VENDOR DATA PRIVACY ADDENDUM

This Vendor Data Privacy Addendum ("**Privacy Addendum**"), is between Cintas Corporation, and its affiliates and subsidiaries, with its offices at 6800 Cintas Blvd., Cincinnati, OH 45040 ("**Cintas**") and the vendor or service provider ("**Service Provider**") in the underlying agreement (the "**Agreement**"). The requirements of this Privacy Addendum are in addition to, and not in lieu of any requirements contained in the Agreement. Capitalized terms which are not otherwise defined in this Privacy Addendum shall have the meanings attributed to such terms in the Agreement.

RECITALS

WHEREAS, Cintas and Service Provider entered into the Agreement that may require Service Provider to process Personal Data provided by or collected for Cintas, or whereby Service Provider may otherwise have access to Cintas' electronic systems or network (the "Services");

WHEREAS, this Addendum sets out the additional terms, requirements, and conditions governing Service Provider's obligations relating to its Personal Data handling and security practices; and

WHEREAS, additional terms, requirements, and conditions governing the Service Provider's obligations relating to the use of Cintas Data, which may or may not overlap with Personal Data, are contained in the Vendor Information Security Addendum, and which are in addition to, and not in lieu of, any requirements contained in this Privacy Addendum.

NOW, THEREFORE, in consideration of the mutual covenants and agreements hereinafter set forth and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties hereto agree as follows:

1. **Definitions**.

a. "Authorized Personnel" means Service Provider's employees, subprocessors, affiliates, and agents, and the officers, partners, employees and agents of each of the foregoing, who have a need to know or otherwise access Personal Data to enable Service Provider to perform its obligations under the Agreement, and who are bound in writing by confidentiality and other obligations sufficient to protect Personal Data in accordance with the terms and conditions of this Privacy Addendum.

b. "Business Purpose(s)" means the Services described in the Agreement or the enumerated Business Purposes set forth in Cal. Civ. Code section 1798.140(d)(1)-(7) and, on or after January 1, 2023, Cal. Civ. Code section 1798.140(e)(1)-(8) that are applicable to the Services as set forth in the Agreement, including but not limited to: performing Services on behalf of Cintas, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing advertising or marketing services, providing analytic services, or providing similar services on behalf of Cintas.

c. "Collects," "collected," "collection," "consent," "consumer," "contractor," "controller," "process(ing)(ed)," "processor," "personal information," "personal data," "sell," "sensitive data," "sensitive personal information," "share," "selling," "service provider," "sale," "sold," and "targeted advertising," shall have the meanings given to such terms in US Privacy Laws, the GDPR, the UK GPDR, or other applicable Data Protection Laws, and that may be further specified or defined in this Section 1.

d. "Data Subject" means an individual who is the subject of the Personal Data and to whom or about whom the Personal Data relates or identifies, directly or indirectly.

e. "Data Protection Laws" means all applicable federal, state, and foreign laws and regulations relating to the processing, protection, or privacy of the Personal Data, including, where applicable, the guidance and codes of practice issued by regulatory bodies in any relevant jurisdiction, including, without limitation, (1) GDPR; (2) the UK GDPR; (3) the Swiss DPA; (4) Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA"); (5) the Canadian Anti-Spam Legislation ("CASL"); (6) US Children's Online Privacy Protection Act ("COPPA"); (7) US Controlling the Assault of Non-Solicited Pornography and Marketing Act ("CAN-SPAM"); and (8) US Privacy Laws.

f. "EU Standard Contractual Clauses" or "EU SCCs" means, where the GDPR applies, the standard contractual clauses adopted by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, or any subsequent version thereof released by the European Commission. In the event any subsequent version of such clauses is released that is applicable to the Services, the Parties agree that the then-current version of the clauses will apply, in which case any references in this DPA to specific clauses shall be deemed to refer to equivalent clauses in the then-current version of the clauses, regardless of their enumeration.

g. "GDPR" means the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

h. "Personal Data" means personal information provided to Service Provider by or at the direction of Cintas, information which is created or obtained by Service Provider on behalf of Cintas, or information to which access was provided to Service Provider by or at the direction of Cintas, in the course of Service Provider's performance under this Agreement that: (i) identifies or can be used to identify an individual (including, without limitation, names, signatures, addresses, telephone numbers, email addresses, and other unique identifiers); or (ii) can be used to identify or authenticate an individual (including, without limitation, employee identification numbers, passwords or PINs, user identification and account access credentials or passwords, student information, answers to security questions, an individual's internet activity or similar interaction history, inferences drawn from other personal information to create consumer profiles, an individual's commercial, employment, or education history, and other personal characteristics and identifiers), in case of both subclauses (i) and (ii), including, without limitation, all Sensitive Personal Data and all other personal data as may be defined by Data Protection Laws. Personal Data is deemed to be Confidential Information of Cintas and is not Confidential Information of Service Provider.

i. "Privacy Rights Request" or "PRR" means a communication from a Data Subject regarding the exercise of rights pursuant to Data Protection Laws, including rights to access, rectification, restriction of processing, erasure, modification, and portability of Personal Data, as applicable.

j. "Process" or "processing" or any other correlative of the foregoing means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

k. "Security Incident" means (i) any act or omission that compromises either the security, confidentiality, availability, or integrity of Personal Data or the physical, technical, administrative, or organizational safeguards put in place by Service Provider (or any Authorized Personnel), or by Cintas

should Service Provider have access to Cintas' systems and to the extent such incident arises from Service Provider's access, that relate to the protection of the security, confidentiality, availability, or integrity of Personal Data, or (ii) receipt of a complaint in relation to the privacy and data security practices of Service Provider

l. or any Authorized Personnel or a breach or alleged breach of this Privacy Addendum relating to such privacy and data security practices. Without limiting the foregoing, a compromise shall include any unauthorized processing of Personal Data.

m. "Sensitive Personal Data" means any data that requires a heightened degree of protection by Data Protection Laws, including, without limitation, an (i) individual's government-issued identification number (including Social Security number, driver's license number, or state-issued identification number); (ii) financial account number, credit card number, debit card number, or 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; (iii) biometric, genetic, health, medical, or medical insurance data; (iv) geolocation data; or (v) other information that is subject to international, federal, state, or local laws or ordinances now or hereafter enacted requiring heightened standards for data protection or privacy, including, without limitation, the Health Insurance Portability and Accountability Act, the Health Information Technology for Economic and Clinical Health Act, the Fair Credit Reporting Act, COPPA, the Gramm-Leach-Bliley Act, and special categories of data as defined in the GDPR.

n. "Swiss DPA" means the Swiss Federal Act on Data Protection 1992 (including as amended or superseded).

o. "Swiss Privacy Addendum" means the EU SCCs as recognized and adopted by the Federal Data Protection and Information Commissioner ("FDPIC") under Art. 6 para. 2 and 3 of the Ordinance to the Federal Act on Data Protection DPO, SR. 235.11, as adopted, amended or updated by the FDPIC.

p. "Third Country(ies)" means any country that is neither a member of the European Economic Area ("EEA") or United Kingdom ("UK") nor has an adequacy status (i.e. (i) a status granted by the European Commission to non-EEA countries which provide a level of personal data protection that is comparable to that provided in EU law in accordance with GDPR, or (ii) a status granted by UK Secretary of State to non-UK countries which provide a level of personal data protection that is comparable to that provided in UK law in accordance with UK Data Protection Laws).

q. "UK Privacy Addendum" means the UK 'International data transfer addendum to the European Commission's standard contractual clauses for international data transfers' as adopted, amended or updated by the UK's Information Commissioner's Office, Parliament or Secretary of State.

r. "UK Data Protection Laws" means the Data Protection Act 2018 (DPA 2018), as amended, and EU General Data Protection Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, as incorporated into UK law ("UK GDPR"), as amended, and any other applicable UK data protection laws.

s. "US Privacy Law(s)" means all applicable U.S. federal and/or state security, confidentiality, and/or privacy laws, and regulations that are applicable to Cintas, the Services, Customer Data, and/or any other programs or products provided pursuant to the Agreement, including but not limited to the California Consumer Privacy Act ("CCPA") as amended by the California Privacy Rights Act ("CPRA"), the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Utah Consumer

Privacy Act, Connecticut's Act Concerning Personal Data Privacy and Online Monitoring, and any implementing regulations thereunder, in each case applicable to this DPA as and when legally effective.

2. **Standard of Care/Warranties.**

a. Service Provider acknowledges and agrees that, in the course of its engagement by Cintas, Service Provider may create, receive, process, or have access to Personal Data. Service Provider shall comply with the terms and conditions set forth in this Privacy Addendum in its processing of such Personal Data and be responsible for any unauthorized processing of Personal Data under its control or in its possession. Service Provider shall be responsible for, and remain liable to, Cintas for the actions and omissions of all Authorized Personnel concerning the treatment of Personal Data as if they were Service Provider's own actions and omissions.

b. Service Provider warrants and represents that:

i. Service Provider, and all Authorized Personnel, shall keep and maintain all Personal Data in strict confidence, using such degree of care as is appropriate to avoid unauthorized access, use, or disclosure, and shall not retain, use, disclose, or process Personal Data outside the business relationship between Cintas and Service Provider;

ii. Service Provider, and all Authorized Personnel, shall process Personal Data solely and exclusively for the Business Purpose and not process, use, retain, sell, share, rent, transfer, distribute, or otherwise disclose or make available Personal Data for Service Provider's own purposes or for the benefit of anyone other than Cintas, in each case, without Cintas' prior written consent;

iii. Service Provider, and all Authorized Personnel, shall process Personal Data in compliance with all Data Protection Laws and the terms of this Privacy Addendum;

iv. Service Provider's Authorized Personnel are reliable and trustworthy and have received the appropriate training on the Data Protection Laws relating to the Personal Data and are aware both of Service Provider's duties and their personal duties and obligations under the Data Protection Laws and this Privacy Addendum;

v. Service Provider will ensure that all Authorized Personnel who process Personal Data or otherwise have access to it are informed of the Personal Data's confidential nature and use restrictions and agree in writing to abide by the terms and conditions of this Privacy Addendum;

vi. considering the current technology environment and implementation costs, Service Provider will take appropriate technical and organizational measures to prevent the unauthorized or unlawful processing of Personal Data and the accidental loss or destruction of, or damage to, Personal Data in accordance with Section 6 hereof;

vii. Service Provider has no reason to believe that any Data Protection Laws prevent it from providing any of the Agreement's contracted Services; and

viii. Service Provider certifies that it understands the restrictions and obligations outlined in this Privacy Addendum and Applicable Data Protection Laws and will comply with them.

c. Neither Service Provider nor its Authorized Personnel will, directly or indirectly, disclose Personal Data to any person other than Authorized Personnel (an "Unauthorized Third Party"), without Cintas' prior written consent unless and to the extent required by applicable law, in which case, Service Provider shall (i) use best efforts to, and to the extent permitted by applicable law, notify Cintas before such disclosure or as soon thereafter as reasonably possible; (ii) be responsible for and remain liable to Cintas for the actions and omissions of such Unauthorized Third Party concerning the treatment of such Personal Data as if they were Service Provider's own actions and omissions; and (iii) require the Unauthorized Third Party that has access to Personal Data to execute a written agreement agreeing to comply with the terms and conditions of this Privacy Addendum and provide a copy of such written agreement to Cintas upon request.

3. **Personal Data Processing.**

a. Cintas retains control of and all rights, title, and interest in the Personal Data and remains responsible for its compliance obligations under the Data Protection Laws, including providing any required notices and obtaining any required consents, and for the Processing instructions it gives to Service Provider.

b. *Service Provider Obligations*.

i. Service Provider will only process, retain, use, or disclose the Personal Data to the extent, and in such a manner, as is strictly necessary for the Business Purposes in accordance with Cintas' written instructions, other reasonable instructions from Cintas, and Data Protection Laws as authorized under the Agreement. Service Provider must promptly notify Cintas if, in its opinion, Cintas' instruction would not comply with any Data Protection Laws. Without limiting the foregoing, Service Provider shall not use Personal Data for its own purposes.

ii. Service Provider shall not sell, rent, transfer, disclose, grant any rights in, or provide access to Personal Data to any third party except as expressly permitted herein.

iii. Service Provider must promptly comply with any Cintas request or instruction requiring Service Provider to amend, transfer, or delete the Personal Data, or to stop, mitigate, or remedy any unauthorized processing.

iv. Service Provider will reasonably assist Cintas with meeting Cintas' compliance obligations under Data Protection Laws, including, without limitation, conducting and documenting data protection assessments and prior consultations with the applicable supervisory authority, taking into account the nature of Service Provider's processing and the information available to Service Provider.

v. Service Provider must promptly notify Cintas of any changes to Data Protection Laws or its own practices or operations that may adversely affect its performance under the

vi. Agreement or this Privacy Addendum, or that would compromise its ability to comply with Data Protection Laws and will reasonably cooperate with Cintas' reasonable and appropriate steps to stop and remediate any unauthorized use of such Personal Data.

vii. Service Provider will only collect Personal Data for Cintas using a notice or method that Cintas specifically pre-approves in writing, which contains an approved data privacy notice informing the Data Subject of Cintas' identity and its appointed data protection representative, where applicable, the purpose(s) for which their Personal Data will be Processed, and any other information that is required by Data Protection Laws. Service Provider will not modify or alter the notice in any way without Cintas' prior written consent.

viii. Service Provider will restrict access to Personal Data to Authorized Personnel who require the Personal Data to meet Service Provider's obligations under this Privacy Addendum and the Agreement and to only the part or parts of the Personal Data that such Authorized Personnel strictly require for the performance of their duties.

ix. Service Provider shall not combine Personal Data processed under this Privacy Addendum with Personal Data it receives from or on behalf of another person or persons or that it collects from its own interaction with a consumer or Data Subject.

x. Service Provider shall delete Cintas Personal Data at the end of the provision of Services, or as otherwise instructed by Cintas, unless retention is (i) required by Data Protection Laws; or (ii) retained as part of backup or record keeping, so long as only used for such purposes and only for as long as reasonably necessary, subject to Data Protection Laws and this Privacy Addendum.

xi. To the extent that CPRA applies to the processing under this Privacy Addendum, Service Provider acknowledges and agrees it is a "service provider" as that term is defined under the CPRA and that it has read and understands the CPRA, including the obligations relating to service providers, and the obligations set forth in this Privacy Addendum. Service Provider further acknowledges that should Service Provider process Personal Data other than in accordance with this Privacy Addendum, Service Provider will be considered the "data controller" or "business" with respect to such Personal Data under applicable Data Protection Laws.

xii. Notwithstanding anything herein to the contrary, Service Provider may retain, use, disclose, or otherwise process Personal Data in manners permitted of a service provider/processor under US Privacy Laws or as otherwise required by Data Protection Laws (e.g., to engage subprocessors, for permitted internal uses such as improving products and services, for security and fraud prevention, compliance with legal obligations, etc.) and may create Deidentified data and Aggregate Consumer Information from Personal Data subject to the following terms ("Permitted SP Purposes"):

A. for the purposes of GDPR and/or UK Data Protection Laws, if and to the extent that Service Provider acts as controller in relation to processing activities falling within the Permitted SP Purposes, Service Provider will be an independent controller and will be solely and entirely responsible for its compliance in that capacity with all applicable Data Protection Law;

B. where Service Provider acts as controller for purposes of GDPR and/or UK Data Protection Laws, the Parties shall enter into EU Standard Contractual Clauses (Module One: Transfers Controller to Controller) and UK Privacy Addendum, in each case validly completed and executed, to ensure that

any actual or deemed transfer of Personal Data from Cintas to Service Provider is in all respects lawful; and

C. to the extent Service Provider receives, or Service Provider creates, Deidentified data in connection with this Privacy Addendum: (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 Cintas as a source of such data; and (iv) contractually obligate any third parties receiving such information from Service Provider to also commit to (i), (ii), and (iii).

c. Subprocessors.

i. Subprocessors shall only be considered Authorized Personnel, and not an Unauthorized Third Party, if:

A. the subprocessor, including name, location, and contact information for the person responsible for data and privacy compliance, has been provided to Cintas and Cintas is given an opportunity to object within 14 days after Service Provider supplies Cintas with such information regarding such subprocessor after the effective date of this Privacy Addendum;

B. Service Provider enters into a written contract with the subprocessor that contains terms substantially the same as those set out in this Privacy Addendum and, upon Cintas' written request, provides Cintas with copies of such contracts;

C. Service Provider maintains control over all Personal Data it entrusts to the subprocessor;

D. the subprocessor's contract, as it relates to Personal Data hereunder, terminates automatically on termination of this Privacy Addendum for any reason; and

E. to the extent that the CPRA applies to the processing under this Privacy Addendum, the subprocessor shall agree to: comply with the applicable obligations of the CPRA; provide the same level of privacy protection as is required under the CPRA; permit Cintas to ensure that the subprocessor is processing Personal Data as set forth herein and under the CPRA and stop and remediate unauthorized use of personal data by the subprocessor; and notify Cintas if it can no longer meet its obligations under the CPRA.

ii. Upon Cintas' written request, Service Provider will audit a subprocessor's compliance with its obligations regarding Cintas' Personal Data and provide Cintas with the audit results.

d. Complaints, Privacy Rights Requests, and Third-Party Rights.

i. Service Provider must notify Cintas immediately if it receives any complaint, notice, or communication that directly or indirectly relates to the Personal Data processing or to either party's compliance with Data Protection Laws.

ii. Service Provider must notify Cintas within three (3) days if it receives a request from a Data Subject to exercise any rights the individual may have regarding their Personal Data, such as access or deletion.

iii. Service Provider shall not respond to any PRR relating to Cintas except that it shall respond that it cannot act upon requests made to it as to data it processes as a service provider/processor, unless and until instructed to do so by Cintas or unless required to do so by applicable law.

iv. Service Provider will give Cintas its full cooperation and assistance in responding to any complaint, notice, communication, or PRR to ensure Cintas is compliant with its obligation to respond to PRRs, including but not limited to, notifying Service Provider's subprocessors to delete Personal Data in response to a PRR made to Cintas.

v. If Cintas requests information from Service Provider to fulfill its obligation to respond to PRR, Service Provider shall provide the requested information without undue delay, and in any event within seventy-two (72) hours of Cintas' request for assistance. Service Provider shall notify Cintas immediately if Service Provider is unable to comply with the request for assistance. Such notification shall provide a detailed explanation as to why Service Provider considers compliance with such request for assistance to be impossible.

vi. Service Provider shall comply with any PRR regarding the deletion of an individual's Personal Data. Upon direction from Cintas to execute a deletion request, Service Provider shall delete the Personal Data in question within thirty (30) days. If Service Provider is unable to delete such Personal Data by the aforementioned deadline, it shall promptly notify Cintas in writing.

vii. Service Provider must not disclose the Personal Data to any Data Subject or to a third party unless the disclosure is either at Cintas' request or instruction, permitted by this Privacy Addendum, or is otherwise required by applicable law.

viii. Service Provider shall provide Cintas with any Personal Data that it processes on Cintas' behalf in a structured, commonly used, electronic, and machine-readable format or in such format as otherwise requested by Cintas.

e. Processing for Cross-Contextual Behavioral Advertising ("CCBA").

i. To the extent that the Services involve processing Personal Data for CCBA ("CCBA Services"), Cintas acknowledges that Service Provider will not qualify as a service provider or contractor under the CCPA/CPRA. Accordingly, with respect to such CCBA Services it is understood that Service Provider will not act as to maintain its status as a service provider or a contractor. In addition, the following terms and conditions apply to such services and processing, and to services that involve processing for purposes of targeted advertising:

ii. Cintas shall:

A. not provide Personal Data to Service Provider for CCBA Services that has been subject to a Data Subject's "Do Not Sell," "Do Not Share," or an opt-out of targeted advertising request provided to Cintas;

B. if it receives a "Do Not Sell," "Do Not Share," or an opt-out of targeted advertising request with respect to Personal Data that it has already provided to Service Provider for processing, provide prompt notice to Service Provider to remove such Personal Data from Service Provider's systems (except for record keeping services); and

C. if the Services involve collection of Personal Data from Cintas' website (or other online property), by a cookie, pixel or otherwise, Cintas shall provide users all necessary notices and manage all necessary user consents (opt-in or opt-out) to enable Service Provider to do so for the CCBA and targeted advertising services, consistent with Data Protection Law.

iii. Service Provider shall, in addition to the other obligations set forth in this Privacy Addendum:

A. restrict processing to providing the Services;

B. comply with Data Protection Laws in performing the Services, including but not limited to, complying with a PRR to opt out of sale or sharing forwarded to it by Cintas; and

C. if Service Provider is permitted to collect Personal Data from Cintas' website (or other online service), Service Provider shall check for and comply with a Data Subject's opt-out preference signal, to the extent made available to Service Provider by Cintas, unless informed by Cintas that the Data Subject has consented to the sharing of their Personal Data for the Services.

4. **Cross-Border Transfers of Personal Data – Controller to Processor Basis.**

a. For data transfers from the EEA/UK to Third Countries, to the extent such transfers are subject to GDPR (including the UK GDPR) and/or the Swiss DPA, the Parties hereby incorporate the EU Standard Contractual Clauses, UK Privacy Addendum, and/or Swiss Privacy Addendum as follows:

b. EU Data Transfers.

i. The Parties hereby incorporate the EU Standard Contractual Clauses (Module 2: Transfers Controller to Processor) by reference and as a safeguard for the transfer of personal data to a Third Country. The EU Standard Contractual Clauses (Module 2: Transfers Controller to Processor) will be deemed completed as follows:

ii. Clause 7 (Optional – Docking Clause) shall be deemed incorporated;

iii. Clause 9(a): General Written Authorisation and 10 business days;

iv. For purposes of Clause 11 (Redress), the Parties agree that the optional wording shall not be incorporated herein and therefore shall not be applicable to the Parties;

v. For purposes of Clause 17 (Governing law), the Parties agree that the EU Standard Contractual Clauses (Module 2: Transfers Controller to Processor) shall be governed by the laws of Ireland and select Clause 17, "Option 1" to this effect;

vi. For purposes of Clause 18 (Choice of forum and jurisdiction), the Parties agree that any dispute arising from the EU Standard Contractual Clauses (Module 2: Transfers Controller to Processor) shall be resolved by the Courts of Ireland;

vii. Annexes I, II, and III of the EU Standard Contractual Clauses (Module 2: Transfers Controller to Processor) shall be deemed completed with the information set out in the Schedule 2 to this Privacy Addendum, the contents of which are hereby agreed by the Parties; and

viii. For the purposes of Annex I.C., the competent supervisory authority is the data protection authority of Ireland.

c. UK Data Transfers:

i. For the transfer of personal data governed by the UK Data Protection Laws to Third Countries, the Parties hereby incorporate by reference the UK Privacy Addendum, which incorporates the EU Standard Contractual Clauses (Module 2: Transfers Controller to Processor). The UK Privacy Addendum will be deemed completed as follows:

ii. Table 1 shall be deemed completed with the information set out in the Processing Appendix 1 within Schedule 1, the contents of which are hereby agreed by the Parties;

iii. In Table 2, the Parties select the checkbox that reads: "Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Privacy Addendum." The applicable Approved EU SCCs Module is number 2 (Controller to Processor) and the accompanying UK addendum Table 2 shall be deemed to be completed according to Parties preferences outlined below;

iv. Clause 7 (Optional – Docking Clause) shall be deemed incorporated;

v. Clause 9(a): General Written Authorisation and 10 business days;

vi. For purposes of Clause 11 (Redress), the Parties agree that the optional wording shall not be incorporated herein and therefore shall not be applicable to the Parties.

vii. Table 3 shall be deemed completed with the information set out in the Processing Appendix 1 within Schedule 1 as well as Schedule 2 for sub-processors, the contents of which are hereby agreed by the Parties; and

viii. In Table 4, the Parties agree that only the Exporter may end the UK Privacy Addendum as set out in Section 19 of the same.

ix. The Information Commissioner's Office ("ICO") will be the competent supervisory authority.

d. Swiss Data Transfers:

i. The FDPIC will be the competent supervisory authority;

ii. Data subjects in Switzerland may enforce their rights in Switzerland under clause 18c of the EU SCCs; and

iii. References in the EU SCCs to the EU GDPR should be understood as references to Swiss Data Protection Law insofar as the data transfers are subject to Swiss Data Protection Law.

e. Service Provider will not transfer any Personal Data to another country unless the transfer complies with Data Protection Laws, and Service Provider and Cintas execute the appropriate Standard Contractual Clauses and, to the extent necessary, cooperate to take all appropriate supplementary measures.

5. **Offshoring.** No Personal Data may be accessed, generated, hosted, downloaded, printed, stored, processed, transferred, or maintained outside of the United States by Service Provider without Cintas' prior written approval. Such approval may be withheld by Cintas for any reason in its sole discretion and/or approval may be subject to additional terms and conditions.

6. **Information Security.**

a. Service Provider shall implement and maintain a written information security program including appropriate policies, procedures, and risk assessments that are reviewed at least annually.

b. Without limiting Service Provider's obligations, Service Provider shall implement administrative, physical, and technical safeguards to protect Personal Data from unauthorized access, acquisition, or disclosure, destruction, alteration, accidental loss, misuse, or damage that are no less rigorous than accepted industry practices under the National Institute of Standards and Technology (NIST) Cybersecurity Framework, or other applicable industry standards for information security, and shall ensure that all such safeguards, including the manner in which Personal Data is processed, comply with applicable Data Protection Laws, as well as the terms and conditions of this Privacy Addendum. If, in the course of its engagement by Cintas, Service Provider has access to or will process credit, debit, or other payment cardholder information, Service Provider 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 Service Provider's sole cost and expense.

c. At a minimum, Service Provider's safeguards for the protection of Personal Data shall include: (i) limiting access of Personal Data to Authorized Personnel; (ii) securing business facilities, data centers, paper files, servers, backup systems, and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability; (iii) implementing network, 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 Highly Sensitive Personal Data stored on any media; (vii) encrypting Highly Sensitive Personal Data when transmitted; (viii) strictly segregating Personal Data from information of Service Provider or its other customers so that Personal Data is not commingled with any other types of information; (ix) conducting risk assessments, penetration testing, and vulnerability scans and promptly implementing, at Service Provider's sole cost and expense, a corrective action plan to correct any issues

that are reported as a result of the testing; (x) implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law; and (xi) providing appropriate privacy and information security training to Service Provider's employees and Authorized Personnel.

d. During the term of each Authorized Person's employment by Service Provider, Service Provider shall at all times cause such Authorized Person to abide strictly by Service Provider's obligations under this Privacy Addendum. Service Provider further agrees that it shall maintain a disciplinary process to address any unauthorized processing of Personal Data by any of Service Provider's officers, partners, principals, employees, agents, contractors or other Authorized Personnel.

7. **Security Incident Procedures.** In the event that Service Provider becomes aware of or suspects a Security Incident, Service Provider shall:

a. provide Cintas with the name and contact information for one or more employees of Service Provider who shall serve as Cintas' primary contact and shall be available to assist Cintas 24 hours per day, seven days per week as a contact in resolving obligations associated with a Security Incident;

b. notify Cintas of a Security Incident as soon as practicable, but no later than 24 hours after Service Provider becomes aware of it. Such initial notice to Company will describe: (i) the nature of the Security Incident, including, where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned; (ii) the likely consequences of the Security Incident; and (iii) the measures taken or proposed to be taken by Service Provider to address the Security Incident, including, where appropriate, measures to mitigate its possible adverse effects. To the extent it is not possible to provide the foregoing information at the same time, the information may be provided in phases without undue further delay;

c. notify Cintas of any Security Incidents by telephone at 1-844-378-7411 or by emailing Cintas at privacy@cintas.com with a copy by email to Service Provider's primary business contact within Cintas;

d. cooperate with Cintas in Cintas' handling of the Security Incident, including, without limitation: (i) assisting with any investigation; (ii) providing Cintas with physical access to the facilities and operations affected; (iii) facilitating interviews with Service Provider's employees, Authorized Personnel and others involved in the matter; (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 reasonably required by Cintas; and (v) in any litigation, investigation, or other action deemed necessary by Cintas to protect its rights relating to the use, disclosure, protection, and maintenance of Personal Data.

e. at its own expense use best efforts to immediately contain and remedy any Security Incident and prevent any further Security Incident, including, but not limited to taking any and all action necessary to comply with applicable privacy rights, laws, regulations, and standards;

f. be responsible to Cintas for all actual costs and expenses incurred by Cintas in responding to, and mitigating damages caused by, any Security Incident, including, without limitation, all costs of notice and/or remediation as set forth in this Section, attorneys' fees and costs, and credit monitoring and/or identity restoration services, all as determined in Cintas' discretion and all of which, for the avoidance of doubt, constitute direct damages, and any limitation of liability set forth in the Agreement will not apply to this Section;

g. not inform any third party of any Security Incident without first obtaining Cintas' prior written consent, other than to inform a complainant that the matter has been forwarded to legal counsel;

h. agree that Cintas shall have the sole right to determine: (i) whether notice of the Security Incident 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 Cintas' discretion; and

i. 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.

j. maintain and preserve all documents, records, and other data related to any Security Incident.

k. Promptly use its best efforts to prevent a recurrence of any such Security Incident.

8. **Audits and Assessments**. Upon Cintas' written request, to confirm Service Provider's compliance with this Agreement, as well as Data Protection Laws and any other applicable laws, regulations, and industry standards, Service Provider grants Cintas or, upon Cintas' election, a third party on Cintas' behalf, permission to perform an assessment, audit, examination, or review of all controls in Service Provider's physical and/or technical environment in relation to all Personal Data being handled and/or the Services being provided to Cintas pursuant to the Agreement. Service Provider shall fully cooperate with such assessment by providing access to knowledgeable personnel, physical premises, documentation, infrastructure, and application software that processes, stores, or transports Personal Data for Cintas pursuant to the Agreement. In its sole discretion and in lieu of or in addition to an on-site audit, Cintas may elect to provide, and Service Provider agrees to accurately and promptly complete, a written data privacy and information security questionnaire regarding Service Provider's business practices and information technology environment in relation to all Personal Data being handled and/or the Services being provided by Service Provider to Cintas pursuant to the Agreement. Service Provider shall fully cooperate with such inquiries. In addition, upon Cintas' request, Service Provider shall provide Cintas with the results of any audit by or on behalf of Service Provider performed that assesses the effectiveness of Service Provider's information security program as relevant to the security and confidentiality of Personal Data shared during the course of the Agreement, which may include, without limitation, all of the following, as applicable: Service Provider's latest Payment Card Industry (PCI) Compliance Report, Statement on Standards for Attestation Engagements (SSAE) No. 18 audit reports for Reporting on Controls at a Service Organization, Service Organization Controls (SOC) Type 1, 2, or 3 audit reports, and any reports relating to its ISO/IEC 27001 certification. Service Provider will promptly address any issues, concerns, or exceptions noted in the audit reports with the development and implementation of a corrective action plan by Service Provider's management.

9. **Return or Destruction of Personal Data**. At any time during the term of the Agreement at Cintas' request or upon the termination or expiration of the Agreement or this Privacy Addendum for any reason, Service Provider shall, and shall instruct all Authorized Personnel to, promptly return to Cintas all copies, whether in written, electronic, or other form or media, of Personal Data in its possession or the possession of such Authorized Personnel, or securely dispose of all such copies, and certify in writing to Cintas that such Personal Data has been returned to Cintas or disposed of securely within 30 days of doing so. Service Provider shall comply with all directions provided by Cintas with respect to the return or disposal of Personal Data. Immediately after the deletion of Personal Data, Service Provider shall provide to Cintas certified written confirmation of such secure deletion. If any law or regulation requires Service Provider to retain any documents or materials that Service Provider would otherwise be required to return or destroy, it will notify Cintas in writing of that retention requirement, giving details of the documents or

materials that it must retain, the legal basis for retention, and establishing a specific timeline for destruction once the retention requirement ends. Service Provider may only use this retained Personal Data for the required retention reason or audit purposes.

10. **Records**. Service Provider will keep detailed, accurate, and up-to-date records regarding all its processing of Personal Data for Cintas, including but not limited to, the access, control, and security of the Personal Data, approved subprocessors and affiliates, the processing purposes, and any other records required by Data Protection Laws ("Records"). Service Provider will ensure that the Records are sufficient to enable Cintas to verify Service Provider's compliance with its obligations under this Privacy Addendum. Service Provider will follow all instructions provided to it by Cintas concerning Record retention and destruction, and will reasonably assist with any and all Cintas recordkeeping requirements. Service Provider must review the information listed in the Appendices to this Privacy Addendum at least once annually to confirm its current accuracy and update it when required to reflect current practices.

11. **Equitable Relief**. Service Provider acknowledges that any breach of its covenants or obligations set forth in Privacy Addendum may cause Cintas irreparable harm for which monetary damages would not be adequate compensation and agrees that, in the event of such breach or threatened breach, Cintas is entitled to seek equitable relief, including a restraining order, injunctive relief, specific performance, and any other relief that may be available from any court, in addition to any other remedy to which Cintas may be entitled at law or in equity. Such remedies shall not be deemed to be exclusive but shall be in addition to all other remedies available at law or in equity, subject to any express exclusions or limitations in this Privacy Addendum to the contrary.

12. **Term and Termination.**

a. This Privacy Addendum will remain in full force and effect so long as the Agreement remains in effect, or Service Provider retains any Personal Data relating to the Agreement in its possession or control. Any provision of this Privacy Addendum that expressly or by implication should come into or continue in force on or after termination of the Agreement in order to protect Personal Data will remain in full force and effect.

b. Service Provider's failure to comply with any of the provisions of this Privacy Addendum is a material breach of this Privacy Addendum and the Agreement. In such event, Cintas may terminate the Agreement effective immediately upon written notice to Service Provider without further liability or obligation to Service Provider.

c. If a change in any Data Protection Laws prevents either party from fulfilling all or part of its obligations under the Agreement or this Privacy Addendum, the parties will suspend the processing of Personal Data until that processing complies with the new requirements. If the parties are unable to bring the processing into compliance with the Data Protection Laws within thirty (30) days, they may terminate the Agreement upon written notice to the other party.

13. **Indemnification**. Service Provider shall defend, indemnify, and hold harmless Cintas and its parents, subsidiaries, affiliates, and their respective officers, directors, employees, agents, successors, and permitted assigns (each, a "Cintas Indemnitee") from and against all losses, damages, liabilities, deficiencies, actions, judgments, interest, awards, penalties, fines, costs, or expenses of whatever kind, including reasonable attorneys' fees, the cost of enforcing any right to indemnification hereunder, and the cost of pursuing any insurance providers, arising out of or resulting from any third-party claim, investigation, or proceeding, including without limitation, administrative or regulatory actions, against any Cintas Indemnitee arising out of or resulting from a Security Incident, a violation of Data Protection Law, and/or Service Provider's and/or Authorized Personnel's breach of and/or failure to comply with any of its

obligations under this Privacy Addendum. Any limitation of liability set forth in the Agreement will not apply to this Section.

14. **Insurance**. During the term of the Privacy Addendum, Service Provider must, at its own cost and expense, obtain and maintain insurance, in full force and effect, sufficient to cover Service Provider's potential indemnity or reimbursement obligations under this Privacy Addendum, and at no less than the following limits:

Each Occurrence: $5 Million

General Aggregate: $5 Million (which may be met by use of an umbrella policy)

a. The required insurance shall be provided by insurance companies of recognized standing and authorized to do business in the jurisdictions where operations are to be performed. All such policies of insurance of Service Provider shall provide that the same shall not be canceled nor the coverage materially modified without first giving 30 days prior written notice thereof to Cintas. No such cancellation or material modification shall affect Service Provider's obligation to maintain the insurance coverage required by the Privacy Addendum. Service Provider shall name Cintas as an additional insured on all policies, with the exception of workers' compensation insurance policies, if any. All liability insurance policies shall be written on an "occurrence" policy form, unless otherwise agreed in writing. Cintas shall be named as loss payee as its interest may appear on any property insurance policies of Service Provider. Service Provider shall be responsible for payment of any and all deductibles, self-insured retentions, and self-insurance carried by Service Provider under its insurance program(s). The coverage afforded under any insurance policy obtained by Service Provider pursuant to the Agreement shall be primary with respect to Service Provider's acts or omissions and not be in excess of, or contributing with, any insurance maintained by Cintas and its assigns. Service Provider shall not perform under the Agreement without the prerequisite insurance. Unless previously agreed to in writing by Cintas, Service Provider shall comply with the insurance requirements herein. If Service Provider fails to comply with any of the insurance requirements herein, upon written notice to Service Provider by Cintas and a 10-day cure period, Cintas shall have the right, but not the obligation, to provide or maintain any such insurance, and to deduct the cost thereof, plus a reasonable administrative fee as designated by Cintas, from any amounts due and payable to Service Provider under the Agreement, or, in the event there are no such amounts due and payable, Service Provider shall reimburse Cintas for such costs on demand.

b. The Parties do not intend to shift all risk of loss to insurance. The naming of Cintas as additional insured is not intended to be a limitation of Service Provider's liability and shall in no event be deemed to, or serve to, limit Service Provider's liability to Cintas to available insurance coverage, nor to limit Cintas' rights to exercise any and all remedies available to Cintas under contract, at law or in equity.

15. **Business Continuity; Disaster Recovery**. Service Provider has in place, and will at all times maintain, a business continuity program and a disaster recovery program that provide appropriate means and procedures to allow for continued operations in the case of system failures or disaster conditions, and provide appropriate mechanisms and procedures for the secure treatment of Personal Data in a manner consistent with the protections of this Privacy Addendum.

16. **Survival**. This Privacy Addendum shall survive termination of the Agreement and shall continue in force as long as Service Provider possesses or processes any Personal Data (or excerpt, summary, copy or extract thereof), or for a period of five (5) years after termination of the Agreement, whichever period is longer.

17. **Hierarchy**. In the event of inconsistencies between the provisions of this Privacy Addendum and the SCCs or the Agreement, the order of priority shall be as follows: (a) the SCCs; (b) this Privacy Addendum; (c) any other data processing agreements or obligations between the Parties that apply

to the Services; and (d) the Agreement (except to the extent this Privacy Addendum is referenced and explicitly superseded).

18. **Cooperation**. Service Provider will promptly cooperate with requests by Cintas to facilitate the processing of Personal Data and to ensure Cintas' compliance with its obligations under the Data Protection Law, including by way of example: (i) maintaining and providing Cintas with a complete, accurate, and up-to-date written record of categories of processing activities carried out on behalf of Company; (ii) providing assistance to Cintas in carrying out a privacy impact assessment; and (iii) providing assistance to Cintas in consulting a supervisory authority in relation to privacy impact assessments. To the extent that Cintas is subject to or involved in an investigation by a governmental authority or litigation arising out of or related to a Security Incident, Service Provider will provide full cooperation to Cintas in responding to such event.

19. **New Privacy Laws**. The parties understand that various countries, states and provinces are actively considering enacting other laws or amending existing Data Protection Laws, which may conflict with, preempt, and/or place additional regulations on current Data Protection Laws ("New Privacy Laws"). Service Provider agrees that it will work in good faith with Cintas to ensure any sharing of Personal Data between the parties is done in compliance with New Privacy Laws. The parties further agree that should any specific Data Protection Law be preempted, invalidated, or cease to be effective, this Privacy Addendum shall continue to survive with respect to each party's rights and obligations under other Data Protection Laws.

SCHEDULE 1

Processing Schedule

Personal Data Processing Purposes and Details

Business Purposes: *Providing the Services, as described in the Agreement*.

Personal Data Categories: ***[To be completed by Service Provider]***

Data Subject Types: *Cintas employees, contractors, and/or candidates (Cintas personnel), Cintas' customer personnel, and other business-to-business contacts*.

Processing Duration: *For the duration of the Agreement, or retain it as otherwise required under applicable law*.

Countries where the Provider may receive, access, transfer or store Personal Data: *The United States of America, Canada, and/or Switzerland*.

SCHEDULE 2

Processing Appendices

ANNEX I

A. **LIST OF PARTIES**

Data Exporter (s) – Identification and contact details	**Capacity of Data Exporter(s)**	**Data Importer(s) – Identification and contact details**	**Capacity of Data Importer(s)**	**Competent Supervisory Authority**
Cintas, as identified in the underlying Agreement	Controller	Service Provider, as identified in the underlying Agreement	Processor	Ireland for EU transfers; the FDPIC for Swiss transfers; the ICO for UK transfers

B. **DESCRIPTION OF THE TRANSFER**

1. Categories of data subjects whose personal data is transferred: *Cintas employees, contractors, and/or candidates (Cintas personnel), Cintas' customer personnel, and other business-to-business contacts.*

2. Categories of personal data transferred: ***[To be completed by Service Provider]***.

3. Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures: *Not applicable.*

4. The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): *Continuous.*

5. Nature of the processing (i.e., processing operations): *Providing the Services, as described in the Agreement.*

6. Purpose(s) of the data transfer and further processing: *Providing the Services, as described in the Agreement.*

7. The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: *Service Provider will retain Personal Data for the duration of the Agreement, or as otherwise required under applicable law.*

8. For transfers to (sub-) processors, also specify subject matter, nature, and duration of the processing: *Service Provider will engage subprocessors as agreed by the parties in this Privacy Addendum.*

9. Deidentified Data: *Service Provider shall be entitled to create Deidentified data and Aggregate Consumer Information as defined by Data Protection Laws and use such data for its own purposes, subject to Service Provider obligations as set forth in this Privacy Addendum. Notwithstanding the foregoing, with respect to Personal Data for which processing is subject to the GDPR, UK GDPR, or the Swiss DPA, such uses by Service Provider are limited to Anonymized data. Cintas has informed or will inform Data Subjects that their Personal Data is subject to Anonymization by third parties.*

C. **COMPETENT SUPERVISORY AUTHORITY**

The Supervisory Authority of Ireland for EU transfers; the FDPIC for Swiss transfers; and/or the ICO for UK transfers.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Service Provider has implemented and shall maintain the following technical and organizational security measures for any transfers of any Personal Data, as agreed by the parties pursuant to Section 6 of this Privacy Addendum.

ANNEX III

LIST OF PRE-APPROVED SUBPROCESSORS

Cintas has authorized the use of subprocessors of Service Provider as described in Section 3(c) of this Privacy Addendum.