Agreement
Between
The State of Arizona Department of Homeland Security
And
City of Yuma (each, a "Party")

Recitals:

a. State of Arizona Department of Homeland Security (hereinafter “AZDOHS”) is an agency of the State of Arizona and operating pursuant to Title 41 of the Arizona Revised Statutes.

b. City of Yuma (hereinafter “Yuma”) is a political subdivision of the State of Arizona.

c. AZDOHS, pursuant to Arizona Revised Statutes (hereinafter “ARS”) 41-4282, is responsible for the State of Arizona’s enterprise cyber security strategy, manages the Statewide Cyber Readiness Program (hereinafter “Program”), and possesses certain skills, tactics, techniques and procedures and other Confidential Information pertaining to certain cyber readiness operations and the administration thereof as further defined in this Agreement (hereinafter, “Agreement”), which AZDOHS desires to share with Yuma and/or use to aid Yuma and its cyber operations, pursuant to the direction of the Governor of the State of Arizona. AZDOHS selects, procures, and funds one or more cyber readiness products which may change over time depending on the evolution of cyber security requirements (hereinafter “Products”) offered through the Program. AZDOHS desires to assist Yuma in Yuma’s use of one or more of the Products, as outlined in this Agreement, which will benefit Yuma’s cyber operations.

d. Yuma has opted to participate in the Program, to deploy and operationalize one or more of the Products, and desires to work with AZDOHS and is seeking assistance from AZDOHS regarding skills, tactics, techniques, and procedures pertaining to the Products, as outlined in this Agreement, which also will benefit AZDOHS.

Based upon the mutual promises contained in this Agreement, the Parties hereby agree to be bound as follows:

1. Incorporation of Recitals. The Recitals set forth above are hereby made terms of this Agreement.

2. Definitions.

a. Disclosing Party. A Party to this Agreement, including directors, officers, employees, agents or representatives (collectively, "Representatives"), that discloses Confidential Information to the Receiving Party.

b. Receiving Party. A Party to this Agreement, including its Representatives, that receives Confidential Information from the Disclosing Party.

c. Transaction. Any interaction between the Parties undertaken pursuant to this Agreement regarding a specific cybersecurity event or incident, or the sharing of information about those events.

d. Confidential Information. Confidential Information need not be novel, unique, patentable, copyrightable or constitute a trade secret in order to be designated Confidential Information. Confidential Information is any data or information that is proprietary to the Disclosing Party and not generally known to the public, whether in tangible or intangible form, whenever and however disclosed, including but not limited to:

i. Information relating to the Program, which if made available to a third-party, would have the potential to enable persons or entities who are not parties to this Agreement to weaken, undermine or penetrate any of the Parties' cyber security measures whether or not such cyber security measures are a part of the Program, including but not limited to the skills, tactics, techniques and procedures associated with the Program;

ii. Information relating to the Products, which if made available to a third-party, would have the potential to enable persons or entities who are not parties to this Agreement to weaken, undermine or any of the Parties' cyber security measures whether or not such cyber security measures are a part of the Program, including but not limited to information obtained from or through a governmental or private entity providing one or more Products to the Parties to this Agreement and including but not limited to proprietary information belonging to such governmental or private entity.

iii. Any scientific or technical information, invention, design, process, procedure, formula, improvement, technology or method, which if made available to a third-party, would have the potential to enable persons or entities who are not parties to this Agreement to weaken, undermine or penetrate any of the Parties' cyber security measures whether or not such cyber security measures are a part of the Program;

iv. Any concepts, reports, data, know-how, tactics, techniques, procedures, works-in progress, designs, development tools, specifications, computer software, source code, object code, flow charts, databases, inventions, information and trade secrets, which if made available to a third-party, would have the potential to enable persons or entities who are not parties to this Agreement to weaken, undermine or penetrate any of the Parties' cyber security measures whether or not such cyber security measures are a part of the Program;

v. Any internal data, user id's, passwords, configuration settings, infrastructure design, non-public employee information, personal identifiable information, or any other data maintained by a Disclosing Party to fulfill any of its functions, which if made available to a third-party, would have the potential to enable persons or entities who are not parties to this Agreement to weaken, undermine or penetrate any of the Parties' cyber security measures whether or not such cyber security measures are a part of the Program; and

vi. Any other information that should reasonably be recognized as confidential information of the Disclosing Party, which if made available to a third-party, would have the potential to enable persons or entities who are not parties to this Agreement to weaken, undermine or penetrate any of the Parties' cyber security measures whether or not such cyber security measures are a part of the Program.

3. Purpose. The purpose of this Agreement is to establish policies and procedures under which AZDOHS will provide Products to Yuma and assist Yuma with its participation in the Program. In furtherance of this purpose, the Parties further agree:

a. That the Products will be provided to Yuma as a hosted solution in a multi-customer environment. AZDOHS personnel will have administrative access to the Product(s) to provide deployment and operational support to Yuma.

b. That AZDOHS personnel with administrative access to the Product(s) will protect administrative credentials against unauthorized use and access by employing protection measures in compliance with State of Arizona Statewide Information Security Policies, Standards, and Procedures (available at https://azdohs.gov/information-security-policies-standards-and-procedures). Documentation of this will be provided by AZDOHS to Yuma upon request.

c. That any Products and Product licenses and support provided by AZDOHS other than in response to a request under the Arizona Mutual Aid Compact will be funded by AZDOHS and shall be provided to Yuma at no cost to Yuma and with no requirement for reimbursement from Yuma.

4. Scope of Products and Assistance. Yuma and AZDOHS intend to work together, and AZDOHS will provide Products, Product licenses, and related assistance to Yuma as set forth in Exhibit A to this Agreement. The Parties further agree that:

a. Additional exhibits or modifications and amendments to Exhibit A may be executed in the future. Any such changes will be made in accordance with Section 13 of this Agreement.

b. Yuma shall not request, and AZDOHS shall not provide, any services not in compliance with all State and Federal laws regulating the access to, and utilization of, cyber information.

c. Yuma and AZDOHS understand that AZDOHS will only access and/or make changes to the Products offered to Yuma and/or Product modifications which impact the Yuma with prior notification.

d. The Parties acknowledge that both Parties' records are subject to Arizona public records law and agree that in the event that either Party receives a public records request, subpoena, or other request or demand for records relating to the matters addressed in this Agreement, (1) the Party receiving the public records request, subpoena, or other request or demand for such records shall immediately notify the other Party and provide the other Party with a copy of the public records request, subpoena, or other request or demand for such records; and (2) the Parties shall communicate and cooperate with each other in responding to and/or resisting the public records request, subpoena, or other request or demand for such records, except that each Party shall retain the right to assert its own independent position on whether a record or portion of a record should or should not be produced. The Parties further agree:

i. AZDOHS may review alerts, statistical data, and other data collected to support the Program.

ii. Yuma agrees that AZDOHS may report summary Program metric data to State executive leadership for the purposes of demonstrating the effectiveness and completeness of implementation of the Program.

iii. Yuma agrees that AZDOHS may report aggregated and anonymized information (including but not limited to threat intelligence and technical indicators) to other AZDOHS strategic partners for the purposes of information sharing and furthering the mission of AZDOHS and the Program.

e. Yuma will permit AZDOHS personnel access to Yuma's systems and information as AZDOHS deems necessary. AZDOHS agrees to access Yuma's systems only with prior notification to Yuma and solely for serving the purposes of the Program.

5. Obligations Specific to Yuma. Yuma understands and acknowledges that participation in the Program is voluntary. The Parties agree that Yuma will:

a. Assign primary technical and executive Points of Contacts ("POCs") for coordination with AZDOHS regarding all Products, Product licenses, and related assistance as set forth in this Agreement. The Yuma's technical POCs will coordinate with AZDOHS for Yuma's participation in the Program including but not limited to deployment and operation of the Products. Yuma shall report to AZDOHS any change in the POCs' identity or the POCs' contact information in a timely manner.

b. Utilize Products and the Program to reduce Yuma's cybersecurity risk, and reasonably collaborate with AZDOHS and other participating agencies to improve the Program.

c. Make consistent progress with deployment of the Products and licenses and will maintain regular and open communications with AZDOHS as appropriate. Failure to communicate with AZDOHS is grounds for AZDOHS to reallocate Yuma's Product licenses to other Program participants.

d. Participate in surveys and provide feedback to AZDOHS to improve the Program.

e. Comply with all end user license agreements required by the Product manufacturers.

f. Agree that any additional add-on options for Products, not already available under the Product portfolio, must be approved by the Arizona State and Local Cybersecurity Program Planning Committee (hereinafter "Committee"). The Committee will include representatives from Arizona local governments, tribal governments, and K-12 public school districts. The mission of the Committee will be to ensure greatest value for the Program participating agencies, approve annual purchases, authorize changes to the portfolio of services offered, oversee operations, and suggest improvements to the Program. The Yuma is solely responsible for the funding, procurement, and implementation of all such add-on options.

g. Be permitted to disclose the following items to any person at any time:

i. The fact that Yuma has entered into this Agreement and the details of this Agreement.

ii. A description of Yuma's participation in the Program as stated in this Agreement.

6. Obligations Specific to AZDOHS. AZDOHS, under direction of the Governor of the State of Arizona, has the mission to assist Arizona local governments, tribal governments, and K12 public school districts to reduce cybersecurity risk and to reduce the impact of cyber-attacks. AZDOHS accomplishes this mission, in part, through the Program. Accordingly, the Parties agree that AZDOHS will:

a. Establish a governance program for the Program, to be overseen by the Committee.

b. Make efforts to maintain current, and identify future, funding sources to continue purchasing and maintaining the Program and Products.

c. If funding is discontinued, AZDOHS will make efforts to ensure Yuma has time to plan for a transition of cybersecurity services.

d. Conduct all procurements relating to the subject matter of this Agreement unless otherwise provided in Section 5(f).

e. Communicate to Yuma all significant changes to the Program that could affect Yuma.

f. Acknowledge that data created by or transferred to Yuma's Product environment is owned by Yuma. AZDOHS will provide Yuma's data to Yuma upon termination of this Agreement and participation in the Program as feasible.

g. Communicate system changes to the Product to the Committee and to Yuma 48 hours prior to the change being made, with exception that in the event of an emergency, AZDOHS will make efforts to communicate, but will make emergency changes without prior communication if AZDOHS determines this is necessary.

h. Communicate changes to Yuma’s Product environment and related information to Yuma 48 hours prior to the change being made, with exception that in the event of an emergency, AZDOHS will make efforts to communicate, but will make emergency changes without prior communication if AZDOHS determines this is necessary.

i. Notify Yuma in writing promptly upon the discovery of a system breach or other unauthorized access and/or change to Yuma‘s Products, but in no case later than 48 hours after discovery of a breach or other unauthorized access.

j. Make efforts to assist Yuma with its regulatory compliance requirements in relation to the Products.

7. Use of Confidential Information. A Receiving Party agrees to use Confidential Information solely in connection with the Program and not for any purpose other than as authorized by this Agreement without the prior written consent of an authorized representative of the Disclosing Party.

8. Disclosure of Confidential Information. A Disclosing Party may disclose Confidential Information to the Receiving Party. The Receiving Party will:

a. Except as provided in Sections 4(d) and 5(g) of this Agreement, limit disclosure of any Confidential Information to only those within its control (i) who have executed a Non-Disclosure Agreement protecting Confidential Information to at least the same extent as this Agreement and (ii) who have a need to know such Confidential Information in connection with the relationship between the Parties under this Agreement. Each Non-Disclosure Agreement between a Party to this Agreement and a third-party shall include language providing that (a) the Party to this Agreement signing a Non-Disclosure Agreement with a third-party shall immediately provide a copy of that Non-Disclosure Agreement to the other Party to this Agreement, and (b) either Party to this Agreement shall have the right to enforce that Non-Disclosure Agreement with that third-party.

b. Advise its personnel and representatives of the confidential nature of Confidential Information and of the obligations set forth in this Agreement.

c. Be under no obligation with respect to any information:

i. Which is, at the time of disclosure, available to the general public; or which at a later date becomes available to the general public through no fault of Receiving Party, but only after that later date;

ii. Which Receiving Party can demonstrate was in its possession before receipt of the information from Disclosing Party, which can be proven by written records or other competent evidence;

iii. Which was developed independently by Receiving Party without reference to the information provided by Disclosing Party;

iv. Which is disclosed to Receiving Party without restriction on disclosure by a third-party who has the lawful right to disclose such information;

v. Which is required to be disclosed pursuant to any applicable law or regulation, or pursuant to any governmental, judicial, or administrative order, subpoena, discovery request, regulatory request, or similar method, except as provided in Section 4(d) of this Agreement.

9. Return of Confidential Information. Receiving Party shall immediately return and redeliver to the other Party all tangible material embodying Confidential Information received hereunder and all notes, summaries, memoranda, drawings, manuals, records, excerpts or derivative information deriving there from and all other documents or materials ("Notes") (and all copies of any of the foregoing, including “copies” that have been converted to computerized media in the form of image, data or word processing files either manually or by image capture) based on or including any Confidential Information, in whatever form of storage or retrieval, upon the earlier of:

a. The completion or termination of the dealings between the Parties contemplated hereunder;

b. The termination of this Agreement; or,

c. At such time as the Disclosing Party may so request.

Provided however that the Receiving Party may retain such of its records as is necessary to enable it to comply with its record retention obligations and policies.

10. Notice of Breach. Receiving Party shall notify the Disclosing Party immediately upon discovery of any unauthorized use or disclosure of Confidential Information by Receiving Party or its Representatives, or any other breach of this Agreement by Receiving Party or its Representatives, and will cooperate with efforts by the Disclosing Party to help the Disclosing Party regain possession of Confidential Information and prevent its further unauthorized use.

11. Limitation of Agreement. The Parties agree that neither Party will be under any legal obligation of any kind whatsoever with respect to a Transaction by virtue of this Agreement, except for the matters specifically agreed to herein. This Agreement does not create a joint venture or partnership between the Parties.

12. Term. This Agreement shall commence on the date of the last signature herein below, and shall end ten (10) years from such date, unless terminated or extended as set forth in Section 14 of this Agreement.

13. Modifications to this Agreement. Any amendments or changes to this Agreement, including but not limited to amendments or changes to Exhibit A hereto, must be in writing and signed by authorized representatives of both Parties.

14. Termination. Either Party may terminate this Agreement by giving 30 days written notice to the other Party. Such termination notice period shall not commence until receipt of the written notice by the other Party. Access to systems will not be terminated by either Party without prior agreement of both Parties.

15. Disclaimer of Liability. In no event shall the State of Arizona, AZDOHS, the Program or their employees, members, agents, servants, independent contractors or suppliers be liable to Yuma or any third parties affected by the actions taken by AZDOHS pursuant to this Agreement for any damages of any kind whatsoever, including, but without limitation, damages for loss of profits, business interruption, loss of information, disclosure of confidential or private information, or other losses, including pecuniary loss arising out of training conducted pursuant to this Agreement or for special, indirect, consequential, incidental, or punitive damages however caused, and regardless of the theory of liability. In no event shall the City of Yuma, their employees, members, agents, servants, independent contractors or suppliers be liable to ASDOHS or any third parties affected by the actions taken by Yuma pursuant to this Agreement for any damages of any kind whatsoever, including, but without limitation, damages for loss of profits, business interruption, loss of information, disclosure of confidential or private information, or other losses, including pecuniary loss arising out of or pursuant to this Agreement or for special, indirect, consequential, incidental, or punitive damages however caused, and regardless of the theory of liability.

16. Warranty. Each Party warrants that it has the right to make the disclosures called for under this Agreement. NO OTHER WARRANTIES ARE MADE BY EITHER PARTY UNDER THIS AGREEMENT WHATSOEVER. The Parties acknowledge that although they shall each endeavor to include in Confidential Information all information that they each believe relevant for the purpose of the evaluation of a Transaction, the Parties understand that no representation or warranty as to the accuracy or completeness of Confidential Information is being made by either Party as the Disclosing Party. Neither Party hereto shall have any liability to the other Party or to the other Party's Representatives resulting from any use of Confidential Information except with respect to disclosure of such Confidential Information in violation of this Agreement.

17. Severability. In the event that any provision or Section herein is held invalid or unenforceable, the remaining provisions and Sections shall remain in full force and effect.

18. No Indemnification. Neither Party shall indemnify or hold harmless the other Party.

19. Funding. Every obligation of AZDOHS under this Agreement is conditioned upon the availability of funds appropriated and allocated for the payment of such obligation. If funds are not appropriated, allocated and available or if the appropriation is changed by the Legislature resulting in funds no longer being available for the continuance of this Agreement, this Agreement may be terminated by AZDOHS or Yuma at the end of the period for which funds are available. No liability shall accrue to AZDOHS or any other agency of the State of Arizona in the event this provision is exercised, and neither AZDOHS nor any other agency of the State of Arizona shall be obligated or liable for any future payments or for any damages as a result of termination under this paragraph.

20. Conflict of Interest. The requirements of ARS § 38-511 apply to this Agreement. Either Party may cancel this Agreement, without penalty or further obligation, if any person significantly involved in initiating, negotiating, securing, drafting or creating this Agreement on behalf of that Party is, at any time while this Agreement or any extension is in effect, an employee, agent or consultant of the other Party with respect to the subject matter of this Agreement.

21. Governing Law. This Agreement shall be construed in accordance with the laws of the State of Arizona, without regard to its conflict of laws provisions.

22. Dispute Resolution. The Parties agree to resolve all disputes arising out of or relating to this Agreement through arbitration, after exhausting applicable administrative review, to the extent required by ARS § 12-1518, except as may be required by other applicable statutes.

23. Forum. The forum for any dispute arising out of this Agreement shall be Maricopa County, Arizona.

24. Entire Agreement. This Agreement constitutes the entire agreement between the Parties and supersedes any other written or oral agreement between the Parties with respect to the subject matter of this Agreement.

25. Rule of Construction. Any rule of construction to the effect that ambiguities are to be resolved against the drafting Party shall not apply in interpreting this Agreement.

26. Further Actions. Each Party hereby agrees to perform any further acts and to execute and deliver any documents that may be reasonably necessary to carry out the provisions of this Agreement.

27. Compliance with All Applicable Law. The Parties agree to comply with all federal, state or local laws, rules or regulations applicable to the subject matter of this Agreement.

28. Independent Status. The Parties are independent contractors, and nothing contained in this Agreement creates a relationship of partnership, joint venture, agency, or employment between the Parties or any of their employees, officers, agents, or contractors.

29. Execution. This Agreement may be executed in one or more counterparts, each of which will be deemed to be an original, but all of which together will constitute a single instrument. A signature on a counterpart may be made by facsimile or otherwise electronically transmitted, and such signature shall have the same force and effect as an original signature. Further, this Agreement may be retained in any electronic format, and all electronic copies thereof shall likewise be deemed to be an original and shall have the same force and effect as an original copy of this Agreement.

30. No Third-party Beneficiaries. This Agreement will inure exclusively to the benefit of and be binding upon AZDOHS and Yuma as the only parties to this Agreement, and to their respective successors, assigns, executors and legal representatives. Except as expressly provided in this Agreement, nothing in this Agreement confers on any person other than the Parties hereto or their respective successors and assigns, any rights, remedies, obligations, or liabilities.

31. Separate Responsibility. Except as expressly provided in this Agreement, each Party agrees that, to the extent authorized by law, it will be responsible for its own acts or omissions and the results thereof and will not be responsible for the acts or omissions of the other Party and the results thereof. In the event that either Party becomes aware of any claim made by or expected from a claimant against a Party to this Agreement, which claim relates to the subject matter of this Agreement, that Party will immediately notify the other Party, and the Parties will share all information regarding such matter and cooperate with each other in addressing the matter.

32. Waiver. Any failure by either Party to enforce the other Party's strict performance of any provision of this Agreement will not constitute a waiver of its right to subsequently enforce such provision or any other provision of this Agreement. It is expressly agreed that in the execution of this Agreement, no Party waives nor shall be deemed hereby to waive any immunity or defense that would otherwise be available to it against claims arising in the exercise of governmental powers and functions.

33. Assignment. Neither Party may directly or indirectly assign or transfer its rights and/or obligations under this Agreement by operation of law or otherwise without the prior written consent of the other Party.

34. Force majeure. The Parties shall exercise their best efforts to meet their respective duties and obligations as set forth in this Agreement, but shall not be held liable for any delay or omission In performance due to force majeure or other causes beyond their reasonable control (force majeure), including, but not limited to, compliance with any government law, ordinance or regulation, acts of God, acts of the public enemy, fires, strikes, lockouts, natural disasters, wars, riots, material or labor restrictions by any governmental authority, transportation problems and/or any other similar causes.

35. Publicity. No Party shall use or mention in any publicity, advertising, promotional materials or news release the name or service mark(s) of the other Party without the prior written consent of that Party.

IN WITNESS WHEREOF, the Parties hereto have executed this Agreement on the ______ day of ______________________, 20______.

Arizona Department of Homeland Security	City of Yuma
________________________________ Signature	_________________________________ Signature
________________________________ Name	John D. Simonton _________________________________ Name
________________________________ Title	Acting City Administrator _________________________________ Title
________________________________Date	_________________________________ Date

10966925.2

Agreement
Between
The State of Arizona Department of Homeland Security
And
City of Yuma (also referred to as “Yuma”)

EXHIBIT A

Products provided by AZDOHS to Yuma under this Exhibit A are as follows:

Products	Description
Advanced Endpoint Protection / Endpoint Detection & Response	Advanced Endpoint Protection (AEP) is next-generation antivirus protection that leverages artificial intelligence and machine learning to identify malware before it executes. Endpoint Detection and Response (EDR), also referred to as endpoint detection and threat response (EDTR), is an endpoint security solution that continuously monitors end-user devices to detect and respond to cyber threats like ransomware and malware.
Anti-Phishing / Security Awareness Training	Anti-phishing training provides employees with examples of how to spot phishing attempts and suspicious emails requesting sensitive information from users or infecting systems with malware. This includes sending emails to employees with fake links, mimicking real phishing attempts from outside threats. Employees who click on simulated links will be prompted to complete security awareness training. Security Awareness Training (SAT) features user-friendly online training courses that cover the latest cybersecurity best practices to educate employees on how to keep data and devices safe.
Converged Endpoint Management	Converged Endpoint Management (XEM) platforms provide unrivaled access to real-time asset visibility and the ability to patch at scale with certainty (including devices that are on or off-network or VPN). XEM brings IT Operations, Security, and Risk Management teams together – with a single platform for complete visibility, control, and trust in IT decision-making.
Multi-Factor Authentication	Multi-Factor Authentication (MFA) is a security system that requires more than one method of authentication to verify a user's identity for a login or other transaction. Categories for authentication may include knowledge (something a user knows), possession (something a user has), and inherence (something a user is). MFA provides an extra layer of security to prevent unauthorized access to systems.
Web Application Firewall	Web Application Firewall (WAF) is an application firewall for HTTP applications. It applies a set of policies to help protect web applications from common web exploits that could affect an application’s availability and compromise data.