MASTER TERMS DIRECT PURCHASING

Mercedes-Benz Vans, LLC

INFORMATION SECURITY REQUIREMENTS

Revision History

Revision Level	Change Date
1.0	9/14/2018

IMPORTANT: *Check with MBV for any late-breaking changes to these directives.*

Information Security Requirements

These Information Security Requirements (the "Requirements") supplement the Master Terms Direct Purchasing (the "Agreement") to which it is attached. All capitalized terms used herein shall have the meanings ascribed to them in these Requirements, or, if not so ascribed, as set forth in the Agreement.

1. Definitions.

1.1 **Industry Standards** means those standards applicable to the Supplier or Buyer, and the automotive industry.

1.2 **Buyer Data** means all data provided to Supplier, and may include, without limitation, the following: compilations of individual records submitted by Buyer to Supplier (e.g. names, addresses, phone numbers, email addresses, transaction histories, transactional information, product-level data, transaction channels, consumer marketing preference data, and lead generation sources), Buyer Proprietary Information, Buyer Intellectual Property, designs/drawings, technical specifications, and other appropriate data. Without limiting the foregoing, Buyer Data shall be deemed to include all information that: (i) identifies or can be used to identify an individual (including, without limitation, names, signatures, addresses, telephone numbers, e-mail addresses, vehicle identification number and other unique identifiers); or (ii) can be used to authenticate an individual (including, without limitation, employee identification numbers, government-issued identification numbers (including social security number, driver's license number or state-issued identified number), passwords or PINs, financial account number, credit card number, debit card number, credit report information, with or without any required security code, access code, personal identification number or password, that would permit access to an individual's financial account, credit report information, biometric or health data, answers to security questions and other personal identifiers). Buyer's business contact information is not by itself deemed to be Confidential Information.

1.3 **Buyer Systems** means any computer, computer network, computer application, imaging device, storage device, mobile computing device or software owned, licensed or leased by Buyer, or operated by a third party on behalf of Buyer, which: (a) connects to or otherwise interacts with Supplier Systems; or (b) is enabled or intended to access or interact with Buyer Data created, stored, processed or transmitted in connection with the Agreement.

1.4 **Privacy and Security Laws** means all international, local country-specific, European, and US State and Federal laws, standards, guidelines, policies, regulations, and procedures, as amended, applicable to Supplier or Buyer pertaining to the security, confidentiality or privacy of the Buyer Data, including, without limitation, the Gramm-Leach Bliley Act of 1999 (Public Law 106-102, 113 Stat. 1338) and its implementing regulations, the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations, and the General Data Protection Regulation (2016/679).

1.5 **Security** means Supplier's technological, physical, administrative, and procedural safeguards, including, without limitation, policies, procedures, guidelines, practices, standards, controls, hardware, software, firmware, and physical security measures, the function or purpose of which is, in whole or part: (a) to protect the confidentiality, integrity or availability of Buyer Data and Supplier Systems; (b) to prevent the unauthorized use of or unauthorized access to Supplier Systems; and/or (c) to prevent a breach or malicious infection of Buyer Systems.

1.6 **Security Breach** means any actual or reasonably suspected: (a) unauthorized use of, or unauthorized access to Supplier Systems; (b) inability to access Buyer Data or Supplier Systems due to a malicious use, attack or exploit of such Buyer Data or Supplier Systems; (c) unauthorized access to, theft of or loss of Buyer Data; (d) unauthorized use of Buyer Data for purposes of actual or reasonably suspected theft, fraud or identity theft; (e) unauthorized disclosure of Buyer Data; (f) breach of, transmission of or infiltration of malicious code into, Buyer Systems arising from, in whole or part, an act, error, or omission by Supplier; of (g) receipt of a complaint in relation to the privacy practices of Supplier or a breach or alleged breach of this Agreement relating to such privacy practices.

1.7 **Supplier Systems** means any computer, computer network, computer application, imaging device, storage device, mobile computing device or software owned, leased or controlled by Supplier or operated by a third party on behalf of Supplier that uses, stores, accesses, processes or transmits Buyer Data or is connected to any computer, computer network, computer application, storage device, mobile computing device or software owned, licensed or leased by Buyer.

2. Information Security.

2.1 Supplier is responsible for the security of Supplier's systems and data and any Buyer Data. Supplier shall, consistent with Industry Standards and its Security obligations under these Requirements, (i) collect and record information and (ii) maintain logs, planning documents, audit trails, records and reports concerning (a) its Security, (b) its compliance with these Requirements, Privacy and Security Laws and Security Breaches, (c) its storage, processing and transmission of Buyer Data and (d) the accessing and use of Supplier Systems.

2.2 Supplier shall implement administrative, physical, and technical safeguards to protect Buyer Data that are no less rigorous than accepted industry practices, specifically, the International Organization for Standardization's standards: ISO/IEC 27001:2013 – Information Technology–Security Techniques–Information Security Management Systems–Requirements and ISO/IEC 27002:2013–Information Technology–Security Techniques–Code of Practice for Informational Security Controls, and other applicable industry standards for information security, and shall ensure that all such safeguards, including the manner in which Buyer Data is collected, accessed, used, stored, processed, disposed of, and disclosed, comply with applicable Privacy and Security Laws, the Alabama Data Breach Notification Act, and the terms and conditions of these Requirements. In the event of any conflict between (i) Supplier's obligation to employ and maintain reasonable, appropriate and adequate Security set forth herein, (ii) Supplier's obligation to meet Industry Standards for Security set forth herein, and (iii) Supplier's obligation to align with the ISO 27002 security standard or any other security-related obligation in this Agreement (including these Requirements), Supplier shall comply with the obligation that provides the most protective and rigorous Security.

2.3 At a minimum, Supplier's safeguards for the protection of Buyer Data shall include: (i) limiting access of Confidential Information to authorized employees (ii) securing business facilities, data centers, paper files, servers, back-up systems and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability; (iii) implementing network, device application, database and platform security; (iv) securing information transmission, storage and disposal; (v) implementing authentication and access controls within media, applications, operating systems and equipment; (vi) encrypting Confidential Information stored on any mobile device or media; (vii) encrypting Confidential Information that will be transmitted; (viii) strictly segregating Confidential Information from information of Supplier or its other customers so that Confidential Information is not commingled with any other types of information; (ix) implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law; and (x) providing appropriate privacy and information security training to Supplier's employees.

2.4 If, in the course of its engagement, Supplier has access to or will collect, access, use, store, process, dispose of or disclose credit, debit or other payment cardholder information, Supplier shall at all times remain in compliance with the Payment Card Industry Data Security Standard ("PCI DSS") requirements, including remaining aware at all times of changes to the PCI DSS and promptly implementing all procedures and practices as may be necessary to remain in compliance with the PCI DSS, in each case, at Supplier's sole cost and expense.

2.5 Supplier shall impose controls on (i) access to and viewing of Buyer Data, (ii) the copying of Buyer Data and (iii) the printing or other duplication of Buyer Data, and (iv) the distribution of Buyer Data.

2.6 Upon completion of contractual requirements or termination of the Agreement, Supplier shall return to Buyer all the information, data, documents and storage media which it has received and any copies thereof in a commercially standard format reasonably accessible to Buyer, including any passwords, encryption keys, or other credentials necessary to access the same. Supplier shall provide evidence and

confirm in writing that all the information, data, documents and storage media and any copies thereof have been returned, and once Buyer has confirmed it has successfully accessed the information, deleted using methods reasonably contemplated to prevent the recovery or recreation of the data. Buyer may decide on an earlier date for data deletion at any time. Supplier shall return Buyer data to authorized Buyer personnel as specified by Buyer.

2.7 **Security Coordinator.** Supplier shall assign an individual working for Supplier that shall act as its Security Coordinator, who will be the security liaison between Buyer and Supplier and (i) oversee compliance with these Requirements, (ii) receive notice of Security Breaches within the Supplier's organization, (iii) coordinate Security Breach incident response and remedial action, and (iv) provide notice, reporting and work within Supplier to undertake other actions and duties as set forth in these Requirements. The Supplier shall ensure that such individual is sufficiently trained, qualified and experienced to be able to fulfill the functions set out in this Section 2.7 and any other functions that might reasonably be expected to be carried out by the individual as a security coordinator.

2.8 **Additional Controls.** During the Term of the Agreement, Supplier shall implement and maintain additional Security, as mutually agreed upon by Supplier and Buyer, in the event of: (i) any material changes to Services; (ii) any Security Breach; or (iii) any material decreases to Supplier's Security; provided, that the failure of Buyer to make a request of Supplier shall not impact, eliminate or decrease Supplier's obligations under these Requirements.

3. Security Breach Procedures.

3.1 Supplier shall use best efforts to immediately remedy any Security Breach and prevent any further Security Breach at Supplier's expense in accordance with applicable privacy rights, laws, regulations and standards. Supplier shall reimburse Buyer for reasonable costs incurred by Buyer in responding to, and mitigating damages caused by, any Security Breach, including all costs of investigation, notice and/or remediation.

3.2 Supplier agrees that it shall not inform any third party of any Security Breach without first obtaining Buyer's prior written consent, other than to inform a complainant that the matter has been forwarded to Buyer's legal counsel. Further, Supplier agrees that Buyer shall have the sole right to determine: (i) whether notice of the Security Breach is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies or others as required by law or regulation, or otherwise in Buyer's discretion; and (ii) the contents of such notice, whether any type of remediation may be offered to affected persons, and the nature and extent of any such remediation.

3.3 Supplier shall notify Buyer as soon as practicable, but no later than four hours after Supplier or a service provider becomes aware of a Security Breach. Supplier shall investigate the Security Breach. Supplier agrees to fully cooperate with Buyer in Buyer's handling of the matter, including, without limitation: (i) assisting with any investigation; (ii) providing Buyer with physical access to the facilities and operations affected; (iii) facilitating interviews with Supplier's employees and others involved in the matter; and (iv) making available all relevant records, logs, files, data reporting and other materials required to comply with applicable law, regulation, industry standards or as otherwise required by Buyer.

4. Breach of Requirements.

4.1 The following shall be considered a breach or default of the Agreement: (a) a Security Breach; and/or (b) Supplier's failure to comply with the obligations set forth in these Requirements. In the event of such a breach, Buyer, in its sole and absolute discretion, may immediately (or on a timeline specified by Buyer) terminate the Agreement in accordance with its terms without any further obligations or penalties.

4.2 Any Security Breach and/or Supplier's failure to comply with the obligations set forth in these Requirements are not subject to the limitations or exclusions of liability set forth in the Agreement.

4.3 **Use of Third Parties.** Supplier shall not provide any subcontractor with access to Buyer Data, unless (i) it has received prior written consent from Buyer or (ii) such access is specifically allowed under the Agreement or applicable mutually signed SOW. Except as allowed per the foregoing sentence, Supplier shall not provide any third party (other than Supplier's regulators) with access to Supplier's systems or

network that would allow the third party to have access to Buyer Data. Prior to providing any subcontractor with access to Buyer's Data, Supplier shall: (a) conduct a reasonable investigation of such party's information security measures to determine that such security is reasonable and consistent with Supplier's obligations under these Requirements; and (b) ensure that such party is obligated by law or contract to protect Buyer Data and cooperate with Buyer in the event of an incident or Security Breach consistent with these Requirements. In all events, Supplier is and shall remain fully responsible for any act, errors or omission of any subcontractor retained by Supplier with respect to compliance with these Requirements.

5. Audit Compliance and Client's Right to Audit Supplier Operations.

5.1 Supplier must, at the Supplier's expense, make available to Buyer a copy of Supplier's most recent SOC-2 Type 2 Report on Controls Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy.

5.2 Supplier shall make available documentation to support Supplier's external audits upon Buyer's request.

5.3 Supplier must permit Buyer to audit its privacy and security controls periodically (no less than annually) and must cooperate with Buyer in the audit. Supplier must provide Buyer with copies of relevant privacy and security policy, process, and procedure documents for review and audit purposes. Buyer may elect to recommend reasonable changes that Supplier must, within a reasonable time period, either (1) use to amend its policies, processes, and procedures; or (2) respond with mitigating controls.

6. Representations and Warranties.

Supplier represents and warrants that:

6.1 It routinely uses industry standard processes to check its systems and software ("IT Service") for malicious code, including, without limitation, viruses, Trojan horses, worms, and any other software routines or code designed to (i) permit unauthorized access by third parties, or (ii) disable, erase, or otherwise harm the IT Service, data, other software or hardware (collectively, "Malicious Code") and that the IT Service, when accessed by Buyer or users, will contain no Malicious Code.

6.2 It routinely, but no less than once a year, has a third party conduct penetration testing and perform vulnerability scans.

6.3 Each of Supplier's employees, consultants, contractors, partners or agents who have been or will be involved in the provision of Services under the Agreement have signed or will sign an agreement with Supplier agreeing not to use or disclose any Confidential Information other than as required for Supplier's performance of its obligations under this Agreement

6.4 Its collection, access, use, storage, disposal and disclosure of Nonpublic Personal Information does and will comply with all applicable federal and, state, and foreign privacy and data protection laws, as well as all other applicable regulations and directives, including, but not limited to the GDPR, GLB, PCI, and the Alabama Data Breach Notification Act.

6.5 It has conducted a criminal background investigation on each employee who will be involved in the provision of Services under the Agreement and further warrants that each of said employees has not been convicted of any felony or a misdemeanor involving crimes of violence, fraud, misappropriation, or other breach of trust.

7. Insurance Coverage. In addition to any insurance requirements specified in the Agreement, Supplier shall also maintain Privacy and Network Security (otherwise known as Cyber Liability) coverage which includes providing protection against liability for (a) system attacks, (b) denial or loss of service attacks, (c) spread of malicious software code, (d) unauthorized access and use of computer systems, (e) social engineering attacks, (f) crisis management and customer notification expenses, (g) privacy regulatory defense and penalties and (h) liability arising from the loss or disclosure of confidential data with coverage limits of not less than $5,000,000 per occurrence.