DuPont Data Security Addendum

The terms of this Data Security Addendum (**"Addendum"**) define information security controls that a Supplier must adopt when (a) accessing DuPont Systems, (b) handling DuPont Data or (c) having custody or control of DuPont Systems or DuPont Data. The Supplier is responsible for compliance to these terms by Supplier Personnel. Additional security compliance requirements may be specified in the Contract. A failure to comply with the requirements of this Addendum shall constitute an event of default under the Contract.

1. Definitions

"Affiliate(s)" means any company, corporation, general or limited partnership, limited liability company, joint venture, organization, association, or other enterprise or entity in which a party directly, or indirectly through one or more intermediaries, has an ownership interest (as a result of ownership of stock or other voting securities, contractual relationship, or otherwise) or any entity controlling or under common control with any such entity.

"Audits" has the meaning ascribed thereto in Section 2.5 of this Addendum.

"Contract" means any agreement (including, but not limited to, appendices and scopes of work) between DuPont and Supplier to which this Addendum applies.

"Computing Device" means any desktop or laptop computer, mobile device (e.g., cellular phone, smartphone, tablet), server or storage device, real or virtual, or removable media storage device (e.g., flash drive, external SSD) that (a) is involved in the performance of the Contract, (b) may be used to access DuPont Systems, or (c) may access, process, transmit or store DuPont Data.

"Data Sanitization Requirements" has the meaning ascribed thereto in Section 5.1 of this Addendum.

"DuPont" means DuPont de Nemours, Inc., its Affiliates, divisions, or subsidiaries that are a party to the Contract.

"DuPont Data" means any data or information in any form or medium, including, without limitation, derivative documents created by Supplier relating to DuPont (including, but not limited to, customers of DuPont or a DuPont distributor) that is: a) submitted (or to which access is permitted by DuPont), including (without limitation) data in DuPont Systems; or (b) collected, processed, developed or produced by Supplier (other than data internal to Supplier) in connection with the Services or Products provided to DuPont by Supplier. For certainty, DuPont Data includes, without limitation, DuPont employee and contractor authentication information and other Sensitive Information.

"DuPont Network" means any DuPont computer network (owned or controlled by DuPont or a third party on behalf of DuPont) to which Supplier is provided access in connection with the Contract.

"DuPont Systems" means any Computing Device, network (including, but not limited to, the DuPont Network), or Information Systems, either owned or controlled by DuPont or Supplier or operated by the Supplier to access, process, transmit, or store DuPont Data.

"DEAA" means the DuPont Electronic Access Agreement required to be executed by the Supplier as a condition of Supplier obtaining access to the DuPont Network.

"Information System(s)" means any system, including (without limitation) development, test, stage and production systems, or storage/backup systems, that may access, process, transmit or store DuPont Data.

"ISR" means the information security requirements mandated by DuPont from time to time.

"Product(s)" means any goods, services, software and deliverables supplied under the Contract.

"Security Breach" has the meaning ascribed thereto in Section 7.1 of this Addendum.

"Sensitive Information" means information that is collected, processed, maintained, used, shared, or disseminated in connection with the Contract that requires protection to ensure its confidentiality, integrity or availability, including (without limitation) any DuPont proprietary information and third-party proprietary information (identified as such in the Contract or provided in connection therewith), or personal information.

"Services" means work or other activities to be performed by Supplier for DuPont as specified in the Contract, including (without limitation) services ancillary to the supply of Products.

"Supplier" means the entity identified in the Contract and includes Supplier Personnel.

"Supplier Personnel" means all Supplier employees, subcontractors and agents who may access DuPont Systems or DuPont Data relating to or in connection with the Contract.

2. Security Requirements and Compliance

2.1. Supplier must have a confidentiality agreement in place with DuPont and comply with requirements of that agreement, including (without limitation) the Confidential Information Requirements for DuPont Suppliers found at:

https://www.dupont.com/content/dam/dupont/amer/us/en/corporate/supplier-center/documents/ConfidentialInformationRequirements.pdf

2.2. Before being granted access to any portion of the DuPont Network, Supplier shall sign a DEAA. DuPont reserves the right, at its sole discretion, to restrict or limit access to the DuPont Network.

2.3. Supplier shall segregate all DuPont Data (with the exception of email communications) from data of third parties. In addition, Supplier shall employ appropriate protective mechanisms against access by third parties to DuPont Data except as may be authorized by the Contract or otherwise by DuPont in writing.

2.4. Supplier shall secure DuPont Data and its own data which are necessary for the delivery of the Products or Services against unauthorized access, modification, destruction and other misuse; and shall utilize state-of-the-art, industry-standard technical and organizational measures to ensure such security. At DuPont's request, Supplier shall provide evidence of the implementation of these measures (e.g., certification to ISO/IEC 27001, ISO/IEC 62443, ISO/SAE 21434) without additional remuneration. Depending on the type and protection requirements of the affected DuPont Data, or the significance of the Products or Services delivered by Supplier for the business operations of DuPont or its customers, DuPont may require Supplier's compliance with particular certification regimes, such as ISO/IEC 27001 or the "Trusted Information Security Assessment Exchange" ("TISAX") of the German Association of the Automotive Industry (Verband der Automobilindustrie e. V.), Berlin, Germany ("VDA").

2.5. Supplier must timely and accurately complete any questionnaires furnished by DuPont assessing Supplier's cybersecurity controls. Supplier shall provide copies of all industry standard cybersecurity attestations and third-party audits performed within the past 12 months. DuPont also has the right to audit compliance by Supplier with the requirements in this Addendum (**"Audits"**) upon reasonable notice, including (without limitation) in the case of a known or suspected Security Breach. Supplier shall cooperate with such Audits, which may be conducted by DuPont itself or by a third party designated by DuPont that is bound by reasonable confidentiality obligations to Supplier. If such assessments or Audits indicate the presence of moderate or high levels of risk, DuPont and Supplier will meet promptly to discuss such risk. The Supplier will be expected to develop and expeditiously implement a remediation plan acceptable to DuPont.

3. Supplier Personnel Security

3.1. Supplier must implement and maintain access/screening policies and processes that include the following controls:

a. Supplier must carry out appropriate background checks on all Supplier Personnel who will have access to the DuPont Systems. If a Supplier Personnel fails a background check, then Supplier must withhold access to the DuPont Systems and DuPont Data.

b. All background checks on Supplier Personnel must be carried out in accordance with DuPont's requirements.

c. Supplier must ensure that all Supplier Personnel undergo adequate training in the care, protection and access to DuPont Systems and handling of DuPont Data prior to being granted access.

3.2 Supplier Personnel working on-premises at DuPont sites or who have access to DuPont Systems or DuPont Data will be required to comply with ISR.

4. Access Controls to DuPont Systems

4.1 Supplier may not make any changes to user access controls or capabilities to any of the DuPont Systems, unless it has obtained DuPont's prior written approval.

4.2 Supplier is required to provide a listing of all parties and locations storing, accessing, maintaining or processing DuPont Data. Supplier will provide an updated list to DuPont when locations or parties change.

4.3 At DuPont's request, Supplier will provide logging, monitoring and reporting on all access to, and security events related to:

a. DuPont Systems managed or maintained by Supplier; and
b. Supplier or Supplier Personnel Computing Devices with access to DuPont Data or DuPont Systems.

Supplier shall retain all log files for not less than ninety (90) days and shall provide copies of them when requested by DuPont for it to conduct data forensics for purposes of assessing accuracy, access, availability and security controls, and evidencing legal and regulatory compliance. Supplier agrees to update event logs to capture additional data as required by DuPont.

4.4 Supplier shall comply with any request by DuPont to initiate a **"**litigation hold**"** related to any DuPont Data stored or processed by Supplier.

4.5 Supplier shall encrypt all DuPont Data in Supplier's custody or control in transit to/from and/or at rest in connection with the Services or Products delivered to DuPont.

4.6 Privileges granted to Supplier Personnel shall be the minimal set required for the performance of his or her job in a timely and efficient manner and only for the duration of the need.

4.7 Passwords and PINs used by Supplier Personnel shall be delivered in a confidential manner that requires the recipient to prove his/her identity before the password/PIN is received.

4.8 Passwords and PINs shall not be delivered with their associated User ID in the same communication unless confidentiality of the delivery and proof of recipient identity is ensured by using industry standard public key cryptography.

4.9 Temporary, reset or initial passwords/PINs shall be unique for each Supplier Personnel and will be required to change upon first use and shall not be reused for at least 24 iterations, or as otherwise communicated by DuPont in writing.

4.10 Valid proof of account holder identity shall be provided and verified before a password or PIN is changed.

4.11 Compromised accounts and accounts suspected of having been compromised shall be disabled as soon as technically possible.

5. Export and Disposal of DuPont Data

5.1 When removing or replacing any media storage devices (whether as a repair, replacement or at end of life) that store DuPont Data, Supplier will clear DuPont Data from the Computing Device using processes that meet or exceed the DoD 5220.22-M or NIST 800-88 standards (**"Data Sanitization Requirements"**). Supplier shall provide certification that all DuPont Data has been removed from the Computing Device has been destroyed in accordance with the Data Sanitization Requirements. Supplier shall also delete all DuPont Data from all Supplier (including Supplier Personnel) locations at the end of the term of the Contract, subject to all applicable legal requirements. Data deletion must render the information unrecoverable.

5.2 Supplier must allow and ensure that DuPont can receive DuPont Data from Supplier and Supplier Personnel at any time or within 60 days following the expiration of the Contract.

6. Data Security Governance

6.1 Supplier's Security Plan

a. Supplier must establish and maintain data safeguards against the destruction, loss, alteration of, or unauthorized access to DuPont Data in the possession or control of Supplier. Supplier shall define and adhere to a coherent, complete set of written information security policies, standards, and practices that comply with all legal, regulatory, and contractual requirements and industry-standard best practices, including, but not limited to: (a) asset management; (b) annual risk assessment and continual risk management; (c) access control and protective technology; (d) data security and information protection; (e) continuous security monitoring and detection; and (f) incident response.

b. Supplier agrees to comply with all ISR. Supplier agrees and understands that security and risk management requirements may be changed by DuPont from time-to-time, and Supplier agrees to abide by the then-current ISR. In some cases, changes in the ISR may give rise to changes in the Contract and, as applicable, will be processed and implemented in accordance with change management processes as may be further defined in the Contract.

c. Supplier shall promptly notify DuPont of any Supplier financial distress, catastrophic events or significant incidents, including (but not limited to) information and data loss breaches (even if DuPont Data is not involved), service or system interruptions, compliance lapses, enforcement or other regulatory actions, or any government agency investigation of Supplier's compliance practices or other significant compliance events, except where Supplier is not permitted under applicable law to notify DuPont.

6.2 Modification or Circumvention of DuPont Security Controls

Supplier shall execute all documents and adhere to all process and procedures generally required by DuPont to access DuPont Systems, including (without limitation) the DEAA. Except as may be specifically set forth in a given Contract or pursuant to written approval by DuPont, Supplier shall not: (i) alter or disable any hardware or software security programs residing on DuPont Systems; or (ii) cause unauthorized traffic to pass into DuPont Systems.

6.3 **Asset Management**

6.3.1 Supplier shall maintain an inventory of its hardware and software assets that documents the identification, ownership, usage, location and configuration for each item.

6.3.2 Supplier shall maintain documentation and other records of baseline system and security configurations, including (without limitation) configuration changes for all hardware and software system components.

6.3.3 Supplier shall have formal policies and practices for performing risk assessments of software, systems and facilities. This includes classifying information and information systems, identifying security requirements, assessing and ensuring compliance with Supplier's policies and other applicable requirements, and adhering to change management processes.

6.3.4 Supplier shall have controls in place to cause Supplier Personnel and other users to abide by acceptable use and other policies to ensure compliance with the DuPont security requirements in this Addendum as well as Supplier's own requirements. Any difference in requirements will require adherence to the more stringent requirement.

6.4 **Mobile Devices and Removable Storage**

With respect to Computing Devices used by Supplier, Supplier must employ malicious software and mobile controls that meet or exceed the following requirements:

6.4.1 Anti-malware software will be installed, properly configured and running at all times on all Computing Devices. The software shall be configured to protect against all known threats, including (but not limited to) viruses, worms, Trojans, rootkits, spyware and keystroke loggers.

6.4.2 Upon detection of malicious content, Supplier’s anti-malware system must immediately quarantine, block, disable, or otherwise halt the malicious content so that it does not spread.

6.4.3 Devices shall be routinely scanned to detect and remove any malicious code or viruses using industry standard end-point protection tools and techniques.

6.4.4 Upon request from DuPont, Supplier shall confirm in writing that a check of its Computing Devices found no indications of any known threats.

6.5 **Network Connections**

If a network connection is established between DuPont and the computing environment(s) used by Supplier, Supplier will (i) permit DuPont or a third party under DuPont’s direction to perform network assessments of such computing environment(s) based on a mutually-agreed schedule, and (ii) maintain an alert status regarding the security of such computing environments, including (without limitation) all vulnerabilities and security patches or corrective actions, by subscribing to an industry-recognized service, such as CERT or CIAC. If DuPont’s assessment reveals that Supplier employs inappropriate or inadequate security controls contrary to DuPont security requirements, DuPont may, in addition to other remedies it may have, refuse continued access to the DuPont Systems.

7. Security Breach and Evaluations

7.1 In the event Supplier suffers or learns of any actual or suspected security breach, any unauthorized release of personal data or other DuPont Data, or any unauthorized intrusions into Supplier's facilities or secure systems used to provide the Products or Services to DuPont or that otherwise have direct or indirect access to DuPont Data (collectively, a **"Security Breach"**), then Supplier will immediately (no later than twenty-four (24) hours): (i) notify the designated person at DuPont; (ii) estimate the Security Breach's effect on DuPont, including (without limitation) DuPont Data or DuPont Systems; (iii) limit the damage; (iv) specify the corrective action to be taken; (v) investigate and determine if a Security Breach has occurred; (vi) take corrective action to prevent further Security Breaches; (vii) accept all appropriate measures taken at DuPont as a result of the Security Breach to protect the DuPont Systems (e.g., disconnection of IT system connections); (viii) ensure trouble-free reconnection to the DuPont Systems; and (ix) support DuPont in the recovery of DuPont Data if the Security Breach causes an interruption or delay in the delivery of Products or Services, a decrease in operational efficiency, or the loss of DuPont Data.

7.2 Supplier must, as soon as is reasonably practicable, make a report to DuPont including details of the Security Breach (including, but not limited to, the nature of the information disclosed and the identity of the parties to whom such information pertains) and the corrective action Supplier has taken to limit damage and prevent further Security Breaches. In the case of a Security Breach involving DuPont Data, including (without limitation) customer information, Supplier must cooperate fully with DuPont for the purpose of notifying DuPont customer(s) as to the facts and circumstances of the breach of the customer's particular information. Additionally, Supplier must cooperate fully with all government regulatory agencies and law enforcement agencies having jurisdiction and authority for investigating a Security Breach and any known or suspected criminal activity.

7.3 Supplier acknowledges and agrees that all damages associated with a Security Breach, including (but not limited to) costs of notifications, costs of reasonable mitigation for affected data subjects, any governmental fines or penalties, and costs and expenses of recreating or reloading any lost, stolen or damaged data, will be considered direct damages.

7.4 Supplier shall regularly test, assess and evaluate the effectiveness of its processes and systems used for compliance with obligations imposed by this Addendum, and the applicable data protection laws with respect to the confidentiality, integrity, availability, and security of DuPont Data. Supplier shall document the results of these evaluations and any remediation activities taken in response to these evaluations.

8. Security Incident Management

Supplier shall employ comprehensive and effective security incident monitoring, reporting and response processes, procedures and controls. These processes, procedures and controls will, at a minimum, (a) identify, report and mitigate/resolve known or suspected security incidents, including (without limitation) any unauthorized access, acquisition, use, disclosure or destruction of DuPont Data, and (b) produce informative and accurate alert notification to DuPont within twenty-four (24) hours of any known or suspected compromise of DuPont Data, DuPont Systems or other Security Breach.

9. Physical Security

9.1 Supplier must establish and maintain physical security policies, practices and controls that include (without limitation): (a) physical access controls and protective equipment; (b) tracking and control methods when media containing DuPont Data are transported; and (c) continuous data security and information protection, monitoring detection, and incident response.

9.2 Supplier Personnel are strictly prohibited from possessing weapons or firearms of any kind on DuPont sites.

10. Supply Chain Obligations

Supplier shall endeavor through appropriate contractual provisions to cause its sub-suppliers to comply with the provisions of this Addendum, as applicable, and to pass this obligation accordingly along their supply chain.