Interlocal Agreement for Cybersecurity Services

This Interlocal Agreement for Cybersecurity Services ("Agreement") is between The Texas A&M University System (the "A&M System"), an agency of the State of Texas, on behalf of its Office of Cybersecurity and College Station Independent School District ("Client"), a local independent school district of the State of Texas.

The A&M System's Office of Cybersecurity has certain cybersecurity capabilities and assets that it uses to aid local governments, consistent with the A&M System's public service mission and Texas Government Code Section 2054.0594(d). Client desires to utilize such services, and so the parties enter into this Agreement pursuant to the Interlocal Cooperation Act, Texas Government Code Chapter 791.

The parties therefore agree as follows:

1. Statement of Work

1.1 The A&M System shall use reasonable efforts to provide the services (the "Services") described in the Statement of Work attached as Appendix A (the "SOW"). The SOW may only be changed by written amendment to this Agreement signed by both parties.

1.2 Each party shall designate a point of contact for the Services.

1.3 If the Services include security scanning, testing, assessment, remediation, or similar Services:

(a) Client:

(1) Understands that the A&M System may use various methods and software tools to probe for security-related information and to detect actual or potential security flaws and vulnerabilities;

(2) Authorizes the A&M System to perform such Services (and all tasks and tests reasonably contemplated by or reasonably necessary to perform the Services) on systems or resources identified by Client;

(3) Certifies that, if Client does not own such systems or resources, Client has obtained authorization from the appropriate party to permit the A&M System to provide the Services; and

(4) Shall disclose to the A&M System in advance:

(a) Any information reasonably necessary to safely and securely conduct the Services;

(b) Any networks, systems, configurations or data of heightened sensitivity or risk; and

(c) Anything that should be excluded from testing.

(b) If either party identifies a potentially significant degradation, interruption, or other impact during the Services, that party shall promptly notify the other and the parties shall collaborate to resolve the issue.

(c) Client acknowledge that:

(1) The Services could possibly result in service interruptions or degradation regarding Client's systems and accepts those risks and consequences; and

(2) Client is responsible for restoring network computer systems to a secure configuration after the completion of the A&M System's testing.

2. Client Responsibilities

2.1 Client shall:

(a) Fulfill all Client responsibilities specified in the SOW;

(b) Ensure that all assumptions in the SOW are accurate;
(c) Provide the A&M System with reliable, accurate, and complete information as required to perform the Services;
(d) Ensure that all of Client's data, programs, and files are backed up and made available to the A&M System; and
(e) Manage the selection, use, and application of the Services.

2.2 The A&M System may rely on all Client decisions, representations, and approvals made before and during the provision of Services. Nothing in this Agreement requires the A&M System to evaluate, advise on, modify, confirm, or reject Client's decisions, representations, or approvals. Client shall manage the selection and use of its internet, data, and telecommunication facilities during the execution of the Services.

3. Period of Performance. The A&M System shall conduct the Services during the period commencing August 1, 2025 and, unless earlier terminated under Article 6, ending July 31, 2026. These dates may be modified or extended only by written agreement of the parties.

4. Hardware

4.1 "Hardware" means any A&M System device, equipment, or hardware installed on Client's computers, networks, or systems to facilitate the delivery of the Services. "Hardware" does not include any device, equipment, or hardware procured by or on behalf of Client.

4.2 The Hardware is installed on a temporary basis only, for use by the A&M System, and Client does not acquire any rights of ownership or any lien or other similar right as to the Hardware. Client may not remove any label or other marking on the Hardware. Client may not bail, loan, consign, sublease, sell, transfer, assign, part with possession or otherwise dispose of the Hardware or place or permit to be placed any liens on the Hardware or otherwise encumber the Hardware.

4.3 Client shall exercise reasonable care to protect the Hardware from loss or damage and may not disassemble, modify, tamper with, move, attempt to repair, or attempt to install any software on the Hardware.

5. Price and Payment

5.1 As compensation for the performance of the Services, Client shall pay the A&M System the annual fixed price amount of $178,398.00.

5.2 Client shall make all payments under this Agreement from current revenues available to Client.

5.3 This is a fixed-price Agreement based on the current SOW. Client acknowledges that any changes to the SOW may affect the cost of the Services.

5.4 Upon the execution of this Agreement and each anniversary of that date, the A&M System shall submit an invoice to Client's address below and Client shall remit payment to the A&M System within 30 days of receipt of invoice.

5.5 The A&M System shall submit invoices to Client at the following address:

College Station ISD
Accounts Payable
1812 Welch Ave.,
College Station, TX 77840

5.6 Client shall submit payments to the A&M System at the following address:

Texas A&M University System
Office of Budgets & Accounting
301 Tarrow Dr, 3rd Floor

College Station, TX 77840-7896

6. Termination

6.1 Either party may terminate this Agreement for any or no reason effective upon 60 days' written notice.

6.2 Either party may terminate this Agreement effective upon written notice to the other party if the other party materially breaches any term of this Agreement and fails to cure such breach within 15 days after receiving written notice of the breach. If the breach is incurable, the non-breaching party may terminate this Agreement effective immediately upon written notice to the breaching party.

6.3 Upon termination, Client shall reimburse the A&M System as specified in Article 5 for all costs and non-cancelable commitments incurred in the performance of the Services up to the date of termination, such reimbursement not to exceed the total amount specified in Article 5. Upon early termination, the A&M System shall reimburse to Client any funds that have been received but remain unexpended at the time of termination, except for those funds needed to pay for non-cancelable obligations.

6.4 Upon termination of this Agreement, Client shall promptly provide the A&M System with reasonable access to remove any Hardware, or, at the A&M System's option, promptly return the Hardware to the A&M System at Client's expense. If Client fails to fulfill its obligations under this Section 6.4, Client will be liable, to the extent authorized by law, for all reasonable costs incurred by the A&M System due to such failure.

7. Intellectual Property Rights

7.1 Except as expressly provided in this Agreement, nothing in this Agreement grants to Client any rights in any software, data, tools, hardware, analyses, designs, documentation, reports, methodologies, processes, specifications, programming logic, pseudo code, technologies, know-how, or related materials, or any patents, copyrights, or other intellectual property rights, made available to Client or otherwise used by the A&M System in providing the Services.

7.2 The A&M System hereby grants Client a nonexclusive, non-transferable, royalty-free license, for Client's internal business purposes, to use, produce, display, distribute, and make derivative works of the reports and other results of the Services described as deliverables in the SOW.

7.3 Except as expressly provided in this Agreement, nothing in this Agreement grants to the A&M System any rights in any software, data, tools, hardware, analyses, designs, documentation, reports, methodologies, processes, specifications, programming logic, pseudo code, technologies, know-how, or related materials, or any patents, copyrights, or other intellectual property rights, made available to the A&M System by Client for purposes of the Services.

7.4 Client hereby grants the A&M System a nonexclusive, royalty-free license to use, disclose, reproduce, distribute, and otherwise exploit any evaluations, assessments, or suggestions (collectively, "Feedback") provided by Client to the A&M System regarding the Services. The A&M System acknowledges that any Feedback is provided as-is, without warranties of any kind.

8. No Endorsement or Certification

8.1 Client acknowledges that the Services do not result in a certification or endorsement by the A&M System of Client or Client's services, systems, programs, policies, or procedures.

8.2 Neither party may use the name or any adaptation of the name of the other party except in factual statements that, in context, are not misleading and do not imply an endorsement by

that party.

8.3 Each party acknowledges that nothing in this Agreement grants the other party any right to use the other party's trademarks, service marks, logos, or other identifiers.

9. Confidentiality

9.1 "Client Data" means nonpublic Client data, other than Excluded Data, disclosed to or accessed by the A&M System in the course of performing the Services, including but not limited to, logs, session data, telemetry, user data, usage data, threat intelligence data, threat detection information, potentially malicious files, system stability data, user experience data, user interface data, network traffic metadata, source and destination IP addresses, active directory information, file applications, URLs, file names, and file content, passwords, personal identification numbers, access codes, encryption, vulnerability assessments, and other information related to Client's cybersecurity.

9.2 "Excluded Data" means data that:

(a) Is or becomes publicly known or available other than as a result of a breach of this Agreement by the A&M System;

(b) Was already in the possession of the A&M System as the result of disclosure by an individual or entity that was not then obligated to keep that information confidential;

(c) Client had disclosed or discloses to an individual or entity without confidentiality restrictions; or

(d) The A&M System had developed or develops independently before or after accessing or collecting equivalent information under this Agreement.

9.3 The A&M System may not disclose Client Data except as permitted under this Agreement or use Client Data except for purposes of fulfilling the A&M System's obligations under this Agreement or as otherwise required by law. The A&M System may disclose Client Data only to the A&M System's employees and contractors having a need to know the Client Data to fulfill the A&M System's obligations under this Agreement, provided that the A&M System remains responsible for such employees' and contractors' compliance with the A&M System's obligations under this Agreement. Client acknowledges that the A&M System's contractors that provide the Hardware and associated services to the A&M System may use Client Data accessed through or collected by the Hardware for the following purposes: (a) providing their services to the A&M System; (b) analyzing, maintaining, evaluating, and improving their products and services; and (c) complying with their legal, governmental, and contractual obligations.

9.4 The A&M System shall handle Client Data with the same care that the A&M System uses to protect its own information of comparable sensitivity, but not less than reasonable care. The A&M System shall implement and maintain appropriate administrative, technical, and physical security measures to safeguard and preserve the confidentiality of Client Data.

9.5 If the A&M System is legally required to disclose Client Data, the A&M System shall, to the extent allowed by law, promptly give Client written notice of the requirement so as to provide Client a reasonable opportunity to pursue appropriate process to prevent or limit the disclosure. If the A&M System complies with the terms of this Section 9.5, disclosure by the A&M System of that portion of the Client Data which the A&M System is legally required to disclose will not constitute a breach of this Agreement.

9.6 The A&M System shall, upon request of Client, promptly return to Client or destroy all materials embodying Client Data other than materials in electronic backup systems or otherwise not reasonably capable of being readily located and segregated without undue burden or expense. The A&M System may also securely retain one copy of materials embodying Client Data in its files solely for record purposes.

9.7 Each party shall comply with all data privacy and information-security related laws, rules, and regulations applicable to personal data and their performance of this Agreement, including but not limited to, the Texas Identity Theft Enforcement and Protection Act (collectively, "Data Privacy Laws"). The parties shall enter into any further agreements as may be necessary to facilitate compliance with Data Privacy Laws.

9.8 Each party acknowledges that the other is obligated to strictly comply with the Texas Public Information Act, Chapter 552, Texas Government Code, in responding to any request for public information pertaining to this Agreement, as well as any other disclosure of information required by applicable Texas law.

9.9 This Article 9 will survive the termination of this Agreement.

10. Acknowledgements and Disclaimer of Warranties

10.1 Client acknowledges that the A&M System:

(a) Does not warrant that its opinions or findings will be recognized or accepted by third parties;

(b) May use Hardware and other tools from third-party vendors while performing the Services, and the A&M System is not liable for the accuracy, completeness, or any flaws the Hardware and tools may provide in the course of the Services;

(c) Cannot and does not warrant that the Services will discover or identify all errors, flaws, vulnerabilities, weaknesses in, or damage to the Client's software, systems or data; and

(d) Cannot and does not warrant that the Services will ensure Client's software, systems, or data will not be vulnerable, susceptible to exploitation, free from hacking, or eventually breached.

10.2 Client acknowledges that Client, and not the A&M System, is solely responsible for the security of its software, systems, and data, and the A&M System's provision of the Services does not relieve Client of any responsibility for the design, testing, or security of Client's software, systems, and data.

10.3 The A&M System makes no warranties, express or implied, as to any matter, including, without limitation, warranties as to the conduct, completion, success, or particular results of the Services, or the condition, ownership, merchantability, or fitness for a particular purpose of the results of the Services.

11. Force Majeure

11.1 For purposes of this Agreement, "Force Majeure Event" means, with respect to a party, any event or circumstance, whether or not foreseeable, that was not caused by that party (other than a strike or other labor unrest that affects only that party, an increase in prices or other change in general economic conditions, a change in law, or an event or circumstance that results in that party's not having sufficient funds to comply with an obligation to pay money) and any consequences of that event or circumstance.

11.2 If a Force Majeure Event prevents a party from complying with any one or more obligations under this Agreement, that inability to comply will not constitute breach if:

(a) That party uses reasonable efforts to perform those obligations;

(b) That party's inability to perform those obligations is not due to its failure to:

(1) Take reasonable measures to protect itself against events or circumstances of the same type as that Force Majeure Event; or

(2) Develop and maintain a reasonable contingency plan to respond to events or circumstances of the same type as that Force Majeure Event; and

(c) That party complies with its obligations under Section 11.3.

11.3 If a Force Majeure Event occurs, the noncomplying party shall promptly notify the other party of the occurrence of that Force Majeure Event, its effect on performance, and how long the noncomplying party expects it to last. Thereafter the noncomplying party shall update that information as reasonably necessary. During a Force Majeure Event, the noncomplying party shall use reasonable efforts to limit damages to the other party and to resume its performance under this Agreement.

12. Export Controls and Restricted Party Screening

12.1 Each party shall comply with U.S. export control laws and all other laws applicable to the activities under this Agreement.

12.2 Each party certifies that none of its personnel participating in the activities under this Agreement is a "restricted party" as listed on the Denied Persons List, Entity List, and Unverified List (U.S. Department of Commerce), the Debarred Parties Lists (U.S. Department of State), the Specially Designated Nationals and Blocked Persons List (U.S. Department of Treasury), or any similar governmental lists.

13. General Provisions

13.1 This Agreement is not intended to create a partnership, joint venture, or employment relationship between the parties. Neither party may bind the other or otherwise act in any way as the representative of the other, unless specifically authorized, in advance and in writing, to do so, and then only for the limited purpose stated in such authorization.

13.2 The substantive laws of the State of Texas (and not its conflicts of law principles) govern all matters arising out of or relating to this Agreement and all of the transactions it contemplates. Exclusive venue for any claim arising out of or relating to this Agreement will be as provided under Texas law.

13.3 To the extent applicable, Client shall use the dispute resolution process provided in Chapter 2260, Texas Government Code, and the related rules adopted by the Texas Attorney General to attempt to resolve any claim for breach of contract made by Client that cannot be resolved in the ordinary course of business. Client shall submit written notice of a claim of breach of contract to the A&M System's designated official, who will examine Client's claim and any counterclaim and negotiate with Client in an effort to resolve the claim.

13.4 Any notices required or permitted under this Agreement will be deemed given (a) three business days after it is sent by certified mail, return receipt requested, (b) the next business day after it is sent by overnight carrier, (c) on the date sent by email transmission with confirmation of transmission and receipt, if sent during the recipient's normal business hours and if not, on the next business day, or (d) on the date of delivery if delivered personally, and in each case, addressed to the intended recipient at the address below or such other address as the intended recipient may specify in writing:

(a) A&M System: Texas A&M University System
Cyber Shared Services
1370 TAMU
College Station, TX 77843-1370
nmclarty@cyber.tamus.edu

(b) Client: College Station ISD
1812 Welsh Ave.,
College Station, TX 77840
dhutchison@csisd.org

13.5 This Agreement contains the entire understanding of the parties as to the Services, and supersedes all other written and oral agreements between the parties as to the Services. The parties may execute other contracts, but those will not alter this Agreement unless

expressly stated in writing. Each party hereby objects to any different or additional terms on any purchase order, invoice, acknowledgement, or other form.

13.6 If there is a conflict between any of the documents that make up this Agreement, the documents will prevail in the following order:

(a) The body of this Interlocal Agreement for Cybersecurity Services;

(b) The SOW; and

(c) Any other documents or specifications that are attached to and expressly incorporated by reference into this Agreement.

13.7 This Agreement is assignable only with the written consent of both parties.

13.8 Each party acknowledges that nothing in this Agreement is intended to waive or relinquish either party's rights to claim any exemptions, privileges, or immunities as may be provided by law.

13.9 The failure of either party at any time to require performance by the other party of any provision of this Agreement will in no way affect the right to require such performance at any time thereafter nor will the waiver by either party of a breach of any provision be taken or held to be a waiver of any succeeding breach of such provision or as a waiver of the provision itself.

13.10 Each provision of this Agreement is severable. If any provision is rendered invalid or unenforceable by statute or regulations or declared null and void by any court of competent jurisdiction, the remaining provisions will remain in full force and effect if the essential terms of this Agreement remain valid, legal, and enforceable.

13.11 This Agreement may be signed in counterparts, each one of which is considered an original but all of which constitute a single instrument.

This Agreement is effective on the date that it has been executed by both parties, as indicated below.

The Texas A&M University System

By:_____
Jeff Zimmermann
Director, Procurement & Business Services
Date:_____

By:_____
Nicholas McLarty
Deputy Chief Information Security Officer
Date:_____

College Station Independent School District

By:_____
Name:_____
Title:_____
Date:_____

By:_____
Name:_____
Title:_____
Date:_____

Appendix A
Statement of Work

EXHIBIT A

STATEMENT OF WORK

The A&M System provides the following Services under Agreement with the Client:

1. Provision endpoint detection and response (EDR) software-as-a-service ("SaaS") subscription for Client.

2. Provision DNS filtering software-as-a-service ("SaaS") subscription for Client, consulting with Client to select appropriate filtering rules and deployment options.

3. Integrate network data and EDR software into the A&M System's Cyber Operations (Cyber Ops) incident management system. Create detection rules and customize existing rules and use cases for property security monitoring and incident reporting.

4. Provide 8x5 staffed and 24x7 on-call threat monitoring and detection, and escalation of threat indicators to Client for attention.

5. Work with Client to integrate Cyber Ops deliverables for subscribed Services with Client's existing IT environment.

6. Provide automated and analyst-generated cyber threat intelligence services via the A&M System Information Sharing and Analysis Organization (ISAO).

7. Provide quarterly vulnerability scanning of Client's Internet-facing services and network ranges, and escalation of vulnerable services to Client for attention.

Client shall provide the A&M System the following under this Agreement for Services:

8. An inventory of high impact information resources and networks within Client network at least annually.

9. Response to each escalated threat indicator notification with validation of the Cyber Ops' assessment within 72 hours of resolution.