PRIVACY AND DATA SECURITY ADDENDUM

This Privacy and Data Security Addendum (this "Addendum") applies to suppliers of goods, services, and/or Software (each a "Supplier") to CHS Inc., a Minnesota cooperative corporation, ("CHS") and/or its Affiliates, where the provisions of this Addendum are imposed or required by contract with Supplier or by Supplier's accession to this Addendum.

This Addendum applies if, and to the extent, that Supplier receives or acquires any Covered Data and this Addendum states obligations of Supplier with respect to such Covered Data. Supplier will conform to the requirements of this Addendum at no additional cost to CHS.

1. **Defined Terms**. Without limiting anything else in this Addendum, the following terms will have the following meanings. Where this Addendum defines a term, the definition applies with respect to this Addendum and, except as otherwise stated in this Addendum, this Addendum does not modify any defined term, as such, in any agreement that refers to this Addendum.

   (a) An "Affiliate" means any entity which is controlled by, controls or is in common control with Processor.

   (b) "Authorized Supplier Person" means a natural person who is, directly or indirectly, an agent of Supplier that has a bona fide need to know and/or possess Covered Data, or have access to CHS Information Systems, for the purpose of performing obligations to one or more CHS Parties.

   (c) "Cardholder Data" has the meaning given to that term by the PCI DSS.

   (d) "CHS Information Systems" means computer, communication, and network equipment, systems, and services (voice, data, or otherwise) owned, controlled, or used by CHS or any CHS Affiliate, including, but not limited to, the corporate wide area network, the electronic switched network, Inter/intranet gateways, electronic mail, telephony, computer systems, system hardware, drives, electronic media, storage areas, software programs, files, and databases.

   (e) "CHS Party" in any particular case is CHS or a CHS Affiliate (i) that contracts with Supplier, (ii) from which Supplier receives Covered Data, or (iii) on whose behalf or for whose benefit Supplier collects or receives Covered Data.

   (f) "CIS Critical Controls" means the then-current Center for Internet Security Critical Security Controls for Effective Cyber Defense.[i]

   (g) "Covered Data" means:

      (i) CHS Personal Information;

      (ii) Any usernames, login credentials, passwords, or other access information pertaining to any CHS Information Systems; and

      (iii) Any other information held by CHS or any Affiliate of CHS, or that Supplier receives or collects as a part of its performance under an agreement with a CHS Party, that is both:

         (A) Not readily ascertainable by the public by proper means; and

         (B) The subject of efforts by CHS or its Affiliates to keep it from becoming readily ascertainable by the public by proper means.

   (h) "Data Protection Laws" means all laws and regulations, including without limitation, laws and regulations of the European Union, the United States and the California Consumer Privacy Act, applicable to the Processing of Personal Data under the Agreement.

   (i) "PCI DSS" means the then-current Payment Card Industry Data Security Standard as promulgated by the PCI Security Standards Council.

   (j) "PCI Service Provider" means a service provider as defined by PCI DSS.

(k) "Permitted System" means a CHS Information System to which CHS or a CHS Affiliate expressly gives Supplier access and that is necessary for Supplier to perform its obligations to one or more CHS Parties.

(l) "Personal Information" means any information relating to an identified or identifiable person defined as such in any Data Protection Law(s) in combination with any one or more of the following pieces of unencrypted information: (1) social security number, (2) birth date; (3) driver's license number or government issued identification card, (4) student, military or passport identification number; (5) any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; (6) medical information, health insurance identification number or biometric data, (7) an individual's user name or email address in combination with a password or security question and answer that allows access to an online account; (8) account number or credit or debit card number, access code, or password that would permit access to an individual's financial account. This information does not include the last 4 digits of an individual's social security number or any information that is legally available in the public records or a federal or a local agency. "Processing" of Personal Information means any operation or set of operations which is performed on Personal Information or on sets of Personal Information, 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.

(m) "Security Breach" means any unlawful access to any CHS Covered Data stored on Supplier's equipment or in Supplier's facilities, or access to equipment or facilities resulting in any loss, disclosure, or alteration of CHS Covered Data. "

2. **Privacy and Data Security Generally**. Supplier shall comply with the terms and conditions contained in this Addendum and will be responsible for any act or omission by any direct or indirect employee, contractor, or agent of Supplier (including, but not limited to, Authorized Supplier Persons) that, if done or omitted to be done by Supplier, would be a violation by Supplier of the requirements of this Addendum.

3. **Privacy and Confidentiality**.

(a) Covered Data Included in Obligations under Agreements. Where any agreement between any CHS Party and Supplier contains any confidentiality obligation or obligation limiting the use or disclosure by Supplier of confidential information of CHS or any CHS Affiliate (whether styled "Confidential Information," "Proprietary Information," or otherwise), the obligations with respect to such information will apply to Covered Data regardless of whether Covered Data is, by the terms of the agreement, included in the scope of the applicable term.

(b) Obligations Generally with Respect to Covered Data. Supplier will:

(i) Keep and maintain all Covered Data in strict confidence, using such degree of care as is necessary to avoid unauthorized access, use, or disclosure, and, in each case, use all protections, safeguards, and care required by applicable law;

(ii) Comply with all law that applies to the collection, use, sharing, storage, protection, transfer, and disposal of such Covered Data;

(iii) Not create, collect, receive, access, or use Covered Data in violation of law;

(iv) Use and disclose Covered Data solely and exclusively for the purposes for which the Covered Data, or access to it, is provided by the CHS Party, and not use, sell, rent, transfer, distribute, or otherwise disclose or make available Covered Data for Supplier's own purposes or for the benefit of any person other than the applicable CHS Party or its designee(s); and

(v) Not, directly or indirectly, disclose Covered Data to any third party without the written consent of the applicable CHS Party.

(c) Compliance with CHS Privacy Statement(s). Supplier will undertake no act or omission that, if done or omitted to be done by the applicable CHS Party, would violate the published public-facing privacy statement or privacy policy of the CHS Party. The CHS Global Privacy Notice can be found here: https://chsinc.com/privacy-policy.

4. **Processing of CHS Covered Data Where Other Contractual Requirements Apply**. Where CHS reasonably deems it necessary in order to comply with applicable law (including, but not limited to, the law of non-US countries that require contractual arrangement in order to legally export Personal Data and law requiring Business Associate Agreements), Supplier will, promptly when requested by any CHS Party, enter into such agreements as CHS reasonably requires in order to comply with applicable law.

5. **Return and/or Destruction of Covered Data**.

   (a) Return or other Provision of Covered Data. At the termination or completion of services in connection with which Supplier holds Covered Data, Supplier will, at CHS's option and upon request made by CHS within 30 days after such termination or completion, provide to CHS, in industry-standard electronic form as requested by CHS, such Covered Data as Supplier holds as of the time immediately before termination or completion. If the relevant agreement associated with such services does not provide for compensation for such provision of Covered Data, and does not require provision of such Covered Data at no charge to CHS, CHS sill pay to Supplier the actual cost of media and personnel necessary to provide the Covered Data as required by this Section 7.

   (b) Deletion and Destruction of Covered Data. If and when Supplier is required to destroy Covered Data, Supplier will destroy such Covered Data using methods at least as complete and reliable as those contained in NIST Special Publication 800-88, as amended, or its successor document. Where Supplier is permitted to retain Covered Data in de-identified or anonymized form, Supplier will de-identify and anonymize the Covered Data according to NISTIR 8053, as amended, or its successor document or, where required by law, as provided for under such law.

6. **Business Continuity Planning**.

   (a) At all times at which Supplier holds Covered Data, Supplier will have in place a bona fide business continuity plan that will ensure that Supplier is able to continue to services when the provision of such services is interrupted for any reason outside of Supplier's reasonable control ("Business Continuity Plan"). Supplier shall maintain and update the Business Continuity Plan at least annually for each of its operational sites related to the provision of services. Supplier will put the Business Continuity Plan in effect if a site becomes unable to perform such services or deliver services for a period of more than five calendar days. Supplier will perform a timely assessment after the occurrence of any event that may delay the performance of maintenance and support or the delivery of services for a period of more than five calendar days. Supplier will activate the Business Continuity Plan if Supplier determines that Supplier will be unable to perform services for a period of more than five calendar days.

   (b) The Business Continuity Plan shall contain, at a minimum, provisions for (a) a risk assessment and business impact analysis, (b) a prevention/mitigation plan, and (c) a resumption of services plan.

   (c) Supplier will provide a copy of the Business Continuity Plan within 10 calendar days of CHS's request for the then-current Business Continuity Plan.

   (d) At CHS's request, and at no additional charge to CHS, Supplier will participate in any tests implemented by CHS or discussions initiated by CHS for purposes of evaluating, coordinating and integrating the business continuity plans of its suppliers with CHS' overall business continuity plan. As reasonably requested by CHS, Supplier will reasonably adjust the Business Continuity Plan to better conform to and integrate with CHS' business continuity plan.

7. **Information Security**.

   (a) Supplier will implement and maintain a written information security program including appropriate policies, procedures, and risk assessments that are reviewed at least annually.

   (b) Supplier will implement administrative, physical, and technical safeguards to:

      (i) Protect Covered Data from unauthorized access, exfiltration, acquisition, or disclosure, destruction, alteration, accidental loss, misuse, or damage; and

      (ii) Take all necessary steps in mitigating damage, losses, costs and expenses caused by the events set forth in Section 9(b)(i).

   (c) Supplier shall notify CHS of any significant changes to administrative, physical, or technical safeguards that could reasonably be expected to adversely affect the protection of Covered Data from

unauthorized access, exfiltration, acquisition, or disclosure, destruction, alteration, accidental loss, misuse, or damage.

(d) Where Supplier receives, stores, and/or Processes Covered Data using Supplier's own systems and facilities, Supplier will implement, and maintain, CIS Critical Controls, including, but not limited to, the following controls, each as is more fully explained in the CIS Critical Controls.

(i) Inventory of Authorized and Unauthorized Devices. Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

(ii) Inventory of Authorized and Unauthorized Software. Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

(iii) Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers. Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

(iv) Continuous Vulnerability Assessment and Remediation. Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

(v) Controlled Use of Administrative Privileges. The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

(vi) Maintenance, Monitoring, and Analysis of Audit Logs. Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

(vii) E-Mail and Web Browser Protections. Minimize the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and e-mail systems.

(viii) Malware Defenses. Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.

(ix) Limitation and Control of Network Ports, Protocols, and Services. Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.

(x) Data Recovery Capability. Use processes and tools to properly back up critical information with a proven methodology for timely recovery of it.

(xi) Secure Configurations for Network Devices such as Firewalls, Routers, and Switches. Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

(xii) Boundary Defense. Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.

(xiii) Data Protection. Use processes and tools to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

(xiv) Controlled Access Based on the Need to Know. Use processes and tools to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

(xv) Wireless Access Control. Use processes and tools to track/control/prevent/ correct the security use of wireless local area networks, access points, and wireless client systems.

(xvi) Account Monitoring and Control. Actively manage the life cycle of system and application accounts – their creation, use, dormancy, deletion -- in order to minimize opportunities for attackers to leverage them.

(xvii) Security Skills Assessment and Appropriate Training to Fill Gaps. For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.

(xviii) Application Software Security. Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.

(xix) Incident Response and Management. Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

(xx) Penetration Tests and Red Team Exercises. Test the overall strength of an organization's defenses (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.

(e) Audits.

Supplier will, with respect to each system that holds, contains, or Processes Covered Data

(A) Cause examinations to be performed by one or more qualified third parties as stated in, and contemplated by, Statement on Standards for Attestation Engagements No. 16 ("SSAE 16") and reports issued by such third party(ies) attesting that Supplier's management's description of Supplier's system fairly presents the system that was designed and implemented, at either a specific date not earlier than one year prior to the date of determination (in the case of a Type 1 report) or implemented throughout a specified time period that includes a date not earlier than one year prior to the date of determination (in the case of a Type 2 report); and

(B) For so long as such system holds, contains, or processes Covered Data, cause the system to conform in all material respects with management's assertions with respect to the system upon which the then-most-recent SSAE 16 report as of the date of determination.

Supplier will, upon CHS's request, make available to CHS for review, as applicable, Supplier's latest Payment Card Industry (PCI) Compliance Report, WebTrust reports, Systrust reports, SSAE 16 audit reports, and any reports relating to its ISO/IEC 27001 certification. CHS shall treat such audit reports as Supplier's confidential information for the purposes of confidentiality obligations, if any, under any then-existing agreement(s) between Supplier and any applicable CHS Party. Supplier will promptly remedy any exception or failure noted in any SSAE 16 report or other audit report.

(f) Upon CHS's request, to confirm Supplier's compliance with this Addendum and any applicable laws, regulations, and industry standards, Supplier will permit CHS or CHS's agents to perform an assessment, audit, examination, or review of all controls in Supplier's physical and/or technical environment in relation to all Covered Data being handled, received or acquired and/or services being provided to CHS under the applicable agreement, and this Addendum. Supplier shall cooperate fully with such assessment by providing access to knowledgeable personnel, physical premises, documentation, infrastructure, and applicable software that processes, stores, or transports the Covered Data for CHS pursuant to the applicable agreement and this Addendum. In addition, upon CHS's request, Supplier shall provide CHS with the results of any audit by or on behalf of Supplier performed that assess the effectiveness of Supplier's information security program as relevant to the security and

confidentiality of the Covered Data shared during the course of the applicable agreement and this Addendum.

(g) PCI DSS. If, and to the extent that, any of the Covered Data is Cardholder Data that Supplier receives or Processes as a PCI Service Provider, Supplier will, unless expressly permitted otherwise in writing by the applicable CHS Party:

(i) Be, at all times while holding or Processing Cardholder Data, a Level 1 Service Provider with current onsite assessments and all other qualifications and certifications necessary to that designation under PCI DSS;

(ii) Deliver to CHS Supplier's Attestation of Compliance promptly upon completion thereof, in such form and containing such information as required under PCI-DSS, dated not more than one year after the previous AOC (if any) delivered by Supplier to CHS;

(iii) If requested by CHS, agree upon a responsibility matrix or other documentation identifying which PCI DSS requirements of CHS will be managed by Supplier; and

(iv) Otherwise comply with all requirements of PCI DSS with respect to the Cardholder Data.

8. **Access to CHS Information Systems**.

(a) Use of Permitted Systems. Supplier will use any Permitted Systems solely to carry out Supplier's obligations to the applicable CHS Party(ies). Supplier will use Permitted Systems for no other purpose.

(b) Conditions of Use. Supplier will use the Permitted Systems solely accordance with the terms of such agreement(s) as is (are) then in place between one or more CHS Parties and Supplier and such further conditions and policies as the applicable CHS Party makes available to Supplier from time to time. Such conditions and policies of use may include (and be described as) policies, procedures, technical requirements, and/or protocols.

(c) Access by Authorized Supplier Persons. Supplier will limit access to the Permitted Systems to Authorized Supplier Persons. Supplier will provide to CHS the name of each Authorized Supplier Person. Each Authorized Supplier Person must establish and maintain a unique identifier for access and follow the same security rules as CHS's personnel. Supplier shall ensure that individuals other than Authorized Supplier Persons (including, without limitation, past employees and current employees who do not have an active role in providing goods, services, or software to CHS or its Affiliates) shall have no access to CHS Information Systems.

(d) Specific Prohibitions. Except as expressly authorized by a CHS Party in a signed writing (whether in a statement of work, project specification, work order, or separate written direction) Supplier shall not (i) attempt to reverse engineer, disassemble, reverse translate, decompile or in any other manner decode any element of the CHS Information Systems; (ii) make modifications, enhancements, adaptations or translations, in whole or in part, to or of any element of the CHS Information Systems; (iii) make copies of any element of the CHS Information Systems; (iv) probe host computers or networks; (v) breach or examine the security controls of a host computer, network component or authentication system; (vi) monitor data on any network or system; (vii) interfere with the service of any user, host or network, or overload a server, network connected device, or network component; (viii) originate malformed data or network traffic that results in damage to, or disruption of, a service or network connected device; (ix) forge data or misrepresent the origination of a user or source.

(e) Failure of Access. Supplier acknowledges that access to the Permitted Systems may be interrupted due to circumstances within or outside the reasonable control of the applicable CHS Party(ies). Nothing in this Addendum or any agreement between Supplier and any CHS Party will be a promise or covenant to deliver access to the Permitted Systems or that any Permitted System will be functional. Aside from the access as provided under this Addendum, no license under any patent, copyright, or any other intellectual property right in respect of CHS Information System is granted to Supplier by virtue of access to the Permitted Systems.

(f) Waiver of Liability. CHS excludes all representations, warranties, and covenants, express or implied, by CHS or any CHS Affiliate with respect to the CHS Information Systems, including, but not limited to, any representations, warranties, or conditions of accuracy, sufficiency, suitability, or non-infringement regarding Supplier's access to, or use of, any Permitted System. CHS and its Affiliates will have no

liability whatsoever for any damages, losses, or expenses incurred by Supplier as a result of Supplier's or its Supplier Authorized Persons' access to the Permitted Systems (including, without limitation, the inadvertent accessing of a computer virus or other harmful computer file or program), or of failure of the Permitted System(s) to be available or accessible.

(g) Supplier Systems. Where Supplier accesses Permitted Systems using Supplier's hardware, software, or networks, the following provisions will apply.

(i) Access Security. Supplier shall ensure that Authorized Supplier Persons obtain access to the Permitted Systems through a computer system that maintains authentication controls and includes a suitable firewall. Supplier shall follow all of CHS' security rules and procedures for restricting access to its computer systems.

(ii) Segregation Wall. Supplier will ensure that Authorized Supplier Persons are effectively isolated from its personnel who are assigned to the account of a known or potential competitor of CHS or of any Affiliate of CHS. Supplier will establish and document physical and electronic procedures to segregate and protect all information, data and communications (including, but not limited to, Covered Data).

9. **Security Breach Procedures**.

(a) Supplier will provide to the applicable CHS Party name and contact information for one or more representatives of Supplier (which may be a live-staffed help desk) who will serve as CHS's primary security contact and be available to assist CHS 24 hours per day, seven days per week as a contact in resolving obligations associated with any actual or suspected Security Breach.

(b) In the case of any actual or suspected Security Breach, the following provisions will apply.

(i) Supplier will notify the applicable CHS Party of the actual or suspected Security Breach as soon as practicable, but in any case not later than 24 hours after Supplier becomes aware of the actual or suspected Security Breach. If the agreement or other terms and conditions under which Supplier provides goods, services, or software to the CHS Party provide for a specific CHS Party contact, supplier will notify that CHS Party contact and also send an e-mail notification to CHSinformationsecurity@chsinc.com. If the agreement or other terms and conditions under which Supplier provides goods, services, or software to the CHS Party do not provide for a specific CHS Party contact, Supplier will notify CHS Information Security by e-mail at CHSinformationsecurity@chsinc.com and/or IT Service Center Phone: 651-355-5555 or 800-852-8185. Supplier will also provide to CHS any other notice required by law.

(ii) Immediately following Supplier's notification to the CHS Party of an actual or suspected Security Breach, Supplier will coordinate with the CHS Party and its designees to investigate the actual or suspected Security Breach. Supplier will reasonably cooperate with the CHS Party in the CHS Party's handling of the matter, including, without limitation: (A) assisting with any investigation; (B) providing CHS with physical access to the facilities and operations affected; (C) facilitating interviews with Supplier's employees and others involved in the matter; and (D) 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 the CHS Party or its designees.

(iii) Supplier will, at its own expense, immediately contain and remedy any Security Breach, including, but not limited to, taking any and all action necessary to comply with applicable privacy rights, laws, regulations, and standards. Supplier shall reimburse CHS and its Affiliates for all costs incurred by CHS in responding to, and mitigating damages caused by, any Security Breach, including, but not limited to, all costs of notice and/or remediation.

(iv) Except as is required by law or as otherwise required to act exigently to mitigate or avoid further harm or damage to persons or property, Supplier will not inform any third party of any Security Breach without first obtaining CHS's prior written consent. Where Supplier informs any third party of a Security Breach as required by law or as otherwise required to act exigently to mitigate or avoid further harm or damage to persons or property, Supplier will give notice to the applicable CHS Party concurrently with such other notice.

(v) Except as is required by law or as otherwise required to act exigently to mitigate or avoid further harm or damage to persons or property, CHS will have the sole right to determine: (A) whether notice of the Security Breach 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 CHS's discretion; and (B) 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.

(vi) Supplier will maintain and preserve all documents, records, and other data related to any Security Breach.

(vii) Supplier shall indemnify, defend, and hold harmless CHS and its Affiliates and their respective directors, managers, officers, employees, and agent from any and all claims, suits, damages, liabilities, obligations, costs, and expenses (including, but not limited to, reasonable attorneys' fees and the costs of any credit monitoring or other services required to mitigate such Security Breach for customers, end users, and other persons whose information was released as part of such Security Breach) arising from or otherwise related to any Security Breach.

10. **Coordination of this Addendum with Other Agreements**.

(a) The obligations in this Addendum are, wherever possible, to be regarded as additional to any other obligations in any agreement between Supplier and any CHS Party.

(b) Where possible, the provisions of this Addendum will be construed as consistent with those of other terms, conditions, and agreements between Supplier on the one hand and CHS and/or its Affiliates on the other hand.

(c) Where the provisions of this Addendum cannot be construed consistently with the provisions of other terms, conditions, and agreements between Supplier on the one hand and CHS and/or its Affiliates on the other hand, the provision containing or imposing the greater restriction or protection benefitting the CHS Party will prevail.

Service Provider (Company Name):_____

Name:_____

Title:_____

Signature:_____

Date:_____

[i] The Center for Internet Security Critical Security Controls for Effective Cyber Defense work is licensed under a Creative Commons Attribution – Non Commercial – No Derivatives 4.0 International Public License. The link to the license terms can be found at https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode. Users of the CIS Critical Security Controls framework are also required to refer to https://www.cisecurity.org/controls/cis-controls-list/ when referring to the CIS Critical Security Controls in order to ensure that users are employing the most up to date guidance.