files on each PC.

Vendor shall ensure that all antivirus programs are capable of detecting, removing, and protecting against all known types of malicious or unauthorized software on a continuous basis.

4.4.3 Security Checks

Vendor shall provide on-going security checks to ensure data security and prevent breaches due to security vulnerabilities in the application or through malicious employees

4.4.4 Unauthorized Software Installations

Vendor shall establish policies and procedures and implement mechanisms to restrict the installation of unauthorized software. Where there is an Adient private environment the Vendor shall report any exceptions, which need to be approved by ADIENT prior to installation.

4.4.5 Production changes

Changes to the Vendor provided Adient production environment shall be documented and tested and need approval by Adient prior to implementation. Production software and hardware changes may include applications, systems, databases and network devices requiring patches, service packs, and other updates and modifications.

5. Information Security Management System

5.1 General Management System

Vendor shall maintain a proper information security management program adequately communicated and published to employees, contractors and other relevant external parties.

5.2 Third-Party Independent Audit Reports

Vendor shall provide evidence of security controls and their effective operation and provide Adient an acceptable annual third-party security report scoped to the specific services Adient is procuring from Vendor and all Vendor Sub-Contractors that transport, store or process Adient data, e.g.

SSAE-18 (U.S.), CSAE-3416 (Canada), ISAE-3402 (International) SOC 2 Type 2 Report on an annual basis at no cost to Adient. This annual security report will follow the AICPA standards for a SOC 2 Type 2 report and will include the tests and effectiveness of Vendor controls associated with security (includes user administration, privileged and emergency access, network and server security), change management, interface and jobs, backup and recovery, configuration management, physical security, confidentiality, processing integrity, privacy and availability. If upon review of the report, the testing was identified as not being performed correctly or reached incorrect conclusion, the Adient Internal Audit and Information Security teams will have the right to audit the Vendor controls.

Vendor agrees to remediate any deficiencies revealed in such report in a commercially reasonable manner and time frame.

Upon Adient request, Vendor shall also provide an acceptable third-party system / application penetration security report and vulnerability assessment security report on an annual basis.

Applicable for Vendors hosting ADIENT IA

Vendor shall develop, document, approve and implement an Information Security Management Program (ISMP) that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction, e.g. ISO 27001:27018.

5.3 Vendor Security Assessment Platform Engagement

Vendor will engage Adient's Vendor Security Assessment platform in an on-going manner with No High-Severity findings.

5.4 Audits / Inspections

In addition, at planned intervals and upon prior written notice, Adient may inspect Vendor's operating facilities or conduct an audit to ensure Vendor is compliant with policies, procedures, standards and applicable regulatory requirements and to ascertain compliance with this Standard. Adient or an independent audit team may carry out the inspection. Vendor shall fully cooperate with any such audit and investigation procedures initiated by Adient.

6. Risk Management

Vendor shall develop and maintain an enterprise risk management framework to manage risk to an acceptable level. Vendor shall perform formal risk assessments at least annually, or at planned intervals, determining the likelihood and impact of all identified risks.

Vendor shall mitigate risks to an acceptable level. Acceptance levels based on risk criteria shall be established and documented in accordance with reasonable resolution time frames and executive approval.

Vendor will provide evidence of cybersecurity insurance, i.e. Privacy / Network Security (Cyber) liability coverage providing protection against liability for (1) Security Breaches (no matter how it occurs); (2) system breach; (3) denial or loss of service; (4) introduction, implantation, or spread of malicious software code; (5) unauthorized access to or use of computer systems. No condition precedent, including any exclusion/restriction for unencrypted portable devices/media may be on the policy. Minimum required insurance limit - $10,000,000.

7. Event, Incident, Threat and Vulnerability Management / Security Incidents and Breach Notification

Vendor shall establish policies and procedures to triage security related events and ensure timely and thorough incident management.
Vendor shall notify Adient promptly without undue delay in the event of a potential Security Breach. The information provided will contain the details of ADIENT IA compromised, including:

- Information on the ADIENT IA, data / persons affected such as categories and number of persons affected;
- A description of the nature of the unlawful disclosure,
- The identity and contact details of a contact person
- The likely consequences of the potential Security Breach, and
- The recommended measures to minimize possible harm.

Vendor shall provide all additional information reasonably requested by Adient to investigate the potential Security Breach.

In addition, Vendor shall inform Adient promptly without undue delay if (i) Vendor or its Personnel, Affiliates or Sub-Contractors infringe Security Rules or obligations under this Standard, (ii) significant failures occur during the Processing, or (iii) there is reasonable suspicion of the occurrence of an event as defined under (i) and (ii) of this paragraph. In consultation with Adient, Vendor shall take appropriate measures to secure ADIENT IA and limit any possible detrimental effect on Adient and any persons.

In the event a follow-up action resulting from a Security Breach requires legal action, subject to the relevant jurisdiction, proper forensic procedures including chain of custody shall be carried out by the Vendor and any Sub-Contractor for collection, retention, and presentation of evidence and shall be made available upon request.

8. Return and Deletion of ADIENT IA

Upon termination of these Terms, Vendor, at the discretion of Adient, shall return to Adient or destroy and delete all ADIENT IA and other materials containing ADIENT IA from Adient subject to Processing, unless applicable rules require storage of the ADIENT IA. Additionally, all ADIENT IA should be expunged from any computer, server, media, storage or similar device including backup storage in which it was stored or processed by Vendor or by its Sub-Contractors. Vendor shall certify that this has been done upon Adient's request.

Vendor shall establish policies and procedures and implement mechanisms for the secure disposal and complete removal of Adient data from all Vendor storage and certification of proper disposal.

9. Implementation of Security Requirements

In accordance with the foregoing, Vendor shall:

	9.1 System Security
1.	Actively monitor industry resources (*e.g.*, www.cert.org pertinent software vendor mailing lists and websites) for timely notification of all applicable security alerts pertaining to Vendor networks and Information Resources. (**Security Alerts**)
2.	Scan externally-facing Information Resources with applicable industry standard security vulnerability scanning software (including, but not limited to, network, server, and application scanning tools) at a minimum monthly.
3.	Scan internal Information Resources with applicable industry standard security vulnerability scanning software (including, but not limited to, network, server, application and database scanning tools) at a minimum monthly.

4. Upon Adient’s request, furnish to Adient its most current scanning results for the Information Resources.
5. Deploy one or more Intrusion Detection/Prevention Systems (IDS or IPS) in an active mode of operation.
6. Have and use a documented process to remediate security vulnerabilities in the Information Resources, including, but not limited to, those discovered through industry publications, vulnerability scanning, virus scanning, and the review of security logs, and apply appropriate security patches promptly with respect to the probability that such vulnerability can be, or is in the process of being exploited.
7. Assign security administration responsibilities for configuring host operating systems to specific individuals.
8. Ensure that its security staff has reasonable and necessary experience in information/network security.
9. Ensure that all of Vendor’s Information Resources are and remain ‘hardened’ including, but not limited to, removing, or disabling unused network services (*e.g.,* finger, rlogin, ftp, simple TCP/IP services) and installing a system firewall, TCP Wrappers or similar technology.
10. Change ALL default account names and/or default passwords or credentials in accordance with the password requirements set forth herein.
11. Limit system administrator/root (or privileged, super user, or the like) access to host operating systems only to individuals requiring such high-level access in the performance of their jobs. Ensure system administrators are not performing tasks for non-privileged users using system administrator accounts or credentials.
12. Require system administrators to restrict access by users to only the commands, data, and Information Resources necessary to perform authorized functions.

9.2 Physical Security

13. Ensure that all of Vendor’s networks and Information Resources are located in secure physical facilities with access limited and restricted to authorized individuals only.
14. Monitor and record, for audit purposes, access to the physical facilities containing networks and Information Resources used in connection with Vendor’s performance of its obligations under the Agreement.

9.3 Network Security

15. When providing Internet-based services to Adient, protect Adient Information by the implementation of a network demilitarized zone (DMZ). Web servers providing service to Adient shall reside in the DMZ. Information Resources storing Adient Information (such as application and database servers) shall reside in a trusted internal network.
16. Vendors hosting Payment Card Industry (PCI)-regulated data must provide attestation of compliance with Payment Card Industry Data Security Standards (PCI DSS).
17. Upon Adient’s request, provide to Adient a logical network diagram detailing the Information Resources (including, but not limited to, firewalls, servers, etc.) that will support Adient.
18. Have a documented process and controls in place to detect and handle unauthorized attempts to access Adient Information.
19. Use Strong Encryption for the transfer of Adient Information outside of Adient-controlled or Vendor-controlled facilities or when transmitting Adient Information over any untrusted network.
20. Require two-factor authentication and encryption for any remote access use of Information Resources.

9.4 Information Security

21. Isolate Adient’s applications and Adient Information from any other applications and information of Vendor or Vendor’s customers, by using physically separate servers or, alternatively, by using logical access controls where physical separation of servers is not implemented.
22. Have a documented procedure for the secure backup, transport, storage, and disposal of Adient Information and upon Adient’s request, provide such documented procedure to Adient.
23. Maintain and, upon Adient’s request, furnish to Adient a business continuity plan that ensures that Vendor can meet its contractual obligations under the Agreement, including the requirements of any applicable Statement of Work or Service Level Agreement. Upon Adient’s request, Vendor shall promptly update its business continuity plan to include a potential threat scenario.
24. Store Adient sensitive information using Strong Encryption.
25. Limit access to Adient Information, including, but not limited to, paper hard copies, only to authorized persons or systems.
26. Be compliant with any applicable government- and industry-mandated information security standards. (Examples of such standards include, but are not limited to, the Payment Card Industry- Data Security Standards (PCI-DSS), National Automated Clearing House Associates (NACHA) Rules, and Electronic Data Interchange (EDI) standards and the information security requirements documented within laws, such as HIPAA.)
27. Return, or, at Adient’s option, destroy all Adient Information, including electronic and hard copies, unless otherwise provided in an Agreement, within thirty (30) days after the sooner of: (a) expiration or Termination or Cancellation of the Agreement; (b) Adient’s request for the return of Adient Information; or (c) the date when Vendor (or its Vendors or representatives) no longer needs the Adient Information. In the event that Adient approves destruction as an alternative to returning the Adient Information, then Vendor shall certify the destruction (*e.g.*, degaussing, overwriting, performing a secure erase, performing a chip erase, shredding, cutting, punching holes, breaking, etc.) as rendering the Adient Information non-retrievable.
28. Unless otherwise instructed by Adient, when collecting, generating, or creating information for, through or on behalf of Adient or under the Adient brand, shall whenever practicable, label such information as “Confidential - Adient Proprietary Information” or at a minimum, label Adient Information as “Confidential” or “Proprietary”. Vendor acknowledges that Adient Information shall remain Adient-owned Information irrespective of labeling or absence thereof.

9.5 Identification and Authentication

29. Assign unique UserIDs to individual users.
30. Have and use a documented UserID Lifecycle Management process including, but not limited to, procedures for approved account creation, timely account removal, and account modification (*e.g.,* changes to privileges, span of access, functions/roles) for all Information Resources and across all environments (*e.g.,* production, test, development, etc.).
31. Enforce the rule of least privilege (*i.e.,* limiting access to only the commands and Adient Information necessary to perform authorized functions according to one’s job function).
32. Limit failed login attempts to no more than five (5) successive attempts and lock the user account upon reaching that limit. Access to the user account can be reactivated subsequently through a manual process requiring verification of the user’s identity or, where such capability exists, can be automatically reactivated after at least three (3) minutes from the last failed login attempt.
33. Terminate interactive sessions, or activate a secure, locking screensaver requiring authentication, after a period of inactivity not to exceed fifteen (15) minutes.
34. Require password expiration at regular intervals not to exceed ninety (90) days.

35. Use an authentication method based on the sensitivity of Adient Information. When passwords are used, they must meet these minimum requirements:
    - Passwords must be a minimum of eight (8) characters in length.
    - Passwords must contain characters from three (3) these groupings: alpha, numeric, and special characters.
    - Passwords must not be the same as the UserId with which they are associated.
    - Password construction must be complex and not contain names, dictionary words, combinations of words, or words with substitutions of numbers for letters, *e.g.*, s3cur1ty.
    - Passwords must not contain repeating or sequential characters or numbers.
    - Passwords must be changed every ninety (90) days or less.
    - Passwords must be at least 1 day old before a change is allowed.
    - The last thirteen (13) passwords must be prevented from re-use.

    Notes: 1. When systems or applications do not enforce these password requirements, users and administrators must be instructed to comply with these password requirements when selecting passwords.

    2. Applications housing more sensitive Adient Information, as identified by Adient, may require an authentication mechanism stronger than passwords and the authentication mechanism must be approved by Adient in advance in writing. Examples of stronger authentication methods include tokens, digital certificates, passphrases, and biometrics.
36. Use a secure method for the conveyance of authentication credentials (*e.g*., passwords) and authentication mechanisms (*e.g*., tokens or smart cards). Ensure user session authentication is protected by utilizing SSL encryption on Vendor websites.

9.6 Warning Banner

37. Display a warning or "no-trespassing" banner on applicable login screens or pages when in Vendor's environment and not an Adient-branded product or service.

    (Example long version):
    This is an <company name> system, restricted to authorized individuals. This system is subject to monitoring. Unauthorized users, access, and/or modification will be prosecuted.

    (Example short version):
    <company name> authorized use ONLY, subject to monitoring. All other use prohibited.

    For Adient-branded products or services or for software developed for Adient, Vendor shall display a warning banner on login screens or pages provided by Adient.

9.7 Software and Data Integrity

38. Have current antivirus software installed and running to scan for and promptly remove viruses.
39. Separate non-production Information Resources from production Information Resources.
40. Have a documented software change control process including back out procedures.
41. For applications which utilize a database that allows modifications to Adient Information, have database transaction logging features enabled and retain database transaction logs for a minimum of six (6) months.
42. For all software developed, used, furnished and/or supported under this Agreement, review such software to find and remediate security vulnerabilities during initial implementation and upon any modifications and updates.
43. Perform quality assurance testing for the application functionality and security components (*e.g.*, testing of authentication, authorization, and accounting functions, as well as any other activity designed to validate the security architecture) during initial implementation and upon any modifications and updates.

9.8 Privacy Issues

44. Restrict access to any Adient information to authorized individuals.
45. Not store Adient information on removable media (*e.g*., USB flash drives, thumb drives, memory sticks, tapes, CDs, external hard drives) except: (a) for backup and data interchange purposes as allowed and required under contract, and (b) using Strong Encryption.

9.9 Monitoring and Auditing Controls

46. Restrict access to security logs to authorized individuals.
47. Review, on a routine basis, security logs for anomalies and document and resolve all logged security problems in a timely manner.
48. Retain complete and accurate records relating to its performance of its obligations arising out of these Security Requirements and Vendor's compliance herewith in a format that will permit audit for a period of no less than three (3) years, or longer as may be required pursuant to a court order or civil or regulatory proceeding. Notwithstanding the foregoing, Vendor shall only be required to maintain security logs for a minimum of six (6) months.
49. Permit Adient to conduct an audit to verify Vendor's compliance with its contractual obligations in connection with these Vendor Information Security Requirements. Upon Adient's request for audit, Vendor shall schedule a security audit to commence within thirty (30) days from such request. In the event Adient, in its sole discretion, deems that a security breach has occurred, Vendor shall schedule the audit to commence within one (1) day of Adient's notice requiring an audit. This provision shall not be deemed to and shall not limit any more stringent audit obligations permitting the examination of Vendor's records contained in an Agreement.
50. Within thirty (30) days of receipt of the audit report, provide Adient a written report outlining the corrective actions that Vendor has implemented or proposes to implement with the schedule and current status of each corrective action. Vendor shall update this report to Adient every thirty (30) days reporting the status of all corrective actions through the date of implementation. Vendor shall implement all corrective actions within ninety (90) days of Vendor's receipt of the audit report.

9.10 Reporting Violations

51. Have and use a documented procedure to follow in the event of an actual or suspected unauthorized intrusion or other security violation, including but not limited to, a physical security or computer security incident (*e.g.*, hacker activity or the introduction of a virus or malicious code), that involves any Information Resources used in conjunction with supporting Adient and/or used by Vendor in fulfillment of its obligations under this Agreement, which includes immediate notification to the Adient Operations Center and/or the primary point of contact for this Agreement.
52. Provide Adient with regular status updates on any actual or suspected unauthorized intrusion or other security violation, that involves any Information Resources used in conjunction with supporting Adient and/or used by Vendor in fulfillment of its obligations under this Agreement, including, but not limited to, actions taken to resolve such incident, at four (4) hour intervals (or at other mutually agreed intervals or times) for the duration of the incident, and within five (5) days of the closure of the incident, a written report describing the incident, actions taken by the Vendor during its response and Vendor's plans for future actions to prevent a similar incident from occurring.

	9.11 Software Development and Implementation
53.	Ensure, prior to furnishing or developing custom software, that such software incorporates applicable industry best practices (OWASP and SANS CWE) to address and avoid potential security risks and common coding vulnerabilities.
	9.12 Compliance with Security Policies and Procedures
54.	Ensure that all personnel, subcontractors, or representatives performing work on any Adient Information Resources, or the Information Resources used to connect to Adient Information Resources or access, or house Adient Information under the Agreement are in compliance with these Security Requirements.
55.	At a minimum, annually review these Security Requirements to ensure that Vendor is in compliance with the requirements.
56.	Return all Adient owned or provided access devices (including, but not limited to, tokens and/or software), as soon as practicable, but in no event more than fifteen (15) days after the sooner of: (a) expiration, Termination, or Cancellation of the Agreement; (b) Adient's request for the return of such property; or (c) the date when Vendor (or its Vendors or representatives) no longer need such devices.

10. Connectivity Requirements

In the event Vendor has, or will be provided access to Adient's networks ("**Connectivity**") in conjunction with the Agreement, then, in addition to the foregoing, the following Connectivity Security Requirements shall apply to Vendor:

1. Vendor shall:

   a. Use only the mutually agreed upon facilities and connection methodologies to interconnect Adient's networks with Vendor's networks and to provide access to the data for each connection.
   b. NOT establish interconnection to endpoint resources and/or end users outside the United States. Interconnections to endpoint resources and/or end users outside the United States require the express prior written consent of Adient.
   c. Provide Adient access to any Vendor facilities during normal business hours for the maintenance and support of any Adient equipment (*e.g.,* router) used for the transmission of Adient Information under the Agreement.
   d. Use any Adient equipment provided under the Agreement only for the furnishing of those Services or functions explicitly defined in the Agreement.
   e. Ensure that all Vendor interconnections to Adient pass through the designated Adient perimeter security gateway (*e.g.,* firewall)**.**
   f. Ensure that Vendor interconnections to Adient terminate at a perimeter security gateway (*e.g.,* firewall) at the Vendor end of the connection
   g. Maintain logs of all sessions that pass through the Vendor's perimeter security gateway. These session logs must include sufficiently detailed information to identify the end user or application, origination IP address, destination IP address, ports / service protocols used and duration of access. These session logs must be retained for a minimum of six (6) months.

2. In addition to other rights set forth herein, in relation to Connectivity, Adient shall have the right to:

   a. Gather information relating to access, including Vendor's access, to Adient networks and Information Resources. This information may be collected, retained and analyzed by Adient to identify potential security risks without further notice. This information may include trace files, statistics, network addresses, and the actual data or screens accessed or transferred.
   b. Immediately suspend or terminate any interconnection if Adient, in its sole discretion, believes there has been a breach of security or unauthorized access to or misuse.