Vendor Data Protection Addendum

During the course of providing Services, Vendor may obtain, access, or otherwise process Cintas Information, including Personal Information and Sensitive Personal Information from, or on behalf of, Cintas, Inc. and any affiliated entity identified in the signature pages (collectively, "**Cintas**"). Vendor agrees to protect all Cintas Information as detailed in this Data Protection Addendum ("**DPA"**).

1. DEFINITIONS. Capitalized terms used but not defined in this DPA will have the meanings set forth in the Agreement.

1.1. "**Cintas Information**" means any information owned or controlled by Cintas, in any form, format, or media (including paper, electronic, and other records), that is provided to Vendor or that Vendor has access to, obtains, uses, maintains, or otherwise handles in connection with the performance of Services.

1.2. "**Data Protection Law**" means any applicable transnational, foreign, or domestic federal, state, or local law, statute, code, ordinance, regulation, rule, consent agreement, order, injunction, judgment, decree, ruling, constitution, treaty, or other similar requirement of any governmental authority relating to the Processing of Cintas Information.

1.3. "**Personal Information**" means any Cintas Information that identifies an individual or relates to an identifiable individual or as defined by Data Protection Law.

1.4. "**Process**" or "**Processing**" means the collection, recording, organization, structuring, alteration, access, disclosure, copying, transfer, storage, deletion, retention, combination, restriction, adaptation, retrieval, consultation, destruction, disposal, sale, sharing, or other use of Cintas Information.

1.5. "**Sensitive Personal Information**" means any of the following types of Personal Information: (i) Social Security or identity card number, taxpayer identification number, passport number, driver's license number, or other government-issued identification number; (ii) credit or debit card details or financial account number, with or without any code or password that would permit access to the account including Cardholder Information or credit history; (iii) username and password; (iv) information on race, religion, ethnicity, sex life or practices or sexual orientation, medical information, health information, genetic or biometric information, biometric templates, political, religious or philosophical beliefs, political party or trade union membership, background check information, or judicial data such as criminal records or information on other judicial or administrative proceedings; (v) geolocation information accurate within a radius of 1,850 feet or less; (vi) citizenship or immigration status; (vii) information from a known child under the age of 13; or (vii) the contents of an individual's mail, email, or text messages unless Cintas or Vendor is the intended recipient of the communication.

1.6. "**Vendor Personnel**" means any Vendor's employee, contractor, subcontractor, or agent to whom Vendor authorizes to access or Process Cintas Information.

2. DATA PROCESSING AND PROTECTION

2.1. **Compliance with Law**. Vendor will comply with all Data Protection Laws applicable to Vendor's Processing of Cintas Information.

2.2. **Limitations on Use**. Vendor will Process Personal Information only (i) on Cintas' behalf; (ii) to perform the Services; and (iii) in accordance with Cintas instructions as documented, specified, and limited in the Agreement and as described in Annex I (Description of Transfer). Vendor will inform Cintas if Vendor believes that any instructions of Cintas regarding the Processing of Cintas Information would violate Data Protection Law. For clarity, and without limiting the generality of the foregoing, in no event may Vendor: (A) sell or share Personal Information (as such term is defined under Data Protection Law); (B) retain, use, or disclose Cintas Information to any third party for the commercial benefit of Vendor or any third party; (C) retain, use, disclose, or otherwise Process Cintas Information outside of its direct business relationship with Cintas or for a commercial purpose other than the business purposes specified in the Agreement and this DPA; or (D) combine Personal Information with other information that identifies, directly or indirectly, an individual or relates to an identifiable individual that Vendor receives from, or on behalf of, other persons, or collects from its own interaction with the individual separate from the Services, except to the extent

expressly permitted under the Data Protection Laws. Vendor certifies that it understands and will comply with the foregoing restrictions.

2.3. **Confidentiality**. Vendor will hold Cintas Information in strict confidence and impose confidentiality obligations on Vendor Personnel who will be provided access to, or will otherwise Process, Cintas Information, including to protect all Cintas Information in accordance with the requirements of this DPA (including during the term of their employment or engagement and thereafter).

2.4. **De-identification and Aggregation**. If Cintas permits or instructs Vendor to Process Cintas Information in de-identified, anonymized, and/or aggregated form as part of the Services, Vendor will ensure that any such Cintas Information qualifies and remains qualified as de-identified information, anonymized data, de-identified data, and/or aggregate information as defined by Data Protection Laws. Vendor will make no attempt to re-identify any individual to whom such Cintas Information relates, will publicly commit to maintaining and using such Cintas Information without attempting to re-identify it, and will take reasonable measures to prevent such re-identification.

2.5. **Information Security Program**. Vendor will implement, maintain, monitor, and, where necessary, update a comprehensive written information security program that contains appropriate administrative, technical, and physical safeguards appropriate to the nature of the Cintas Information, that are designed protect Vendor's information systems and all Cintas Information against anticipated threats or hazards to its security, confidentiality, or integrity (such as unauthorized access, collection, use, copying, modification, disposal, or disclosure; unauthorized, unlawful, or accidental loss, destruction, acquisition, or damage; or any other unauthorized form of Processing) ("**Information Security Program**"). Vendor will assist Cintas in meeting Cintas' obligations under the Data Protection Laws in relation to the security of Processing Cintas Information. The safeguards will meet or exceed prevailing industry standards or an applicable third-party security assurance standard such as ISO 27001/2, SSAE 18 SOC 2, or ISAE 3402 SOC 2. The Information Security Program will include the measures listed in the attached Annex II (Security Measures).

2.6. **Data Integrity**. Vendor will ensure that all Cintas Information created by Vendor on Cintas' behalf is accurate and, where appropriate, kept up to date, and ensure that any Cintas Information that is inaccurate or incomplete is erased or rectified in accordance with Cintas' instructions.

2.7. **Sub-processing**. Vendor will not disclose or transfer Cintas Information to, or allow access to Cintas Information by (each, a "**Disclosure**"), any third party without Cintas' express prior written consent; provided, however, that Vendor may Disclose Cintas Information to its affiliates and subcontractors for purposes of providing the Services to Cintas, subject to the following conditions: (a) Vendor will maintain a list of the affiliates and subcontractors (with contact information and location) and the processing activities to be performed in connection with such Disclosures and will provide this list to Cintas upon Cintas' request; (b) Vendor will provide Cintas with at least 30 days' prior notice of the addition of any affiliate or subcontractor to this list and the opportunity to object to such addition(s); and (c) if Cintas makes such an objection on reasonable grounds and Vendor is unable to modify the Services to prevent Disclosure of Cintas Information to the additional affiliate or subcontractor, Cintas will have the right to terminate the relevant Processing. If Cintas does not object to an added third party, the new third party will be considered an "**Authorized Subprocessor**." Vendor will, prior to any Disclosure, enter into an agreement with such third party that is at least as restrictive as this DPA. The agreement will be provided to Cintas promptly upon request. Vendor will be liable for all actions by such third parties with respect to the Disclosure.

2.8. **Requests or Complaints**. Vendor will promptly notify Cintas in writing, and in any case within five (5) business days of receipt, unless specifically prohibited by applicable law, if Vendor or any Authorized Sub-processor receives: (i) any requests from an individual with respect to Personal Information Processed, including, but not limited to, opt-out requests; requests for access and/or rectification, erasure, or restriction; requests for data portability and all similar requests; or (ii) any complaint relating to the Processing of Cintas Information, including allegations that the Processing infringes on an individual's rights. Vendor will not respond to any such request or complaint except to redirect individual to Cintas and/or inform individual that his/her request was redirected to Cintas unless expressly authorized to do so by Cintas. Vendor will cooperate with Cintas with respect to any action taken relating to an individual's request or complaint and will seek to implement appropriate processes (including technical and organizational measures) to assist

Cintas in responding to such requests or complaints. Vendor will promptly and securely delete or destroy any Personal Information pertaining to an individual identified by Cintas where such information is within Vendor's possession or control. If applicable, Vendor will direct any Authorized Subprocessor that Processes Personal Information related to the identified individual to promptly and securely delete or destroy such Personal Information. Vendor will confirm to Cintas in writing that it has complied with its obligations under this section.

2.9. **Production Requests**. If Vendor receives any order, demand, warrant, or any other document requesting or purporting to compel the production of Cintas Information (including, for example, by oral questions, interrogatories, requests for information or documents in legal proceedings, subpoenas, civil or criminal investigative demands, or other similar processes) by any competent authority ("**Production Request**"), Vendor will immediately notify Cintas (except to the extent prohibited by applicable law). Vendor will provide Cintas with at least forty-eight (48) hours' notice prior to the required disclosure, so that Cintas may, at its own expense, exercise such rights as it may have under law to prevent or limit such disclosure. Notwithstanding the foregoing, Vendor will exercise commercially reasonable efforts to prevent and limit any such disclosure and to otherwise preserve the confidentiality of Cintas Information and will cooperate with Cintas with respect to any action taken relating to such request, complaint, order, or other document, including to obtain an appropriate protective order or other reliable assurance that confidential treatment will be accorded to Cintas Information.

2.10. **Audit**. Upon Cintas' written request, to confirm Vendor's compliance with this DPA, as well as Data Protection Laws and any other applicable laws, regulations, and industry standards, Vendor 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 Vendor's physical and/or technical environment in relation to all Cintas Information being handled and/or the Services being provided to Cintas pursuant to the Agreement. Vendor shall fully cooperate with such assessment by providing access to knowledgeable personnel, physical premises, documentation, infrastructure, and application software that process, store, or transport Cintas Information 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 Vendor agrees to accurately and promptly complete, a written data privacy and information security questionnaire regarding Vendor's business practices and information technology environment in relation to all Cintas Information being handled and/or the Services being provided by Vendor to Cintas pursuant to the Agreement. Vendor shall fully cooperate with such inquiries. In addition, upon Cintas' request, Vendor shall provide Cintas with the results of any audit by or on behalf of Vendor performed that assesses the effectiveness of Vendor's information security program as relevant to the security and confidentiality of Cintas Information shared during the course of the Agreement, which may include, without limitation, all of the following, as applicable: Vendor'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. Vendor will promptly address any issues, concerns, or exceptions noted in the audit reports with the development and implementation of a corrective action plan by Vendor's management.

2.11. **Regulatory Investigations**. Upon notice to Vendor, Vendor will assist and support Cintas in in connection with requests from Cintas customers and law enforcement bodies, regulators, or data protection authorities, including in the event of an investigation, if and to the extent such request relates to Cintas Information handled by Vendor on behalf of Cintas in accordance with this DPA. Such assistance will be at Cintas' sole expense, except where investigation was required due to Vendor's acts or omissions, in which case, such assistance will be at Vendor's sole expense.

2.12. **Security Incident**.

a) Vendor will notify Cintas in writing by emailing NotifySecurity@cintas.com and by telephone at 1-844-378-7411 promptly (and in any event within seventy-two (72) hours) whenever Vendor reasonably believes that there has been any accidental or unauthorized access, acquisition, use, modification, disclosure, loss, destruction of, or damage to Cintas Information or any other unauthorized Processing of Cintas Information (each, a "**Security Incident**"). Vendor will provide Cintas with information regarding (i) the nature of the Security Incident; (ii) the number of individuals affected, the number of records affected, and the types of records affected; (iii) the likely consequences of the Security Incident;

and (iv) the measures taken or proposed to be taken to address the Security Incident, including measures to terminate unauthorized access or mitigate possible adverse effects of the Security Incident.

b) After providing notice, Vendor will investigate the Security Incident, take all necessary steps to eliminate or contain the exposure of the Cintas Information, and keep Cintas informed of the status and cause of the Security Incident and all related matters. Vendor further agrees to provide reasonable assistance and cooperation requested by Cintas and/or Cintas' designated representatives in the furtherance of any correction, remediation, investigation, or recording of any Security Incident and/or the mitigation of any potential damage, including any notification that Cintas may determine appropriate to send to affected individuals, regulators, or third parties, and/or the provision of any credit reporting service that Cintas deems appropriate to provide to affected individuals.

c) Unless required by law applicable to Vendor, Vendor will not notify any individual or any third party other than law enforcement of any potential Security Incident involving Cintas Information without first obtaining written permission of Cintas.

d) In addition, within thirty (30) days of identifying or being informed of any Security Incident arising from any act or omission by Vendor, Vendor will develop and execute a plan, subject to Cintas' approval, that reduces the likelihood of a recurrence of a Security Incident.

e) 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, Vendor will provide full cooperation to Cintas in responding to such event.

f) To the extent the Security Incident resulted from a violation of Vendor's duties under this DPA or the Agreement, Vendor will (i) assist with curing any alleged violation and ensure that no further violations shall occur; (ii) provide Cintas with a written statement confirming such cure and no further violations; and (iii) be responsible to Cintas for all actual costs and expenses incurred by Cintas in responding to and mitigating damages caused by any Security Incident, which, for the avoidance of doubt, constitute direct damages, and any limitation of liability set forth in the Agreement will not apply.

2.13. **Cardholder Information**. For purposes of this DPA, "**Cardholder Information**" means any Cintas Information that includes: (i) with respect to a payment card, the account holder's name, account number, service code, card validation code/value, PIN or PIN block, valid to and from dates, and magnetic stripe data; and (ii) information relating to a payment card transaction that is identifiable with a specific account. If Vendor has access to Cardholder Information, Vendor must at all times comply with the security standards for the protection of Cardholder Information with which payment card companies require merchants to comply, including, but not limited to, the Payment Card Industry Data Security Standards currently in effect and as may be updated from time to time ("**PCI Standards**"). Vendor will promptly provide, at Cintas' request, current certification of compliance with the PCI Standards by an authority recognized by the payment card industry for that purpose. If, during the term of any relevant agreement (including, for the avoidance of doubt, this DPA), Vendor undergoes, or has reason to believe that it will undergo, an adverse change in its certification or compliance status with the PCI Standards, Vendor will promptly notify Cintas of such circumstances. Vendor will not take any actions that will compromise Cintas' ability to comply with the PCI Standards.

2.14. **Return or Disposal**. Vendor will, as appropriate and as directed by Cintas, regularly dispose of Cintas Information that is maintained by Vendor but that is no longer necessary to provide the Services. Upon termination or expiration of this DPA for any reason or at any time, upon Cintas' request, Vendor will immediately cease handling Cintas Information and will return such Cintas Information in a manner and format reasonably requested by Cintas or, if specifically directed by Cintas, will destroy any or all Cintas Information in Vendor's possession, power, or control. If Vendor disposes of any paper, electronic, or other record containing Cintas Information, Vendor will do so by taking all reasonable steps (based on the sensitivity of Cintas Information) to destroy Cintas Information by: (i) shredding; (ii) permanently erasing and deleting; (iii) degaussing; or (iv) otherwise modifying Cintas Information in such records to make it unreadable, unreconstructable, and indecipherable. Upon request, Vendor will provide a written certification that Cintas Information has been returned or securely destroyed in accordance with this DPA. If Vendor is required to retain any Cintas Information to comply with a legal requirement. Vendor is permitted to retain

one copy of the foregoing materials, as required, provided that any such copy is encrypted, is not used or accessed for any other purpose, is protected in accordance with the requirements of this DPA, and is promptly destroyed in accordance with this section if no longer required to be retained by law.

2.15. **Cooperation**. Upon Cintas' request, Vendor will provide assistance and all information in its possession necessary to demonstrate Vendor's compliance with its obligations under this DPA and the Data Protection Laws and assist Cintas in meeting its obligations under Data Protection Laws, including: (i) registration and notification obligations; (ii) accountability; (iii) ensuring the security of Cintas Information; (iv) establishment and maintenance of a record of Cintas Information processing; and (v) conducting and documenting privacy and data protection impact assessments and related consultations of data protection authorities.

2.16. **Adverse Changes**. Vendor will notify Cintas in writing promptly if Vendor: (i) has reason to believe it is not or will not be able to comply with any of its obligations under the Data Protection Laws or this DPA; or (ii) becomes aware of any circumstances or change in law that is likely to prevent it from fulfilling its obligations under this DPA. Cintas has the right, upon providing notice to Vendor, to take reasonable and appropriate steps to stop and remediate unauthorized Processing of Cintas Information, including where Vendor has notified Cintas that it can no longer meet its obligations under the Data Protection Laws. In the event that 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 law applicable to each party, the parties will negotiate in good faith upon an appropriate amendment to this DPA.

3. PROCESSING LOCATIONS

3.1. **Vendor Locations**. Personal Information will be transferred to and/or accessed from the jurisdiction(s) specified in Annex I ("**Vendor Locations**"). Vendor will not transfer, or participate in any transfer of, Personal Information to any other jurisdictions without the prior written consent of Cintas. To the extent that Cintas consents to such transfer, Vendor represents and warrants that any transfer of Personal Information will comply with applicable Data Protection Law.

4. MISCELLANEOUS

4.1. **Indemnification**. Vendor agrees to indemnify, keep indemnified, hold harmless, and, upon Cintas' request, defend Cintas and its directors, officers, employees, shareholders, and agents from and against any and all damages, liabilities, expenses, claims, fines, and losses of any type, including, without limitation, reasonable attorneys' fees in connection with, arising out of, or relating to, in whole or in part, Vendor's failure (or the failure of any employee, contractor, or agent of Vendor) to comply with the obligations concerning information security or protection of Cintas Information under this DPA.

4.2. **Survival**. The obligations of Vendor under this DPA will continue for as long as Vendor continues to have access to, is in possession or control of, or acquires Cintas Information, or for a period of five (5) years after termination of the Agreement, whichever period is longer.

4.3. **Conflicts**. To the extent the terms of the DPA conflict with any Agreement between the parties with regard to the Processing of Cintas Information, the terms of the DPA will prevail.

Annex I – Description of Transfer

Personal Information Details	
1. Categories of Data Subjects	See terms of the Agreement.
2. Categories of Personal Information	See terms of the Agreement.
3. Sensitive Personal Information and applied safeguards	See terms of the Agreement.
4. The frequency of any transfer	Continuous for the term of the contract.
5. Nature of the Processing	See terms of the Agreement.
6. Processing Purposes	See terms of the Agreement.
7. Personal Information retention	Retention will be for the length of the Agreement or in accordance with Cintas' instructions.
8. For Sub-processors, also specify subject matter, nature, and duration of the Processing	Same as described in the Agreement for the processor.
9. Vendor Locations	See terms of the Agreement.

Annex II – Security Measures

Vendor maintains and enforces various policies, standards, and processes designed to secure Cintas Information and other data to which Vendor Personnel are provided access and to protect Cintas Information and other data from accidental loss or destruction. This Annex represents the minimum security measures that will be taken by Vendor. If any commercial agreement with Vendor requires a higher level or more extensive security measures, Vendor will abide by those terms. Where applicable, Vendor will comply with Section 880 of the John S. McCain National Defense Authorization Act and will not leverage prohibited technologies from associated vendors.

1. **Information Security Policies and Standards**. Vendor will implement security requirements for Vendor Personnel or agents who have access to Cintas Information that are designed to ensure a level of security appropriate to the risk and address the requirements detailed in this Annex.
   - Vendor will conduct periodic risk assessments and review and, as appropriate, revise its information security practices at least annually or whenever there is a material change in Vendor's business practices that may reasonably affect the security, confidentiality, or integrity of Cintas Information, provided that Vendor will not modify its information security practices in a manner that will weaken or compromise the confidentiality, availability, or integrity of Cintas Information.
   - Vendor will conduct security assessments and/or internal audits, including in the form of technical scans, testing of information systems, networks, and applications at planned intervals, at least annually, to verify compliance with organizational security policies and standards. Vendor will leverage an internationally recognized standard framework to assess its security posture and data security practices. Vendor must promptly correct any noncompliance issues identified during the security assessment process.
   - Vendor will maintain documented change management procedures that provide a consistent approach for controlling and identifying configuration changes for information systems, network devices, and applications.
   - If services involve the processing of payment card information, Vendor will maintain compliance with the current version of the Data Security Standards (DSS) from the Payment Card Industry Security Standards Council (PCI SSC) for the duration of the services provided. Upon request, Vendor will provide the most recent PCI "Attestation of Compliance" (AoC) report to Cintas.

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

3. **Organizational Security.**
   - Vendor will maintain an inventory of assets that includes all business-critical information systems and information processing sites that are used in the delivery of services to Cintas. The asset inventory should be accurate, up to date and have owners assigned to each asset.
   - When media are to be disposed of or reused, Vendor will implement procedures to prevent any subsequent retrieval of any Cintas Information stored on the media before they are withdrawn from the inventory. When media are to leave the premises at which the files are located as a result of maintenance operations, procedures will be implemented to prevent undue retrieval of Cintas Information stored on them.
   - Vendor will implement security policies and procedures to classify sensitive information assets, clarify security responsibilities, and promote awareness for employees.
   - All Cintas Information security incidents are managed in accordance with appropriate and documented information security and incident response procedures that enable the effective and orderly management of security incidents. The procedures must cover the reporting, analysis, monitoring and resolution of security incidents. Security incidents should be handled by a dedicated security incident response team or personnel who are trained in handling and assessing security incidents to ensure appropriate procedures are followed for the identification, collection, acquisition, and preservation of information.
   - Vendor will encrypt, using industry-standard encryption tools, using AES-256-bit or higher encryption, all Cintas Information that Vendor: (i) transmits or sends wirelessly or across public networks; (ii) stores at rest, including on laptops, mobile devices, or storage media; and (iii) stores on portable devices. Vendor will safeguard the security and confidentiality of all encryption keys associated with encrypted Cintas Information.
   - Vendor will ensure (i) that Cintas Information cannot be read, copied, modified, or deleted without authorization during electronic transmission, transport, or storage; and (ii) that the target entities for any transfer of Cintas Information by means of data transmission facilities can be established and verified.
   - Vendor will ensure that Cintas Information collected for different purposes can be processed separately.
   - Vendor must not use Cintas Information from production systems for development, testing, or staging purposes. Any use of Cintas Information for artificial intelligence models or training purposes is strictly prohibited unless expressly authorized by Cintas in a separate agreement.

4. **Network Security**.
   - Vendor maintains network security using commercially available equipment and industry-standard techniques and security management services and infrastructure, including firewalls, intrusion detection and prevention systems (IDS/IPS), access control lists, routing protocols, and other security controls that provide continuous monitoring, have the capability to restrict unauthorized network traffic, detect, and limit the impact of attacks.
   - Laptop/desktop computers should be configured to automatically receive operating system patches and updates from a centralized service that manages and distributes updates.
   - Vendor's information systems, network devices, and applications should be configured and deployed using a secure baseline. Ports/services that are not used should be disabled.

- Prior to implementation of information systems, network devices, and applications that will be used to Process Cintas Information, a security review process should be followed to validate security of the information systems, network devices, and applications to identify and remediate critical security issues ahead of deployment.
- If mobile devices are used in the delivery of services to Cintas, devices should be managed using a centralized solution that has the capability to remotely lock and wipe lost/stolen devices.
- Where applicable to services provided to Cintas, if VPN access (either site-to-site or IPsec) is used to connect to Cintas networks and information systems, Vendor must segregate computers that remotely connect to Cintas (using either physical segregation or VLAN subnets) to prevent Cintas confidential information, networks and information systems from potentially being accessible or visible by other personnel on the Vendor network.
- To the extent permitted by law, Cintas reserves the right to monitor Vendor's access to and use of Cintas information systems, networks, and applications.

5. Access Control.

- Vendor will maintain appropriate access controls, including, but not limited to, restricting access to Personal Information to the minimum number of Vendor Personnel who require such access and limited for the purpose of performing the services, as specified in the Agreement. Where applicable, Vendor will maintain a complete list of all personnel with permission to access Cintas and customer facilities, information systems, networks and applications.
- Vendor must have account management procedures to support the secure creation, amendment and deletion of accounts on information systems, network devices and applications.
- Access lists for information systems, networks, and applications must be reviewed on a regular basis.
- Vendor will promptly Vendor Personnel access to information systems, networks, and applications when Vendor Personnel is terminated or when a change to job role results in access no longer being required. This will include the return of company hardware. Vendor will remind Vendor Personnel that they must not retain any Cintas Information.
- Only authorized staff can grant, modify, or revoke access to an information system that uses or houses Cintas Information. Vendor will maintain an audit trail to document whether and by whom Cintas Information has been accessed, entered into, modified, transferred, or removed from Cintas Information Processing, which must be presented to Cintas upon Cintas' request.
- Vendor must maintain logs from information systems, network devices, and applications for a minimum period of ninety (90) days and store log files on a centralized logging server. Logs should be sufficiently detailed to assist in the identification of the source of an issue and enable a sequence of events to be recreated. Logs must record when (date and time), who (such as user or service account) and where (IP address/hostname) for all access and authentication attempts. Logs must also contain information system, network device and application security related event information, alerts, failures, and errors. Logs must be monitored, reviewed and analyzed for suspicious and unauthorized activity and to verify the integrity of the logging process.
- User administration procedures define user roles and their privileges and how access is granted, changed, and terminated; address appropriate segregation of duties; and define the logging/monitoring requirements and mechanisms.
- All employees of Vendor are assigned unique User IDs. Account authentication credentials must not be reused for other accounts.
- Access rights are implemented adhering to the "principle of least privilege."

- Vendor will implement commercially reasonable physical and electronic security to create passwords and protect and maintain passwords in accordance with privileged user management and password policies and requirements including, but not limited to the following:
    - Password must have no less than a minimum of twelve characters for password length and require character complexity (e.g., no dictionary words, using a mix of alpha numeric characters and symbols etc.). Multifactor authentication is highly recommended wherever technically feasible.
    - Passwords must be distributed separately from account information.
    - Passwords must be encrypted when transmitted between information systems, network devices, and applications.
- Vendor will establish security procedures to prevent Cintas Information Processing systems from being used without authorization, such as through logical access controls.
- Remote access to the Vendor's network must be approved and restricted to authorized Vendor Personnel. Remote access must be controlled by secure access control protocols, strong encryption, authentication and authorization.

6. Virus and Malware Controls.

- Vendor must install, use, and maintain endpoint protection (such as EDR, anti-virus/malware detection software) on all devices containing, accessing, processing, or transmitting Cintas Information. This software must be installed, configured, enabled, and updated to prevent, detect and remove malicious code. Endpoint protection solutions should detect if the software has been removed, disabled, or is not receiving regular updates. The Vendor will implement scheduled malware monitoring and system scanning to protect Cintas Information from anticipated threats or hazards and protect against unauthorized access to or use of Cintas Information.
- Vendor implements and maintains industry standard measures designed to prevent the introduction of any "back door," "drop dead device," "time bomb," "Trojan horse," "virus," "worm," "spyware," or "adware" (as such terms are commonly understood in the software industry) or any other code designed or intended to have, or capable of performing or facilitating, any of the following functions: (i) disrupting, disabling, harming, or otherwise impeding in any manner the operation of, or providing unauthorized access to, a computer system or network or other device on which such code is stored or installed; (ii) compromising the privacy or data security of a user; or (iii) damaging or destroying any data or file without a user's consent ("**Malicious Code**") into Vendor's information technology systems (including any hardware, software, firmware, equipment, and other deliverables). Vendor will monitor such systems regularly to verify that they do not and will not contain or make available any Malicious Code.
- Automatic virus and malware scanning checks must be carried out on all e-mail attachments that are sent to or received from external sources. Attachments that are identified as containing Malicious Code must be removed.

7. Threat and Vulnerability Management

- Vendor must develop, document and implement procedures for security vulnerability detection and management (including infrastructure security vulnerability). These procedures must include criteria for vulnerabilities classifications, management, and prioritization based on severity, defined remediation plans, and service level agreements to implement remediation plans and patching for vulnerabilities. Vendor must promptly apply patches to all technology in use including hardware, operating systems, applications and network devices in a consistent, standardized and prioritized manner based upon criticality and risk. If a security patch cannot be promptly applied, then effective risk mitigation controls must be implemented until such time patches can be applied.

- Vendor must procure penetration tests by independent third parties on all critical applications and infrastructure at least annually.
- Vendor may only use technology vendors that provide patch updates.

8. **Personnel**.
   - Prior to providing access to Cintas Information to Vendor Personnel, Vendor will require Vendor Personnel to comply with its Information Security Program.
   - Vendor will implement a comprehensive security awareness program with defined goals and objectives to train all Vendor Personnel about their security obligations and will conduct such training for personnel at hiring and at least annually thereafter. This program will include, at a minimum, training about data classification obligations, physical security controls, security practices, policies, procedures and related requirements, and security incident reporting.
   - If Vendor is provided with access to Cardholder Information, Vendor Personnel will receive training at least once each year to prevent the loss, theft, leakage, falsification, or damage of Cintas Information.
   - Vendor will clearly define roles and responsibilities for Vendor Personnel. Screening will be implemented before employment with terms and conditions of employment applied appropriately.
   - Vendor employees will strictly follow established security policies and procedures.
   - Background screening is required for all Vendors, Vendor Personnel who have, or will have, access to Cintas systems or Cintas Information or that of Cintas customers. Vendors must use a reputable background screening provider approved by Cintas. Approved providers are HireRight, Checkr, BIB, First Advantage, and GoodHire. If a Vendor wishes to use a provider not listed, prior approval from Cintas is required.
     - For U.S.-based accounts, where permissible by law, the background screening must include, at a minimum: (i) verification of identity and employment eligibility; and (ii) a search of federal, state, and local criminal conviction records for all counties of residence and employment over the past seven (7) years.
     - For non-U.S.-based accounts, background screening must comply with local laws and regulations and include criminal record checks as applicable.
   - All Vendor Personnel with access to Cintas systems or Cintas Information must pass the aforementioned background checks prior to the access being given and the checks can be no older than three months prior to assignment on the account. While neither the results nor confirmation of completion is required to be presented to Cintas prior to assignment, the Vendor must confirm the results are sufficient for Vendor Personnel to work.
   - Cintas reserves the right to audit Vendor records at any time to confirm that all Vendor Personnel who have, or will have, access to Cintas systems have a completed background check on file. This audit will not include access to the detailed results of the background check.
   - Vendor Personnel are required to abide by Cintas's security requirements and direction when working at Cintas facilities. Vendor Personnel are required to abide by Cintas customers' security requirements and direction when working at Cintas customer facilities. Vendor Personnel may not photograph or otherwise record such facilities or infrastructure, unless required for the performance of services.
   - Vendor will not permit the use of personal email accounts for exchanging Cintas Information.
9. **Business Continuity**. Vendor will implement, document, and maintain appropriate back-up and disaster recovery, business continuity plan (BCP), and business resumption plans. These plans must be designed to ensure that Vendor can continue to function through operational interruption and

continue to provide services, as specified in the agreement. These plans will include processes to ensure recovery of Cintas Information that was modified or destroyed due to unauthorized access.

- Vendor must ensure that the scope of the BCP covers all locations, personnel, and information systems that are used to perform services for Cintas or Cintas customers.
- Vendor will regularly review, test, and update its business continuity plan and risk assessment to ensure that they are up to date and effective and Vendor will document the results of such tests. If requested but no more than once a year, Vendor will provide documentation confirming tests are being performed.
- If there is an event, which will or does impact Vendor's capability to perform services for Cintas, including execution of the Disaster Recovery plan, Vendor must promptly notify their Cintas business contact.

  Vendor must ensure that information systems, computers and software involved in the performance of the services provided to Cintas are backed up. Backups must be tested in accordance with operational backup standards.

10. **Primary Security Manager**. Vendor will notify Cintas of its designated primary security manager. The security manager will be responsible for managing and coordinating the performance of Vendor's obligations set forth in its Information Security Program and in this DPA.