3M DATA SECURITY EXHIBIT
INFORMATION SECURITY REQUIREMENTS

This 3M Data Security Exhibit ("**Data Security Exhibit**") supplements the Agreement or any Purchase Order Terms ("Agreement") into which it is incorporated. Capitalized terms not defined in this Data Security Exhibit have the meaning ascribed to such terms in the Agreement. The provisions of this Data Security Exhibit supplement, and in the event of any inconsistency supersede, the security provisions of the Agreement.

1. DEFINITIONS

"**Cybersecurity Incident**" means an unauthorized incident, or a series of related unauthorized incidents, on or conducted through Supplier Information Systems that impacts the confidentiality, integrity or availability of Supplier Information Systems, including by jeopardizing business operations, finances, legal compliance, or reputation. For example, Cybersecurity Incidents may include malware, cyber-attacks, insider actions, or systemic control failures that allow unauthorized access, theft, exposure, alteration, or destruction of assets or data; or that may cause business interruptions to Supplier or its customers; or that may cause direct or indirect financial impact to Supplier or its customers.

"**Information Systems**" means information technology resources, owned, or used by the organization (including information technology services provided by third-party service providers), including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of the organization's information to maintain or support the organization's operations.

"**Process**" means any operation or set of operations which is performed on 3M Confidential Information or sets of 3M Confidential Information, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, access, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

2. INFORMATION SECURITY PROGRAM REQUIREMENTS

2.1 General. Supplier shall, during the term of the Agreement, maintain and comply with security controls and safeguards (including environmental, safety, and facility procedures and data security practices) against destruction, loss, alteration, or inappropriate access or disclosure of 3M Confidential Information. Such security controls shall be (i) in conformance with the Agreement and this Data Security Exhibit; (ii) in conformance with, and sufficient for 3M to meet, applicable laws and regulations, including Applicable Privacy Laws; (iii) at least equal to industry standards; and (iv) reasonably appropriate to protect against unauthorized destruction, loss, alteration or unauthorized disclosure of or access to 3M Confidential Information.

2.2 Written Information Security Program. Supplier, at its sole expense, shall implement, maintain, and comply with a comprehensive written information security program ("**Security Program**") and only Process 3M Confidential Information in compliance with this Agreement and applicable law. The Security Program shall include provisions covering: (a) security principles of "segregation of duties" and "least privilege" with respect to 3M Confidential Information, including (i) a process by which Supplier Personnel user accounts may only be created with proper leadership approval and are timely deleted, (ii) an auditable history of changes, and (iii) an annual review and remediation for excess access authorization; (b) retention policies applicable to 3M Confidential Information for all reports, logs, audit trails and other documentation that provides evidence of data security, systems, and audit processes and procedures; (c) information security policies compliant with ISO27001 and/or the NIST Cybersecurity Framework, and which are applicable to 3M Confidential Information and document, among other things, the consequences for violations of information security policies; (d) timely deployment of security patches to all systems that Process 3M Confidential Information as necessary to comply with this Agreement and applicable law; and (e) securely returning or disposing of all 3M Confidential Information once Supplier no longer needs 3M Confidential Information to perform the Services under the Agreement.

2.3 Security Program Certification.

(a) Supplier certifies that at all times during the Term, the Security Program and all applicable security controls will conform to relevant industry standards and best practices, including ISO 27001 and/or the NIST Cybersecurity Framework. Supplier represents and warrants that: (i) its Security Program complies with applicable law and (b) Supplier holds a current and compliant external security certification such as ISO 27001 or SOC2. Upon 3M's written request, Supplier will provide 3M with its current certification of compliance with ISO 27001 or SOC2.

(b) If Supplier Processes 3M Confidential Information containing card holder or other related data in connection with the Services, Supplier represents and warrants that the Security Program complies with the Payment Card Industry Data Security Standard ("PCI DSS") including establishing, implementing, and maintaining, a Security Program that is designed to protect the security, confidentiality, and integrity of 3M Confidential Information in both electronic and physical form, and that it shall undergo independent, third-party quarterly system vulnerability scans, and Supplier shall promptly provide, upon 3M's written request, current certification of compliance with the PCI DSS, by an authority recognized by the payment card industry for that purpose.

2.4 Ongoing Review of Security Program. Supplier represents and warrants that it has and will maintain a process for identifying, assessing, and mitigating the risks to 3M Confidential Information Processed by Supplier in each relevant area of Supplier's operations and evaluating the effectiveness of the safeguards for controlling these risks. Supplier shall continue to improve its Security Program to ensure security and compliance with applicable law. Supplier shall regularly monitor, test, and update its Security Program. Supplier shall provide 3M with such information concerning Supplier's Security Program as 3M may reasonably request from time to time.

2.5 Encryption of 3M Confidential Information. Supplier shall encrypt 3M Confidential Information while at rest or in motion using then-current appropriate, non-proprietary, industry encryption technologies and at a minimum of 256-bit encryption, including additional encryption requirements that may be necessary for compliance with applicable law and in the following circumstances: (a) the Processing of 3M Confidential Information on any mobile device or mobile storage or removable media, including laptop computers, smart phones, USB devices, and tapes/DVDs, and (b) electronic transfers of 3M Confidential Information by Supplier outside of its network. Data encryption is required for any servers, desktop and laptop computers, removable storage media, and other mobile devices where 3M Confidential Information may be stored.

2.6 Monitoring and Security Flaw Resolution. Supplier shall proactively ensure the security of its applications and environment. Supplier shall ensure that the Services and its networks, servers and applications are continuously monitored for potential security vulnerabilities (each, a "**Security Flaw**"). Supplier shall respond to and remediate any detected Security Flaws applicable to the Services in accordance with prevailing industry standards and applicable law, and the following remediation timeframes based on the risk level of such Security Flaw under the Common Vulnerability Scoring System ("**CVSS**"):

Risk Level	Definition	Remediation Timeframe
Critical	CVSS Scores 9.0-10	Five (5) Days
High	CVSS Scores 7.0-8.9	Seven (7) Days
Medium	CVSS Scores 4.0-6.9	Ninety (90) Days

Notwithstanding the foregoing, Supplier shall: (i) promptly respond to and contain any detected Security Flaw subject to a known exploit, remotely exploitable by an unauthenticated user within 36 hours of discovery and (ii) notify 3M of any detected zero-day vulnerability applicable to the Services within 24 hours of such detection, and immediately address such vulnerability.

2.7 Vulnerability Assessments. If Supplier hosts an internet-facing and/or mobile application capable of Processing 3M Confidential Information in connection with the Services, then Supplier shall annually have a vulnerability threat assessment ("**VTA**") performed by a reputable supplier and provide 3M with a summary attestation of the VTA including: (a) a definition for how vulnerabilities are rated (e.g., high/medium/low, serious/moderate/minimal), (b) evidence that the application has no open vulnerabilities at the high-equivalent rating, and (c) the number of vulnerabilities at any below high-equivalent ratings and evidence that such vulnerabilities have been promptly remediated. Supplier acknowledges that Supplier's failure to comply with the foregoing requirement is deemed a material breach of the Agreement.

2.8 Training. Supplier shall provide data privacy, data security, and confidentiality awareness training at least annually to all individuals authorized by Supplier to Process 3M Confidential Information (including all of Supplier's employees and contractors). Training must occur before such individuals Process 3M Confidential Information, and such individuals shall repeat such training at least annually. 3M may review Supplier's training materials (or a reasonable summary) upon reasonable advance notice to Supplier.

2.9 Identified Subcontractors. If Supplier subcontractors or affiliates ("**Contractors**") Process 3M Confidential Information on behalf of Supplier subject to 3M's express consent elsewhere in the Agreement, Supplier shall: (a) ensure that each Contractor maintains security controls, safeguards, and a written information security program that complies with this Data Security Exhibit via sufficient diligence and oversight; and (b) be responsible and liable for the acts and omissions of Contractors and all Supplier Personnel as if their acts and omissions were made by Supplier. Supplier shall promptly notify 3M in writing prior to changing or appointing any new Contractors who will Process 3M Confidential Information on behalf of Supplier.

2.10 Changes to Processing. Supplier shall provide 3M with no less than 30 days prior notice of a proposed material modification to the process, method, or means by which 3M Confidential Information is Processed (including any geographic change). If 3M reasonably determines and notifies Supplier that such modification could materially degrade the security of 3M Confidential Information, then Supplier shall not make such modification.

2.11 Incident Management. The Security Program will maintain, monitor, and enforce reasonable organizational, administrative, technical, and physical safeguards to protect the security, integrity, confidentiality, and availability of 3M Confidential Information, including a comprehensive program plan to immediately detect, respond to, and manage Cybersecurity Incidents. Supplier shall promptly investigate, contain within 24 hours, and remediate all Cybersecurity Incidents affecting 3M Confidential Information, 3M Systems, and/or 3M's use of the Services, and shall take, at its own expense, appropriate measures reasonably necessary to mitigate any known, harmful effect of a Cybersecurity Incident. Supplier shall: (a) regularly update 3M of the results of the investigation and remediation efforts; (b) provide 3M with written assurances reasonably satisfactory to 3M that such Cybersecurity Incident shall not reoccur; and (c) cooperate, at its own expense, with 3M in its investigation of any Cybersecurity Incident affecting 3M Confidential Information, 3M Systems, or 3M's use of the Services.

2.12 Notification and Report to 3M of Cybersecurity Incidents and Privacy Incidents.

(a) Supplier shall notify 3M via email at GlobSecOpsCenter@mmm.com within 24 hours of Supplier's becoming aware of any Cybersecurity Incident impacting 3M Confidential Information, 3M Systems, or 3M's use of the Services or any Privacy Incident ("**Security Incident Notification**"). 3M reserves the right to disclose Supplier's name in connection with a reported Cybersecurity Incident or Privacy Incident .

(b) Within three (3) business days of the initial Security Incident Notification, Supplier shall provide a written report ("**Security Incident Report**") that includes, at a minimum subject to the availability of necessary information and as applicable, the following: (i) a description of the Cybersecurity Incident or Privacy Incident (including cause) and the affected 3M Confidential Information; (ii) the date that the Cybersecurity Incident or Privacy Incident occurred; (iii) the date that the Cybersecurity Incident or Privacy Incident was discovered; (iv) the identity of each affected individual; (v) the affected categories of Personal Information, if any, for each affected individual; (vi) the approximate number of affected individuals and the approximate number of records containing Personal Information that are involved; (vii) an identification of any law enforcement agency or government agency that has been contacted about the Cybersecurity Incident or Privacy Incident and contact information for the relevant official; (viii) a description of the steps that have been, or will be, taken to mitigate the Cybersecurity incident or Privacy Incident; (ix) a description of the steps that have been, or will be, taken to prevent a recurrence; (x) the likely consequences of the Cybersecurity Incident or Privacy Incident; and (xi) contact information for the person at Supplier principally responsible for responding to the Cybersecurity Incident or Privacy Incident.

(c) Supplier shall update the written Security Incident Report periodically as new information becomes available. Supplier shall provide the Security Incident Notification and Security Incident Report, as required by this Section 2.12, by email to 3M at GlobSecOpsCenter@mmm.com. Supplier acknowledges that its determination that a particular set of circumstances constitutes a personal data breach as defined by Applicable Privacy Laws shall not be binding on 3M.

(d) If a Cybersecurity Incident or Privacy Incident results from either (i) the negligence or misconduct of Supplier (or any Contractor) or (ii) a failure of Supplier to comply with the terms of this Data Security Exhibit, the Privacy Exhibit, or the Agreement, Supplier shall bear the actual costs associated with resolving the Cybersecurity Incident or Privacy Incident, including the costs of notifying individuals, regulators and others as required by law or needed to address a real risk of harm, providing individuals with credit monitoring (or other appropriate remediation service), and responding to individual, regulator, and media inquiries.

2.13 3M Notifications. Supplier acknowledges and agrees that 3M shall determine (i) whether and when to notify any government agency of the Cybersecurity Incident or Privacy Incident and which government agency to notify; (ii) whether 3M will provide notice to individuals with respect to any Cybersecurity Incident involving Personal Information or Privacy Incident; (iii) the content of any such notice(s); (iv) the timing for, and method of, delivery of any such notice(s); and (v) the products or services, if any, to be offered to affected individuals. Unless prohibited by applicable law, Supplier shall obtain 3M's prior written consent to disclose that 3M has been impacted by a Cybersecurity Incident or Privacy Incident in any public notices, filings, or press releases.

2.14 Audit of Security Controls. Upon 3M's written request, Supplier shall: (a) provide to 3M copies of third party assessments, test results, audits or reviews; (b) complete 3M's security questionnaire, and (c) reasonably cooperate with 3M, its designees and government authorities, in connection with onsite or virtual inspections of Supplier and its Contractors storing 3M Confidential Information, and with self-assessment security compliance reviews. On-site inspections will be performed upon reasonable advance notice during Supplier's regular business hours and subject to reasonable confidentiality obligations. Supplier and 3M will be responsible for their own costs in connection with such inspections.

2.15 Business Continuity. Supplier shall implement, document, and maintain appropriate business continuity and disaster recovery plans to enable it to continue or resume providing Services (including restoring access to 3M Confidential Information) in a timely manner after a disruptive event. At appropriate intervals or as otherwise requested by 3M, Supplier shall provide reasonable information regarding its business continuity and disaster recovery plans to 3M. All such information is Supplier's confidential information.