Customer Data Protection Addendum ("DPA")

1. Data Processing. This DPA supplements the underlying services agreement(s) between Cintas and Cintas's Customer ("**Customer**") (the "**Agreement**") pursuant to which Cintas provides functions for or on behalf of Customer ("**Services**") involving the processing of Personal Information (defined below). Customer and Cintas are each a "**Party**" and collectively referred to herein as the "**Parties**."

2. Definitions. The following definitions shall apply for purposes of interpreting this DPA. Capitalized terms used but not defined in this DPA have the meaning given to them in the Agreement or Data Protection Laws.

   a) "**Collects**," "**collection**," "**consent**," "**deidentified**," "**controller**," "**process(ing)(ed)**," "**processor**", "**sell**," "**selling**," "**share**," and "**service provider**" shall have the meanings given to such terms in applicable Data Protection Laws.

   b) "**Data Protection Laws**" means any law that governs the Party's processing of Personal Information, including the California Consumer Privacy Act (CCPA).

   c) "**Personal Information**" or "**Personal Data**" means information that relates to an identified or identifiable natural person ("**Data Subject**") provided to Cintas by or on behalf of Customer for the purpose of enabling Cintas to provide the Services. Personal Information does not include business-to-business contact information exchanged by the Parties for the purposes of negotiating and executing the Agreement.

3. Customer Obligations. Customer will provide only Personal Information that is adequate, relevant, and reasonably necessary for Cintas to perform the Services. Customer represents and warrants that its collection of Personal Information and disclosure to Cintas complies with all applicable Data Protection Laws.

4. Instructions. Cintas will process the Personal Information only (i) in accordance with Customer's instructions as documented in the Agreement, and further described in Annex I; and (ii) as needed to comply with applicable law, provided that Cintas shall not be required to act on any Customer instruction that could (in Cintas's reasonable opinion) cause Cintas to breach applicable law. Cintas will comply with Data Protection laws in performing the Services and will inform Customer if it believes that any Customer instructions regarding Personal Information processing would violate applicable Data Protection Law. Notwithstanding anything herein to the contrary, Customer acknowledges that Cintas may retain, use, disclose, or otherwise process Personal Information in manners permitted of a service provider/processor under Data Protection Laws and may create Deidentified data from Personal Information subject to Section 4(a).

   a) Deidentified data. To the extent Cintas receives or creates deidentified data in connection with this DPA, Cintas will: (i) maintain such information as deidentified and take reasonable measures to ensure that it cannot be associated with an individual or household (including implementing technical safeguards and business processes to prevent reidentification or inadvertent release of the deidentified data); (ii) publicly commit to maintain and use the information in deidentified form and not to attempt to reidentify the information; (iii) not attribute Customer as a source of such data; and (iv) contractually obligate any third parties receiving such information from Cintas to also commit to the same.

5. Security. Cintas will take reasonable steps to implement appropriate technical and organizational measures designed to protect Personal Information against anticipated threats or hazards to its security,

confidentiality, or integrity as described in Schedule 2 (Technical and Organizational Security Measures). Cintas will ensure that persons authorized to process Personal Information have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

6. Security Breach. Cintas will notify Customer without undue delay whenever Cintas learns that there has been a breach of Cintas's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Information processed that requires notification to Data Subjects, government authorities, and/or other third parties under Data Protection Laws, unless such notification is prohibited by applicable law or otherwise instructed by law enforcement or a supervisory authority. Taking into account the nature of processing and the information available to Cintas, Cintas will take reasonable steps to assist Customer at Customer's reasonable request in complying with Customer's notification obligations as required by applicable Data Protection Law. Cintas reserves the right to charge a reasonable fee to Customer for any requested assistance.

7. Return or Disposal. Within 30 days of termination of the Agreement, Customer may request that Cintas destroy or return to Customer all Personal Information, unless retained as part of Cintas's backup process or where applicable law requires Cintas to store the Personal Information so long as used only for those purposes.

8. Assessments. Upon Customer's reasonable request (to be exercised no more than once a year, unless required more frequently by a supervisory authority) Cintas will make available to Customer information in its possession necessary to demonstrate Cintas's compliance with this DPA and will allow for and contribute to reasonable assessments by Customer or its designated assessor (or if mutually agreed and at Cintas's expense, Cintas's qualified assessor) using an appropriate and accepted control standard or framework and assessment procedure for such assessments, and subject to reasonable access and confidentiality restrictions. If Cintas engages its own assessor, it shall provide a report of such assessment to Customer upon request. Any assessments shall be subject to Cintas's reasonable access and confidentiality requirements.

9. Subcontracting. Customer authorizes Cintas to transfer Personal Information to sub-processors for purposes of providing the Services to Customer. Cintas will maintain a list of the sub-processors and will provide this list to Customer upon request. Cintas will provide Customer 10 days' prior notice when adding a sub-processor to this list and the opportunity to object to such addition. If Cintas does not receive an objection within 10 days of the notice, the sub-processor is deemed to be accepted by Customer. Cintas will enter into an agreement with such sub-processor that includes data protection terms similar to this DPA.

10. Cintas Assistance. At Customer's reasonable request and taking into account the nature of the processing, Cintas will take reasonable steps to assist Customer with Customer's obligation to respond to Data Subjects' requests to exercise their rights under applicable Data Protection Law by taking appropriate technical and organizational measures. Taking into account the nature of the processing and the information available to Cintas, Cintas also will assist Customer at Customer's reasonable request in meeting Customer's compliance obligations to conduct data protection impact assessments and engage in related consultations of supervisory authorities. Cintas reserves the right to charge a reasonable fee to Customer for any requested assistance.

11. Processing Location. Customer agrees that Cintas may process Personal Information in countries where it or its sub-processors have operations, including the United States, Canada, Mexico, Honduras, Switzerland, and Singapore.

12. CCPA Compliance. Cintas will provide the same level of privacy protection for Personal Information of California residents as required of Customer under the CCPA. Cintas will notify Customer in writing if Cintas determines that it can no longer meet its obligations under the CCPA. Customer has the right, upon providing notice to Cintas, to take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Information, including where Cintas has notified Customer that it can no longer meet its CCPA obligations.

    In no event may Cintas: (a) disclose Personal Information of California residents to a third party for monetary or other valuable consideration or disclose Personal Information to a third party for cross-context behavioral advertising; (b) disclose Personal Information of California residents to any third party for the commercial benefit of Cintas or any third party; (c) retain, use, or disclose Personal Information of California residents outside of Cintas's direct business relationship with Customer or for a commercial purpose other than the business purposes specified in the Agreement or as otherwise permitted by applicable laws; or (d) combine Personal Information of California residents with personal information that Cintas receives from, or on behalf of, other persons, or collects from its own interaction with the Data Subject, except as permitted under applicable laws. Cintas certifies that it understands and will comply with the foregoing restrictions.

13. Conflicts; Enforceability. If any provision of this DPA is held to be invalid or unenforceable by any court of competent jurisdiction, such holding will not invalidate or render unenforceable any other provision of this DPA or any other contract between Customer and Cintas. This DPA supplements the Agreement. This DPA will control in the event of any inconsistency between the Agreement and this DPA. Any other provisions of or obligations under the Agreement that are otherwise unaffected by this DPA will remain in full force and effect. If this DPA, or any actions to be taken or contemplated to be taken in performance of this DPA, do not or would not satisfy either Party's obligations under the laws applicable to each Party, the Parties will negotiate in good faith upon an appropriate amendment to this DPA.

SCHEDULE 1 – DESCRIPTION OF PROCESSING

Categories of Data Subjects whose Personal Data is transferred:	• Customer personnel, including employees and contractors.
Categories of Personal Data transferred:	• Names and other business-to-business contact information, such as work e-mail, phone number, address. • Order details, including garment sizing where relevant, delivery address.
Sensitive data transferred (if applicable) and applied restrictions or safeguards:	• Not applicable.
Frequency of the transfer:	• Continuous for the term of the Agreement.
Nature of the processing:	• Collect and process orders.
Purpose(s) of the data transfer and further processing:	• Fulfill and provide customer service related to orders placed by data subjects.
The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period:	• Personal data will be retained for the period required to perform the Services under the Agreement unless a longer period is required by applicable law.
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:	• See description above.

SCHEDULE 2 – TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

This Schedule describes the security measures that will be taken by Cintas with respect to any Personal Information processed under the DPA.

1. **Information Security Policies and Standards.** Cintas will implement security requirements for personnel with access to Personal Information that are designed to ensure a level of security appropriate to the risk and address the requirements detailed in this Schedule. Cintas will conduct periodic risk assessments and, as appropriate, revise its information security practices whenever there is a material change in Cintas's business practices that may reasonably affect the security, confidentiality, or integrity of Personal Information, provided that Cintas will not modify its information security practices in a manner that will materially weaken Personal Information protection.

2. **Physical Security.** Cintas will maintain commercially reasonable security systems at all Cintas sites where an information system that uses or houses Personal Information is located. Cintas reasonably and appropriately restricts access to such Personal Information and implements practices to prevent unauthorized individuals from gaining access to Personal Information.

3. **Organizational Security.**
   a. Upon Customer's request, Cintas will provide contact information for its designated primary security manager.
   b. Cintas will implement procedures to prevent any subsequent retrieval of any Personal Information stored on media before the media is disposed of or reused.
   c. Cintas will implement security policies and procedures to classify information assets, clarify security responsibilities and promote awareness for employees.
   d. Cintas will manage all Personal Information breaches in accordance with appropriate procedures.
   e. Cintas will encrypt, using industry-standard encryption tools, Personal Information that Cintas: (i) transmits or sends wirelessly or across public networks; and (ii) stores on portable devices or at rest, where technically feasible.

4. **Network Security.** Cintas maintains network security using commercially available equipment and industry-standard techniques, including firewalls, intrusion detection and prevention systems, access control lists and routing protocols.

5. **Access Control.** Cintas will maintain appropriate access controls, including, but not limited to, restricting access to Personal Information to the minimum number of Cintas personnel who require such access. Cintas will maintain a list of the persons who have accessed Personal Information and a list of those who are permitted to access the Personal Information.

6. **Virus and Malware Controls.** Cintas will install and maintain anti-virus and malware protection software on the system and has in place scheduled malware monitoring and system scanning to protect Personal Information from anticipated threats or hazards and protect against unauthorized access to or use of Personal Information.

7. **Personnel.** Cintas will require personnel to comply with its Information Security Program. Cintas will train personnel on their security obligations.

8. **Business Continuity.** Cintas will implement appropriate back-up and disaster recovery and business resumption plans. Cintas will regularly review, test, and update its business continuity plan.