Data Privacy and Security Addendum ("DPSA") To

_____ (the "Agreement") Dated as of _____

Between Volkswagen Group of America ("VWGoA") and _____ ("Supplier")

This DPSA shall, effective as of the date executed below, be incorporated into and become a part of the Agreement. Terms not defined herein shall have the meaning set forth in the Agreement. Nothing in this DPSA limits or restricts VWGoA's rights or Supplier's obligations under the Agreement in relation to the protection of Personal Information (defined below) or permits Supplier to Process (defined below) (or permit the Processing of) Personal Information in a manner which is prohibited by the Agreement. In the event of a conflict between the DPSA and Agreement, the terms and conditions of the DPSA shall prevail.

All VWGoA Data (defined below) shall be deemed "Confidential Information" under the Agreement. The parties' obligations under this DPSA shall survive after the termination or expiration of the Agreement to the extent that Supplier lawfully continues to retain any VWGoA Data.

1. Definitions.

1.1 "Applicable Law" shall mean all applicable state, federal and international privacy, data protection and security laws and regulations applicable to Personal Information, such as the California Privacy Rights Act of 2020 (CPRA), California Consumer Privacy Act (CCPA), US state security and breach notification laws, the Health Insurance Portability and Accountability Act (HIPAA), the Gramm Leach Bliley Act (GLBA), and the EU General Data Protection Regulation 2016/679 (GDPR).

1.2 "Authorized Persons" shall mean Supplier's employees, contractors, subcontractors, or other agents who need to access VWGoA Data or VWGoA Systems to enable Supplier to perform the Services and who are bound by confidentiality and other obligations sufficient to protect VWGoA Data in accordance with the terms and conditions of this DPSA and Applicable Law.

1.3 "Personal Information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household, and any other information regulated by Applicable Law, such as, "Personal Information," "Personal Data," "Non-Public Personal Information," "Protected Health Information," "Sensitive Information," "Sensitive Personal Information," or "Special Categories of Personal Information,".

1.4 "Process" or "Processed" or "Processing" shall mean any operation or set of operations which is performed on Personal Information or sets of Personal Information, whether or not by automated means, such as, access, 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.

1.5 "Security Breach" shall mean the accidental or unlawful destruction, loss, alteration, unauthorized use, disclosure, acquisition, or access to VWGoA Data or VWGoA Systems that compromises the availability, confidentiality or integrity of VWGoA Data or VWGoA Systems.

1.6 "Services" means the products or services provided or to be provided under the Agreement.

1.7 "VWGoA Data" shall mean any VWGoA non-public or proprietary information and data in any form, ***including Personal Information***, provided by VWGoA and its authorized agents or subcontractors or otherwise Processed by Supplier in connection with the provision of Services under the Agreement.

1.8 "VWGoA Systems" shall mean any VWGoA system or network to which Supplier has access in order to perform Services for VWGoA.

1.9 "Sell," "Selling," "sale," or "sold" and "share," "shared," or "sharing" shall have the meanings set forth in Applicable Law, including the CCPA and CPRA.

2. Compliance with Laws

2.1 Supplier shall comply with Applicable Law relating to the privacy and security of VWGoA Data Processed by Supplier for or on behalf of VWGoA, and its affiliates, including, without being limited to, the laws of the countries whose citizens' or residents' Personal Information Supplier Processes in performing the Services. In the event of a claim against Supplier alleging a violation of a state or country specific Applicable Law, Supplier agrees to submit to a court of competent jurisdiction in that state or country.

2.2 To the extent that Supplier shares Personal Information, as defined by applicable law, with VWGoA, Supplier will do so in compliance with Applicable Law, including providing appropriate notice (including notice regarding the sharing of Personal Information with third parties) and obtaining consent if required; or, if Supplier is not the first party collector of such Personal Information, ensuring that suppliers of such data have provided appropriate notices and obtained any required consents to share such data. Supplier agrees to make available, upon request, information to demonstrate compliance, including a copy of the compliant notices or consents.

2.3 GLBA. To the extent the Gramm-Leach-Bliley Act applies, Supplier expressly understands and acknowledges that Supplier may have access to, or VWGoA may disclose to Supplier, "non-public personal information" ("NPPI"), as such term is defined in Regulation P issued by the Consumer Financial Protection Bureau. Without limiting any other obligations in this Addendum, the following shall apply to NPPI:

(a) Supplier will use or disclose NPPI only as strictly necessary to carry out the purposes for which VWGoA is disclosing the information to Supplier.

(b) Supplier has implemented and will continue to maintain safeguards reasonably designed to (i) ensure the security and confidentiality of NPPI; (ii) protect against any anticipated threats to or hazards to the security or integrity of NPPI; and (iii) protect against unauthorized access to or use of NPPI that could result in substantial harm or inconvenience to any individual.

2.4 As between the parties, all VWGoA Data remains, at all times, the property of VWGoA, and VWGoA has the right to direct Supplier in connection with Supplier's Processing of such VWGoA Data.

2.5 Supplier shall immediately inform VWGoA if it cannot comply with an instruction or, in its opinion, an instruction infringes any law applicable to VWGoA or Supplier, or if Supplier can no longer meet its obligations under Applicable Law.

2.6 VWGoA hereby instructs Supplier to Process Personal Information as necessary for the provision of the Services.

3. Supplier's Obligations

3.1 Supplier shall Process VWGoA Data and access VWGoA Systems solely for the purpose of providing the Services in accordance with the Agreement and upon VWGoA's written instructions, and not for any other purpose. Supplier shall not retain, use, or disclose the Personal Information for any purpose other than for the specific purpose of performing the Services specified in the Agreement or as otherwise permitted by law, including retaining, using, or disclosing the Personal Information for a commercial purpose other than performing the Services. Without limiting the generality of the foregoing, Supplier agrees it shall not: (i) Sell or Share the Personal Information; (ii) retain, use, or disclose the Personal Information for any purpose other than for the specific purpose of performing the Services in accordance with the Agreement, including retaining, using, or disclosing the Personal Information for a commercial purpose other than providing Services specified in the Agreement; (iii) retain, use, or disclose the Personal Information outside of the direct business relationship between Supplier and VWGoA, or (iv) combine VWGoA Data, including Personal Information, with Personal Information it receives from another source except to perform business purposes permitted by Applicable Law. Supplier hereby certifies that it understands the restrictions set forth in this Section and will comply with them.

3.2 Supplier shall maintain records of Processing activities carried out pursuant to this DPSA, containing all relevant details required by Applicable Law, but at a minimum, the following:

- the name and contact details of the Supplier and any other subcontractors and, where applicable, of the VWGoA' or Supplier's representative;
- the categories of Processing carried out on behalf of VWGoA;
- where applicable, information on cross-border transfers, including transfers of Personal Information to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers outside of the legally specified transfer mechanisms, the documentation of suitable safeguards for the Personal Information;
- where possible, a general description of the technical and organizational security measures.
- Supplier agrees to make such records available upon request to VWGoA and any relevant government authority.

3.3 Supplier shall provide information about Supplier and its Processing of VWGoA Data as reasonably requested by VWGoA for the purpose of assisting VWGoA in complying with its obligations under Applicable Law or contracts, including the exercise of Data Subject Rights (as defined in section 3.5 below) and Security Breach notification obligations as well as investigations.

3.4 Supplier shall immediately notify VWGoA of any requests, inquiries or complaints received about the Processing of Personal Information from third parties, including regulators, authorities, data subjects and law enforcement authorities. Supplier shall not respond to any such requests, inquiries or complaints except on the documented instructions of VWGoA or as required by Applicable Law and in all cases subject to the obligations in Section 3.6.

3.5 If VWGoA responds or allows the response to a request, inquiry or complaint (whether received through Supplier or by VWGoA directly), Supplier shall provide VWGoA with reasonable cooperation and assistance in responding to any such request, inquiry or complaint in a manner that allows VWGoA to meet the legal timelines for response, including requests by data subjects to access, amend, transfer, opt out of Sale or Sharing, delete or exercise other data subject rights around Personal Information (collectively, "Data Subject Rights").

3.6 If disclosure of VWGoA Data is required by Applicable Law or a compulsory legal process, Supplier shall, unless prohibited by Applicable Law or compulsory legal process: (i) notify VWGoA promptly in writing before complying with any such disclosure request in order to provide VWGoA an opportunity to intervene, if appropriate; and (ii) disclose the minimum amount of VWGoA Data necessary to comply with Applicable Law or a compulsory legal process.

4. Sub-processing

4.1 VWGoA on its own behalf grants Supplier a general consent to engage Authorized Persons, including subcontractors, to perform the Services as needed.

4.2 If Supplier uses subcontractors to fulfill its obligations under the Agreement, it will:

- Conduct reasonable due diligence to ensure that the subcontractor is capable of providing the level of protection for the VWGoA Data or Systems as required by the DPSA and Applicable Law;
- Execute a written contract detailing the terms of the sub-processing activities and providing for provisions which offer at least the same level of protection of VWGoA Data or VWGoA Systems as this DPSA and provide a copy to VWGoA;
- Ensure no transfer outside the jurisdiction in which the Personal Information was collected without prior authorization from VWGoA;
- Ensure any subcontractor adheres to the terms of this DPSA as if it were a party to it;
- Keep a list of subcontractor agreements, which shall be updated regularly and made available to VWGoA upon request;
- Ensure that the subcontractor performs the obligations under this DPSA, as if it were a party to the DPSA in place of Supplier, except that Supplier will coordinate communication with VWGoA and is entitled to make and receive communication in relation to this DPSA on behalf of any subcontractors. Supplier shall obtain the necessary authorization from the subcontractors in this regard.
- Ensure that Supplier notifies VWGoA of any subcontractors hired by its subcontractors and that such additional subcontractors are bound by written agreement to the terms of this DPSA, Applicable Law and offer the same level of protection to VWGoA Data or VWGoA Systems as Supplier and its subcontractors.

4.3 Supplier shall give VWGoA prior written notice of the appointment of any subcontractor, including full details of the Processing to be undertaken by the subcontractor, the name and contact details of the subcontractor and the date of the subcontracting agreement. If, within 4 weeks of receipt of that notice,

VWGoA notifies Supplier in writing of any objections (on reasonable grounds) to the proposed appointment, Supplier shall not appoint that proposed subcontractor except with the prior written authorization of VWGoA. Should Supplier choose to retain the objected-to subcontractor, Supplier will notify VWGoA at least fourteen (14) days before appointing the subcontractor and VWGoA may immediately discontinue using the relevant portion of the Service and VWGoA may terminate the relevant portion of the Service within thirty (30) days. Upon termination by VWGoA pursuant to this section, Supplier shall refund VWGoA any prepaid fees for the terminated portions of the Service that were to be provided after the effective date of termination.

4.4 Where subcontractor fails to fulfil its obligations with respect to VWGoA Data or Systems, Supplier shall remain fully liable to VWGoA for that subcontractor.

5. Disclosure of and Access to Personal Information.

5.1 Supplier shall take reasonable steps to ensure the reliability of any Authorized Persons who may have access to VWGoA Data or VWGoA Systems, ensuring in each case that access is strictly limited to those Authorized Persons who need to know / access the relevant VWGoA Data or VWGoA Systems, as strictly necessary for the purposes of the Agreement, and to comply with Applicable Law in the context of that Authorized Persons' duties to VWGoA, ensuring that all such Authorized Persons are subject to confidentiality undertakings or professional or statutory obligations of confidentiality and do not Process VWGoA Data or access VWGoA Systems except on the written instructions of VWGoA and in accordance with the Agreement and this DPSA.

5.3 Supplier shall instruct all Authorized Persons to whom it provides VWGoA Data or allows access to VWGoA Systems to implement appropriate safeguards to protect the VWGoA Data or VWGoA Systems, which provide at least the same degree of protection as the terms of this DPSA, and to immediately report to Supplier any actual or potential Security Breach involving VWGoA Data or VWGoA Systems of which they become aware. Supplier shall be responsible for and remain liable for each Authorized Person's compliance with the terms of this DPSA.

5.4 Supplier shall limit access to VWGoA Data and VWGoA Systems by Authorized Persons to ensure that any given Authorized Person receives only the level of access necessary to perform their job functions to provide the Services to VWGoA.

5.5 Supplier shall provide VWGoA with the name and contact details of the person who is responsible for compliance with this DPSA within Supplier.

5.6 Supplier shall not disclose the VWGoA Data or allow access to VWGoA Systems to any third party beyond Authorized Persons, unless required to do so by law to which the Supplier is subject; in such a case, the Supplier shall inform VWGoA of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest.

6. Return or Destruction of VWGoA Data

6.1 Upon termination or expiration of the Agreement for any reason, or if any part of the VWGoA Data retained by Supplier ceases to be required by Supplier to perform its obligations under the Agreement, Supplier shall, and shall use reasonable means to ensure that all Authorized Persons, as requested by VWGoA, either destroy all VWGoA Data Processed under this Agreement and in its possession or control (including all originals and copies) as soon as practicable, and no later than 30 days after termination or

expiration or it is no longer required or, return all such VWGoA Data to VWGoA in any manner reasonably requested by VWGoA, within 30 days.

6.2 Upon VWGoA' request, Supplier must promptly certify in writing to VWGoA that it has destroyed or returned, as applicable, all VWGoA Data. In the event that Supplier is unable to return or destroy all VWGoA Data, Supplier shall, and shall ensure that each affected Authorized Person, retain VWGoA Data only to the extent and for such period as required by Applicable Law, maintain the security and confidentiality of all such retained VWGoA Data in accordance with the protections of this DPSA, and ensure that such VWGoA Data is only Processed as necessary for the purposes specified in the Applicable Law requiring its storage and for no other purposes.

7. Security Measures.

7.1 Supplier warrants and undertakes to have in place and shall maintain physical, organizational and technical processes and procedures and measures to protect against any unauthorized or unlawful access, Processing, loss, destruction, theft, damage, use, disclosure or other compromise of VWGoA Data or VWGoA Systems (collectively, "Appropriate Safeguards"), including, at a minimum, the technical and organizational security measures set forth as **Annex 1** to this DPSA. Such Appropriate Safeguards shall, in all material respects, be in accordance with good industry practice and not less stringent than the measures Supplier applies to its own equivalent of VWGoA Data or VWGoA Systems of similar kind. These Appropriate Safeguards shall be appropriate to the harm that might result from any risks to VWGoA Data or VWGoA Systems and having regard to the nature of the VWGoA Data or VWGoA System which is to be protected and shall take into consideration the state of the art, the costs of implementation and the nature, scope, context and purpose of the Processing and the risks to the individuals whose Personal Information it Processes on behalf of VWGoA.

7.2 PCI Compliance. To the extent applicable, Supplier agrees to fully comply with the PCI Standards and provide to VWGoA a Report of Compliance completed by a qualified security assessor no less than once annually. For purposes of this section, "PCI Standards" shall mean all applicable standards, guidance, and requirements issued by the PCI-SSC, including but not limited to the Payment Card Industry Data Security Standard ("PCI-DSS"), Payment Application Data Security Standard ("PA-DSS"), Tokenization Product Security Guidelines, and any additional applicable standards, guidelines, or requirements established from time to time by a major payment card network with respect to the security of Account Data. Any reference to a standard, guideline, or requirement document means the operable version of the document, as its issuing organization may amend it from time to time.

8. Security Breach and Response

8.1 Supplier shall promptly notify VWGoA without undue delay and no later than 24 hours upon Supplier becoming aware of an actual or potential Security Breach. Supplier should notify VWGoA by telephone to Supplier's primary business contact and via email at privacy@vw.com if it has knowledge that there is, or reasonably believes that there has been, an actual or potential Security Breach. Notice must include the following:

- the nature of the Security Breach,
- the categories and numbers of data subjects concerned, and the categories and numbers of records concerned;
- the name and contact details of the Supplier contact from whom more information may be obtained;
- describe the likely consequences of the Security Breach; and
- describe the measures taken or proposed to be taken to address the Security Breach.

- Other information as VWGoA may reasonably request

8.2 Supplier shall (i) cooperate with VWGoA in the manner reasonably requested by VWGoA and in accordance with law to investigate and resolve the Security Breach, and mitigate any harmful effects of the Security Breach; (ii) promptly implement any necessary remedial measures to ensure the protection of VWGoA Data or VWGoA Systems; and (iii) properly document responsive actions taken related to any Security Breach, including, without limitation, post-incident review of events and actions taken to make changes in business practices to ensure the protection of VWGoA Data or VWGoA Systems.

8.3 Except as required by Applicable Law or regulation, Supplier agrees that: (i) it shall not inform any third party of any Security Breach without first obtaining VWGoA' prior written consent, other than to inform a complainant that VWGoA shall be/has been informed of the Security Breach; and (ii) VWGoA shall have the right, but not the obligation, to determine whether notice of the Security Breach is to be provided to any individuals, authorities, regulators, law enforcement agencies, consumer reporting agencies, or others and the contents of any such notice.

8.4 If the Security Breach was a result of Supplier's or Authorized Persons' negligence or breach of the requirements of this DPSA, Supplier shall bear all costs associated with (i) any investigations and resolution of the Security Breach, including, but not limited to, internal investigations as well as investigations by regulators or other authorities; (ii) notifications to individuals, authorities, regulators, or others; (iii) defense of any and all claims based on the Security Breach; (iv) any remedial actions required by law, recommended by an authority, regulator, governmental body or agreed to by the Parties; (v) any other costs associated with the Security Breach. For a Security Breach resulting from Supplier's or Authorized Persons' negligence or breach of the requirements of this DPSA that results in a breach defined by Applicable Law, in addition to the above and where available, Supplier agrees to bear the costs associated with i) the provision of two years of credit monitoring by a reputable provider; and (ii) establishing a toll-free number and call center for affected individuals to receive information.

9. Cross-Border Transfer of Personal Information

9.1 Supplier shall not Process Personal Information in a jurisdiction outside of the jurisdiction in which it was collected without the written consent of VWGoA. To the extent that such written consent to the Processing of Personal Information outside of the jurisdiction in which it was collected is provided, Supplier agrees to comply with Applicable Law governing the cross-border transfer of Personal Information. If the activities of the Supplier involve the Processing of Personal Information from the European Economic Area or Switzerland to locations outside of the European Economic Area or Switzerland, Supplier agrees to comply with a legally valid data transfer mechanism, including Supplier's EU-approved Binding Corporate Rules for Processors (and related obligations) or to execute EU Standard Contractual Clauses (SCCs) with VWGoA to ensure compliance with restrictions on cross-border transfers.

9.2 With respect to any Subprocessing conducted under the SCCs, Supplier understands and agrees that it is subject to all the obligations under this DPSA and the SCCs pursuant to Clause 11 of the SCCs and in particular the data subjects can enforce against the Supplier as third-party beneficiaries the clauses in the underlying SCCs as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in Clause 6(1) against the data exporter or the data importer in the cases listed in Clause 11 (2) of the SCCs.

9.3 The Parties agree to amend this DPSA or put in place additional safeguards, to enable them to comply with any international data transfer restrictions pertaining to the Personal Information, in case a data transfer mechanism is no longer deemed adequate.

10. Audit Rights

10.1 Supplier shall make available to VWGoA on request all information necessary to demonstrate compliance with this DPSA, and shall allow for and contribute to audits, including inspections at least once every twelve (12) months, by VWGoA or an auditor mandated by VWGoA in relation to the Processing of the VWGoA Data or access to VWGoA Systems by Supplier.

10.2 VWGoA shall give Supplier reasonable notice of any audit or inspection to be conducted under this section and shall make (and ensure that each of its mandated auditors makes) reasonable endeavors to avoid causing (or, if it cannot avoid, to minimize) any damage, injury or disruption to Supplier's premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection.

10.3 Supplier shall cooperate with and provide reasonable assistance to VWGoA, allowing VWGoA to satisfy its obligations under Applicable Law, taking into account the nature of the Processing and the information available to Supplier (and its Subcontractors). Supplier shall also cooperate with VWGoA and provide any required information to VWGoA in any investigation of VWGoA or Supplier by an authority or governmental or regulatory authority, any internal investigation by VWGoA or any legal proceedings regarding the Processing of Personal Information. Supplier will inform VWGoA immediately of any inspections, proceedings or measures conducted by a governmental or regulatory authority, court or tribunal and coordinate with VWGoA before responding to the extent legally permitted.

11. Remedies for Failure to Comply with DPSA

In the event that Supplier materially breaches this DPSA or fails to comply with Applicable Law, VWGoA shall have the right to terminate the Agreement immediately, or stop Supplier Processing and demand remediation of any unauthorized use of Personal Information.

12. Severance

Should any provision of this DPSA be invalid or unenforceable, then the remainder of this DPSA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

By signing this DPSA, Supplier certifies that it understands the restrictions set forth in this DPSA and will comply with them.

VWGoA Corporation Supplier:

By:_____ By:_____

Date: _____ Date: _____

ANNEX 1: TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

Security Measures

Supplier shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk and to protect VWGoA Data or VWGoA Systems against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access.

At a minimum, Supplier has implemented and shall maintain the following security measures.

Business Continuity, Enterprise Resilience, and Disaster Recovery

1. Business Impact Analysis:

   a) Critical IT systems and components must be identified and documented, including recovery time objective and recovery point objective.

2. Recovery Strategies

   a) Mission critical information must be fully backed-up on a weekly basis and incrementally changes must be backed up daily.

   b) Backed-up information must be stored encrypted with FIPS 140-2 compliant encryption protocols.

   c) Backed-up information must be stored in a secure off-site facility.

   d) Backed-up information must be immutable.

   e) Restoration of critical data back-ups must be successfully tested no less than annually.

3. Recovery Plans and Procedures, and Maintenance

   a) A documented business continuity and disaster recovery plans for business functions and supporting technology must be updated and maintained.

   b) The business continuity and disaster recovery plans must be available in the event of disaster.

   c) VWGoA must be alerted of any deficiencies discovered in the business continuity or disaster recovery plan that would adversely affect VWGoA.

4. Testing and Exercising

a) The business continuity and disaster recovery plans for business functions and supporting technologies must be tested annually.

5. Escalation and Crisis Management

a) The business continuity plan must contain notification procedures to alert VWGoA of service disruptions including off-hour and weekend coverage.

b) The disaster recovery plan must have notification procedures to alert VWGoA of service disruptions including off-hour and weekend coverage.

IT Risk and Compliance Management

1. Regulatory and Standards Implementation

a) An information security officer must be assigned.

b) An on-going and documented security awareness program must be established and communicated to all Authorized Persons to make them aware of the confidentiality of information, the Supplier's security policies, standards, and good security practices.

c) Information Security awareness information must be distributed to all Authorized Persons on a periodic basis.

d) An on-going and documented privacy awareness program must be established and communicated to all Authorized Persons to make them aware of the Supplier's privacy policies and the requirements to protect the confidentiality of information.

e) Privacy awareness information must be distributed to all Authorized Persons on a periodic basis.

f) Mandatory privacy training must be delivered to, managed, and validated for all Authorized Persons on no less than an annual periodic basis.

g) All Authorized Persons are required to sign confidentiality and non-disclosure agreements.

2. Risk and Compliance Assessments

a) An accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of Personal Information is conducted at least annually.

b) All Authorized Persons are required to have a background check.

3. Policies, Standards, and Procedure Management

a) A documented risk management function and/or program supported by executive management must exist.

b) A documented information security function and/or program supported by executive management must exist.

c) A documented privacy function and/or program supported by executive management must exist.

d) The information security function/program must establish security policies and standards that are enforced through automated systems and administrative procedures that are maintained and updated as needed.

e) The privacy function/program must establish confidentiality policies which are maintained and updated as needed.

4. Issue and Corrective Action Management

a) Controls must be implemented to reduce risks and vulnerabilities to a reasonable and appropriate level.

5. Exception Management

a) Disciplinary measures for violations must be included in the Information Security and Privacy Program.

b) A documented security incident response plan must exist to ensure incidents are tracked, monitored, and investigated until closure is achieved.

c) A documented privacy incident response plan must exist to ensure that incidents are tracked, monitored, investigated and reported internally and to VWGoA until remediation and closure is achieved.

Data Protection

1. Data Classification & Inventory

a) A documented information classification scheme must be utilized to ensure proper protection, use and destruction of Supplier's data.

2. Data Lifecycle Analysis

a) Systems containing Personal Information must be documented, including security and privacy controls.

b) Documents showing the flow of Personal Information through systems and business processes must exist.

3. Data Encryption & Obfuscation

a) Personal Information must be encrypted during storage on all devices including handhelds, laptops, workstations, and removable media with FIPS 140-2 compliant encryption protocols.

b) Personal Information must be encrypted during storage on servers with FIPS 140-2 compliant encryption protocols.

c) Personal Information must be encrypted during transmission with FIPS 140-2 compliant encryption protocols.

d) Business to business communications with Personal Information must be encrypted.

4. Data Loss Prevention

a) A documented policy and process must exist with regard to the removal or movement of Personal Information to unsecured systems or media.

b) Personal Information, stored on removable media must be secured with restricted access to those with a business need.

c) Technical controls must exist to prevent transmission of Personal Information to unauthorized recipients.

d) Technical controls must exist to prevent storage of Personal Information on unsecured systems.

5. Data Retention and Destruction

a) A documented policy and process must exist with regard to the removal or destruction of Personal Information. When appropriate, Personal Information, must be purged or destroyed using a NIST 800-88 approved process when no longer needed.

Identity & Access Management

1. Authorized Persons Account Management

a) Access to systems and applications must require a unique identifier (e.g. user ID) and multi factor authentication (NIST 800-63B AAL2).

b) Authorized Persons IDs must be locked after 5 consecutive unsuccessful login attempts.

c) Authorized Persons IDs must be disabled after 60 days or less of inactivity.

d) Passwords must be issued to Authorized Persons in a secure manner and be changed at first login.

e) Password policies must meet or exceed NIST 800-63B Appendix A.

f) Passwords cannot be displayed on screens or on reports.

g) Passwords must be encrypted in transmission and storage.

2. Access Management

a) Access to Personal Information must be restricted to individuals that have a business need and access control mechanisms must be implemented that limit access to Personal Information.

b) Security administration procedures must include procedures for access requests for a new Authorized Person, changing access, prompt deletion of Authorized Persons involving terminations, user transfers and periodic verification of Authorized Persons and access rights.

c) All Authorized Persons access requests must be documented with management approval including privileged Authorized Persons.

d) Documented remote access policies must exist and be enforced.

e) Shared or System IDs must be documented describing their functions and risks.

f) Shared or System IDs must be required to have passwords that meet or exceed NIST 800-63B Appendix A.

g) Shared or System IDs must not be able to be accessed by an individual user for interactive use.

3. Data Platform Integration

a) All systems containing Personal Information have system access controls to prevent unauthorized disclosure or modification.

b) Single sign on technologies are leveraged wherever possible to eliminate the need for multiple access controls systems.

4. Access Reporting and Audit

a) All Authorized Persons access to systems containing VWGoA Data must be revalidated at least annually.

b) All Authorized Persons IDs and System IDs with privileged authorities must be revalidated at least quarterly.

5. Access Governance

a) Authorized Persons access must be defined by job roles to ensure segregation of duties.

b) Authorized Persons access must be logged and tracked to an individual for accountability.

6. Federation

a) Access to systems by agents, Subprocessors, or outsourced services are subject to the same Identity Management requirements as VWGoA personnel.

Secure Development Lifecycle

1. Security and Risk Requirements

a) A documented process exists to conduct an accurate and thorough assessment and mitigation of potential risks and vulnerabilities as part of the System Development Life Cycle.

b) Security controls are considered and implemented throughout the System Development Life Cycle.

c) Production and non-production environments must be separated.

d) Non-production environments must not contain production data.

2. Application Role Design and Access Privileges

a) Application access privileges must follow the least privilege concept.

b) Access is controlled by a common access methodology.

c) Application role design must account for separation of duties.

3. Secure Coding Guidelines

a) Secure coding principles and practices are documented and followed.

4. Secure Build

a) Information technology systems deployment procedures must ensure implementation of security configuration settings.

b) All security controls must be tested prior to implementing new systems or upgrades into production.

Infrastructure, Operations and Network Security/Cyber Threat and Vulnerability Management

1. Antivirus (AV) & Malware protection

   a) A documented policy and procedures exist for guarding against, detecting, and reporting malicious software.

2. Intrusion Detection and Prevention

   a) Intrusion detection and prevention systems must be implemented for critical components of the network and systems containing or processing Personal Information.

3. Network Access Controls

   a) A documented policy and procedures exist to prevent unauthorized/unsecured devices from accessing the network.

4. Network and Application Firewalls

   a) Firewalls must be implemented and configured to deny all access except authorized documented business services.

5. Data Loss Prevention

   a) A documented policy and procedures exist to prevent Personal Information from being transmitted to unauthorized recipients or stored in unauthorized locations.

6. Remote Access Controls

   a) Multi factor authentication (NIST 800-63B AAL2) must be implemented for all remote network access (e.g. VPN, Citrix, etc.).

7. Security Monitoring and Logging

   a) A documented policy and procedures exist to monitor networks, systems, and applications for potential security events.

   b) A documented process exists to respond to potential security events on a 24x7x365 basis.

   c) Security relevant events must be securely logged and tamper proof.

   d) All events must be traceable to specific individuals or systems.

   e) Logs must be implemented on all systems storing or processing critical or Personal Information.

   f) Logs must be retained for a minimum of twelve (12) months.

   g) Logs must be reviewed for inappropriate activities in a timely manner and appropriate actions must be taken.

Cyber Threat and Vulnerability Management

1. OS Hardening & Secure Configuration

a) Required security configuration settings must be selected and documented.

b) Documented processes must exist to periodically verify security configuration settings.

c) Any and all information systems able to access or process any Personal Information must actively and automatically blank the screen or enable a screen saver and require re-authentication after fifteen (15) minutes of inactivity or less.

2. Patch Management

a) A documented patch management process must exist and be enforced.

b) Prompt application of security patches, service packs, & hot fixes is required for all systems that store, process, manage, or control access to Personal Information.

3. Vulnerability Management and Security Assessments

a) A documented process and procedures exist to identify, quantify, prioritize, track, and remediate vulnerabilities.

a) Periodic third party assessments must be conducted from outside and within the network at least annually.

b) Vulnerability assessment must be performed at least quarterly.

4. Incident and Problem Management

a) A documented problem management system must exist.

5. Capacity Management

a) A documented policy and process exists to evaluate current capacity against projected requirements.

6. Change and Release Management

a) A documented policy and process must exist for change management.

b) A documented policy and process must exist for release management.

c) All systems and application resources must be changed through an enforced and documented change management process which includes appropriate reviews, testing, and management approvals.

7. Asset and Configuration Management

a) An auditable and documented inventory of information technology assets and architectures must exist.

Physical Security

1. Policies, Standards, and Procedure Management

a) A documented physical security function and/or program must exist.

b) The physical security function/program must establish physical security policies and be enforced through automated systems and administrative procedures.

c) All servers storing or processing Personal Information must be located in a secure data center or equivalent secure facility.

2. Facility Access Controls

a) Employees must be required to wear identification badges at all times in sensitive facilities.

b) Visitors must be required to be identified, sign in, wear temporary visitor badges, and be escorted.

c) Data center access to sensitive areas, such as a computer room, must require two levels of authentication.

d) Data center and other sensitive facilities access must be periodically reviewed to ensure that access is still valid.

e) Facility access logs must be retained for at least twelve (12) months and be reviewed as needed.

3. Issue and Corrective Action Management

a) Any known HIGH risk physical security vulnerabilities affecting VWGoA or Personal Information must be communicated to privacy@vw.com.

b) The Data Center facility must be equipped and maintained with fire detection/suppression, surge and brown-out, air conditioning, and other computing environment protection systems necessary to assure continued service for critical systems.

c) Policies and procedures must be in place to document repairs and modifications to physical components of facilities where Personal Information is stored, which are related to security (for example, hardware, walls, doors and locks).

d) All hardware and electronic media containing Personal Information must be identified and tracked during movement.

Changes

VWGoA may change the above security requirements by providing new requirements in writing to Supplier. Supplier shall comply with such new security requirements within thirty (30) days after receipt of notice. In the event Supplier's compliance with the new requirements materially increases Supplier's cost to provide services under the Service Agreement, Supplier shall notify VWGoA of the amount Supplier believes is necessary to reimburse Supplier for its actual and reasonable additional costs and the Parties will negotiate in good faith to determine if reimbursement to Supplier for such increased costs are warranted. If the Parties cannot reach agreement, either Party may terminate the Agreement by providing thirty (30) days' written notice to the other.