RIVIAN THIRD PARTY DATA PROTECTION REQUIREMENTS FOR CONFIDENTIAL/PROPRIETARY DATA

Rivian has developed these Third Party Data Protection Requirements ("**Requirements**") in accordance with its third party risk management framework to enable Rivian's vendors, suppliers, service providers and other third parties (collectively, "**Third Parties**") to meet Rivian's standards for maintaining the confidentiality, integrity and availability of Rivian's information. These Requirements apply to Third Parties who will handle confidential and/or proprietary information on behalf of Rivian and who are not expected to handle Rivian personal data as part of their services. A Third Party agrees to these Requirements by entering into a contractual relationship with Rivian, providing goods or services to Rivian, and/or by receiving any information from Rivian in the course of providing goods or services to Rivian. Third Party will immediately inform Rivian if it is unable to comply with these Requirements at any time. Third Party agrees that these Requirements may be amended from time to time, as technologies evolve. Rivian will make reasonable efforts to notify Third Party of any changes to these Requirements. Exceptions to these Requirements may only be granted by Rivian's Chief Information Security Officer or their delegate.

THIRD PARTY DATA PROTECTION RESPONSIBILITIES:

1. **Information Security Program:** Third Party will maintain a written information security program (the "**Program**") that documents Third Party's policies, standards, and controls relating to these Requirements. The Program must include industry standard organizational administrative, technical, and physical safeguards appropriate to Third Party's size and complexity, the scope of Third Party's activities for Rivian, and the sensitivity of Rivian's information being shared with the Third Party. Third Party will make available to Rivian the policies, standards, and control documentation based on reasonable requests from Rivian.

2. **Information Security Function:** Third Party must maintain an information security role responsible for promoting company-wide information security. Third Party will provide Rivian with the name, job title, and business contact information of such individual and promptly notify Rivian of any personnel changes with regard to its information security function.
3. **Awareness & Training:** Third Party will undertake regular Program awareness and education efforts to ensure all Third Party personnel are aware of, and able to comply with, these Requirements.

4. **Personnel Obligations:** Third Party will ensure that all Third Party personnel who will process or otherwise have access to Rivian's information have been appropriately informed of these Requirements before accessing any of Rivian's information. Third Party will further ensure that all such Third Party personnel are subject to contractual obligations of confidentiality consistent with these Requirements.

5. **Network Segmentation:** To the extent applicable to Third Party's services, Third Party will install and maintain appropriate network and/or data segmentation to protect data accessible via the Internet and Third Party will keep all Rivian information protected by **appropriate control points** at all times.

6. **Updates:** Third Party will keep its systems and software up-to-date with the latest upgrades, updates, bug fixes, new versions and other modifications necessary to ensure security of Rivian's information.

7. **Enterprise Vulnerability Management:** Third Party will implement and maintain a vulnerability management program to discover and eliminate vulnerabilities in Vendor systems that could be exploited by malware or other technical methods, including but not limited to (i) vulnerability identification and remediation; (ii) software and firmware patching; and (iii) hardware maintenance.

8. **Malware and Ransomware:** Third Party will, at all times, use and keep up-to-date anti-malware software. Third Party will mitigate threats from all viruses, spyware, and other malicious code that are or should reasonably have been detected.

9. **Secure Storage and Transmission:** Third Party will encrypt Rivian's information at rest and when sent across open networks in accordance with industry best practices.

10. **Third Party System Monitoring:** Third Party will implement monitoring tools that identify and log malicious, unauthorized, or otherwise abnormal activity (e.g., account activity, invalid access attempts, creation and deletion of accounts, initiation and pausing of audit logging) within Third Party's network and systems. Third Party shall regularly review logs to proactively identify anomalies or suspicious activity.

11. **Access to Rivian's Network or Systems:** If Third Party will have access to Rivian's network or systems, or integrate its own network or systems with those of Rivian, Third Party agrees that: (i) any wireless access must be authorized, authenticated, encrypted and permitted only from approved locations (and such locations shall maintain system firewalls in accordance with Section 5 above and anti-malware software in accordance with Section 8 above); (ii) remote access from unapproved locations must be through a virtual private network; (iii) Third Party will not share any credentials with any third parties; (iv) Third Party will require industry standard multi-factor authentication for any accounts or systems used by employees in accessing Rivian's Network or Systems; (v) Third Party will maintain a secure logical and physical environment when connecting to Rivian's network or systems; (vi) Third Party will regularly review access rights and, within twenty-four (24) hours of determining that an individual no longer needs access to Rivian's network or systems, revoke such access; (vii) Third Party will provide to Rivian, on an annual basis, or more frequently upon Rivian's request, (a) log data about all use of Rivian's accounts or credentials provided to Third Party for use on behalf of Rivian, and (b) detailed log data about any impersonation of, or attempt to impersonate, Rivian personnel or Third Party personnel with access to Rivian's information; (viii) Third Party will not download, mirror or permanently store any of Rivian's information on any medium, including any machines, devices, or servers; (ix) Third Party will terminate the account of each of Third Party's personnel within the earlier of 24 hours after such personnel no longer needs access to Rivian's information or leaves Third Party's

employ; and (x) Rivian reserves the right to implement security software to monitor Third Party's compliance with these Requirements.

12. **Software:** If Third Party provides software or develops code on behalf of Rivian, or provides any type of cloud-based services to Rivian, Third Party will maintain an industry standard Secure Development Lifecycle program ("**SDLC**") aligned with the principles of Secure by Design and Secure by Default, which includes, but is not limited to: (i) static code analysis, (ii) testing against the most current OWASP Top 10, and (iii) testing systems hardware for CWE Top 25. Furthermore, Third Party will provide patching and vulnerability management during the term of the agreement between the parties. Software updates provided by Third Party must be implementable using typical patch management or automation systems. Third Party will notify Rivian within twenty-four (24) hours of the discovery of a critical security vulnerability within the software or code, and within seventy-two (72) hours of the discovery of a high vulnerability, and in all cases, will remediate vulnerabilities as soon as practicable.

13. **Access Controls:** Third Party will secure Rivian's information, including by complying with the following requirements: (i) Third Party will assign a unique identification to each person with computer access to Rivian's information; (ii) Third Party recognizes that Rivian utilizes industry standard multi-factor authentication mechanisms and agrees to follow this standard; (iii) Third Party will restrict access to Rivian's information to only those people with a "need to know" for a purpose permitted under the agreement with Rivian; (iv) Third Party will regularly (at least once every 90 days) review the list of people and services with access to Rivian's information and remove accounts that no longer require access; (v) except where expressly authorized by Rivian in writing, Third Party will isolate Rivian's information at all times (including in storage, processing, or transmission), from Third Party's and any third party's information; and (vi) Third Party will regularly review access logs for signs of malicious behavior or unauthorized access.

14. **Passwords and Login Attempts:** Third Party shall enforce replacement of default passwords with unique passwords that (i) contain a minimum of eight (8) characters; and (ii) do not match previous passwords, the user's username, or the user's common name. Third Party shall disable accounts after ten (10) consecutive invalid login attempts. Passwords must be changed whenever an account compromise is suspected and must be regularly replaced after no more than ninety (90) days. In lieu of the aforementioned standards, Third Party may implement industry-standard multi-factor authentication.

15. **Physical Security:** Third Party must secure facilities where Rivian's information is stored, processed or transmitted from. Entrances must be secured and monitored (for example, by security guard, badge reader, electronic lock, or CCTV). Physical access must be restricted to those with a business need and facility access logs must be maintained.

16. **Business Continuity & Disaster Recovery:** Third Party must have a viable business continuity and disaster recovery plan that addresses all reasonably-foreseeable risks to Rivian's information. For example, Third Party's applications, systems, and networks must be run on robust, reliable hardware and software, and supported by alternative hardware or duplicate facilities. Third Party must ensure that backups of software and Rivian's information are performed on a regular basis, according to a defined cycle discussed with

and approved by Rivian. If Third Party performs a "recovery" for the purpose of disaster recovery, Third Party will have and maintain a process that ensures that all of Rivian's information that is required to be deleted pursuant to these standards will be redeleted or overwritten from the recovered data in accordance with this Section 16 within twenty-four (24) hours after recovery occurs. Rivian's information shall not be recovered to a less secure environment than the previous production environment without Rivian's prior written approval. Rivian reserves the right to require a security review of the third-party system before permitting recovery of any of Rivian's information to any third-party system.

17. **Information Management, Retention & Destruction:** The Program shall include controls designed to ensure that: (i) Third Party will manage essential information about hardware, software, and data flows/extracts/interfaces (e.g., unique identifiers, version numbers, data recipients, physical locations) with regard to devices, networks and systems that will be used to store, access, or otherwise process Rivian's information; (ii) Rivian's information is kept by Third Party no longer than necessary for the provision of Third Party's services to Rivian, or, for such longer period as required by applicable law; and (iii) Rivian's information is securely disposed of, in accordance with industry best practices. Third Party will permanently and securely delete all live (online or network accessible) instances of Rivian's information within 90 days after the earlier completion of Third Party's services for Rivian or the expiration of Third Party's agreement with Rivian. If Third Party is required by law to retain archival copies of Rivian's information, they must be stored in one of the following ways: (a) as a "cold" or offline backup stored in a physically secure facility; or (b) encrypted, where the system hosting or storing the encrypted files does not have access to a copy of the keys used for encryption. Third Party will, upon Rivian's request, provide Rivian with a certificate of destruction certifying Third Party's secure deletion of Rivian's information. All of Rivian's information will be deleted in accordance with the NIST special publication 800-88 Revision 1, Guidelines for Media Sanitation December 18, 2014, or through degaussing of magnetic media in an electromagnetic flux field of 5000+ GER, or by shredding or mechanical disintegration, or such other standards Rivian may require based on the classification and sensitivity of Rivian's information. With regard to encrypted information, this deletion may be done by permanently and securely deleting all copies of the keys used for encryption. Before disposing of any hardware, software, or any other media that contains, or has at any time contained, Rivian's information, Third Party will perform a complete forensic destruction of the hardware, software, or other media so that none of Rivian's information can be recovered or retrieved in any form. Third Party will not sell, resell, donate, or otherwise transfer any hardware, software, or other media that contains Rivian's information that has not first been forensically destroyed. Third Party must prevent Rivian's information from being used for training any machine learning or artificial intelligence systems.

18. **Use of Third-Party Systems:** To the extent Third Party uses subcontractors or other third-party vendors in performance of its obligations to Rivian, Third Party will inform such third parties of their obligations to Rivian under these Requirements. Use of a subcontractor does not relieve Third Party from the responsibility of compliance with these Requirements. Third Party will obtain Rivian's prior written approval before it uses any third-party system that stores or may otherwise access Rivian's information unless (a) Rivian's information is encrypted in accordance with Section 9 above, and (b) the third-party system will not have

access to the decryption key or unencrypted "plain text" versions of Rivian's information. If Third Party uses any third-party system that stores or otherwise accesses Rivian's unencrypted information, Third Party will perform a security review of the third-party system and will provide Rivian with periodic reporting about the third-party system's security controls in the format requested by Rivian. Third Party shall require that its internal and third party software developers remain current on application security and secure coding industry best practices.

19. **Incident Response & Reporting:** Third Party will maintain and regularly test a documented Incident Response Plan ("IRP"). The IRP will describe Third Party's process for incident response, escalation, and remediation. Third Party's IRP must have an established process for forensic investigation in compliance with applicable legal standards for the preservation of evidence. Third Party will notify Rivian at cybersecurity@rivian.com within twenty-four (24) hours following a suspected or actual information security incident, including those that risk exposure or unauthorized access of Rivian's information, and including any incidents involving contractor or third-party system storing Rivian's information, and incidents affecting the integrity or availability of Rivian's information. Third Party will provide reasonable assistance, information, and cooperation to Rivian to investigate and remediate any incident at Third Party expense.

20. **Cybersecurity Insurance:** Subject to the policies' terms and conditions, Third Party shall maintain, at its own cost and expense, Media/Technology/Cyber Liability insurance, including coverage for breaches of network security, wrongful disclosure of confidential information, unauthorized access to or use of data, corruption of data (aka Errors and Omissions) in a form acceptable to Rivian and in amounts sufficient to ensure its obligations hereunder (the "**Policy**"). Third Party will provide Rivian with at least thirty (30) calendar days prior written notice of cancellation or nonrenewal of the policies.

21. **Program Review by Rivian:** Third Party agrees to provide Rivian with evidence of the Program and Third Party's compliance with these Requirements upon Rivian's reasonable request, from time to time. Rivian agrees that all evidence provided to Rivian will only be shared with Rivian's personnel that have a need to know such information as part of their job function for Rivian. If Rivian identifies instances of non-compliance with these Requirements, Third Party will, at its sole cost and expense, take all actions necessary to remediate such non-compliance and Rivian reserves the right to exercise any remedies available under the contract in place between the parties or otherwise available at law.

22. **Security Review by Rivian:** Rivian or its authorized third-party service providers may perform a comprehensive security assessment of Third Party's external technology infrastructure against these standards, including vulnerability scanning and, upon reasonable prior notice, penetration testing. Rivian will make reasonable efforts to minimize interference with Third Party's operations and Rivian agrees the results of any security review will only be shared with the Third Party and Rivian's personnel that have a need to know such information as part of their job function for Rivian.

23. **Annual Program Review:** Third Party will review the Program on an annual basis.

24. **Vendor Noncompliance:** Unless otherwise expressly stated in a written agreement between the parties, Third Party's noncompliance with these Requirements shall constitute a material breach of the agreement between the parties.