Participating Addendum Number 505ENT-O26-NASPOITRSRC-02

for
Procurement Assistance Support Services and IT Research, Advisory, and Consulting (IT RAC) Services
between
The State of Wisconsin
and
Gartner, Inc

This Participating Addendum is entered into by the State of Wisconsin ("Participating Entity") and the following Contractor (each a "Party" and collectively the "Parties") for the purpose of participating in NASPO ValuePoint Master Agreement Number **DPC-1428523190-SA-21-PASS_ITRAC**, executed by Contractor and the State of North Carolina ("Lead State") for Procurement Assistance Support Services (PASS) and IT Research, Advisory, and Consulting (IT RAC) services ("Master Agreement"):

Gartner, Inc ("Contractor")
325 N Salisbury St.
Raleigh, NC 27603

I. PARTICIPATING ADDENDUM CONTACTS.

Contractor's contact for this Participating Addendum is:

Will McGuire
Contract Manager
will.mcguire@gartner.com
(571) 683-4482

Participating Entity's contact for this Participating Addendum is:

Susanne Matschull
IS Comp. Services Specialist
Susanne.matschull@wisconsin.gov
608-266-9796

II. TERM. This Participating Addendum is effective as of the date of the last signature below or **January 19, 2026**, whichever is later, and will terminate upon termination of the Master Agreement, as amended, unless the Participating Addendum is terminated sooner in accordance with the terms set forth herein.

III. PARTICIPATION AND USAGE. This Participating Addendum may be used by all state agencies, institutions of higher education, cities, counties, districts, and other political subdivisions of the state, and nonprofit organizations within the state if authorized herein and by law. Participating Entity has sole authority to determine which entities are eligible to use this Participating Addendum. If Contractor becomes aware that an entity's use of this Participating Addendum is not authorized, Contractor will notify NASPO ValuePoint to initiate outreach to the appropriate parties.

IV. GOVERNING LAW. The construction and effect of this Participating Addendum and any Orders placed hereunder will be governed by, and construed in accordance with, Participating Entity's laws.

V. SCOPE. Except as otherwise stated herein, this Participating Addendum incorporates the scope, pricing, terms, and conditions of the Master Agreement and the rights and obligations set forth therein as applied to Contractor and Participating Entity and Purchasing Entities. **Contractor may provide any products and/or services it was awarded and as described in the Master Agreement.**

a. **Products.** All products available through the Master Agreement may be offered and sold by Contractor to Purchasing Entities.

b. **Services.** All services available through the Master Agreement may be offered and sold by Contractor to Purchasing Entities.

c. **Contractor Partners**. All subcontractors, dealers, distributors, resellers, and other partners identified on Contractor's NASPO ValuePoint webpage as authorized to provide Products and Services to Participating Entity may provide Products and Services to users of this Participating Addendum. Contractor will ensure that the participation of Contractor's subcontractors, dealers, distributors, resellers, and other partners is in accordance with the terms and conditions set forth in the Master Agreement and in this Participating Addendum.

Any amendment to the Master Agreement shall be deemed incorporated into this Participating Addendum unless the amendment is rejected by Participating Entity in writing to Contractor within fifteen (15) calendar days of the amendment's effective date and is documented thereafter via written amendment hereto.

Any conflict between this Participating Addendum and the Master Agreement will be resolved in favor of the Participating Addendum. The terms of this Participating Addendum, including those modifying or adding to the terms of the Master Agreement, apply only to the Parties and shall have no effect on Contractor's participating addenda with other participating entities or Contractor's Master Agreement with the Lead State.

VI. ORDERS. Purchasing Entities may place orders under this Participating Addendum by referencing the Participating Addendum Number on an Order, 505ENT-O26-NASPOITRSRC-02. Each Order placed under this Participating Addendum is subject to the pricing and terms set forth herein and in the Master Agreement, including applicable discounts, reporting requirements, and payment of administrative fees to NASPO ValuePoint and Participating Entity, if applicable.

VII. FEDERAL FUNDING REQUIREMENTS. Orders funded with federal funds may have additional contractual requirements or certifications that must be satisfied at the time the Order is placed or upon delivery. When applicable, a Purchasing Entity will identify in the Order any alternative or additional requirements related to the use of federal funds. By accepting the Order, Contractor agrees to comply with the requirements set forth therein.

VIII. ATTACHMENTS. This Participating Addendum includes the following attachments:

a. Attachment A: State of Wisconsin Modifications and Additions to Master Agreement Terms and Conditions
b. Attachment B: State of Wisconsin Security Rider

IX. NOTICE. Any notice required herein shall be sent to the following:

For Contractor:

Will McGuire
Contract Manager
will.mcguire@gartner.com
(571) 683-4482

For Participating Entity:

Susanne Matschull
IS Comp Services Specialist
Susanne.matschull@wisconsin.gov
608-266-9796

X. SUBMISSION OF PARTICIPATING ADDENDUM TO NASPO VALUEPOINT. Upon execution, Contractor shall promptly email a copy of this Participating Addendum and any amendments hereto to NASPO ValuePoint at pa@naspovaluepoint.org. The Parties acknowledge and agree that the Participating Addendum, as amended, may be published on the NASPO ValuePoint website.

SIGNATURE

The undersigned for each Party represents and warrants that this Participating Addendum is a valid and legal agreement binding on the Party and enforceable in accordance with the Participating Addendum's terms and that

the undersigned is duly authorized and has legal capacity to execute and deliver this Participating Addendum and bind the Party hereto.

IN WITNESS WHEREOF, the Parties have executed this Participating Addendum.

CONTRACTOR:

Signed by:
Ashley Beluch
4351ACB10518430...

Signature

Ashley Beluch

Printed Name

Senior Contracts Specialist

Title

4/8/2026 | 9:53 AM CDT

Date

PARTICIPATING ENTITY:

Signed by:
Anne Hanson
9C8FD2F019F84E0...

Signature

Anne Hanson

Printed Name

Deputy Secretary

Title

4/13/2026 | 11:23 PM CDT

Date

ATTACHMENT A: STATE OF WISCONSIN MODIFICATIONS AND ADDITIONS TO MASTER AGREEMENT TERMS AND CONDITIONS

(Contract #505ENT-O26-NASPOITRSRC-02)

1. **DEFINITIONS.** Words and terms shall be given their ordinary and usual meanings. Unless negotiated otherwise by the parties, where capitalized, the following words and terms shall have the meanings indicated. The meanings shall be applicable to the singular, plural, masculine, feminine and neuter.

   "Acceptance" means a manifestation of assent by the State to the terms, Services, Deliverables or other items offered by the Contractor under the Contract after Inspection by the State.

   "Agency" or "State Agency" means an office, department, agency, institution of higher education, association, society or other body in the State of Wisconsin government created or authorized to be created by the State Constitution or any law, which is entitled to expend moneys appropriated by law, including the legislature and the courts, but not including an authority, as defined in Wis. Stat. s. 16.70(2).

   "**Business Day**" means any day on which the Contracting Agency is open for business.

   "**Confidential Information**" means all tangible and intangible information and materials being disclosed in connection with this Contract, in any form or medium without regard to whether the information is owned by the State or by a third party, which satisfies at least one of the following criteria: (i) Personally Identifiable Information; (ii) Proprietary Information; (iii) non-public information related to the State's employees, customers, technology (including data bases, data processing and communications networking systems), schematics, specifications, and all information or materials derived therefrom or based thereon; or (iv) information expressly designated as confidential in writing by the State. Confidential Information includes all information that is restricted or prohibited from disclosure by state or federal law.

   "Contracted Personnel" means a Contractor's employees or other personnel (including officers, agents and Subcontractors) provided by the Contractor specifically to render Services under this Contract.

   "Contracting Agency" means the Agency entering into this Contract on behalf of the State.

   "Day" means calendar day unless otherwise specified in this Contract.

   "Default" means the omission or failure to perform a contractual duty or provide Deliverables or render Services as contractually required.

   "Deliverables" means all project materials, including Goods, software licenses, data, and documentation originally created during the rendering of Services hereunder. Such Deliverables shall be the property of the State of Wisconsin unless otherwise specified in the Contract.

   "**Goods**" means articles of trade or items of merchandise, supplies, raw materials, or finished products, and may also include incidental or related services as the situation may require.

"Inspection" means an examination of Deliverables or Services provided under this Contract.

"Key Personnel" means specifically identified Contracted Personnel that play a lead and critical role in rendering Services during the Contract term.

"Personally Identifiable Information" means an individual's last name and the individual's first name or first initial, in combination with and linked to any of the following elements, if that element is not publicly available information and is not encrypted, redacted, or altered in any manner that renders the element unreadable: (a) the individual's Social Security number; (b) the individual's driver's license number or state identification number; (c) the number of the individual's financial account, including a credit or debit card account number, or any security code, access code, or password that would permit access to the individual's financial account; (d) the individual's DNA profile; or (e) the individual's unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation, and any other information protected by state or federal law.

"Proprietary Information" means information, including a formula, pattern, compilation, program, device, method, technique or process to which all of the following apply:

a. The information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use.

b. The information is the subject of efforts to maintain its secrecy that are reasonable under the circumstances.

"Properly-submitted Invoice" is one that is submitted in accordance with instructions contained on the State's Purchase Order, includes a reference to the proper Purchase Order number, and is submitted to the proper address for processing.

"Purchase Order" means the State's standard document of a purchase of Deliverables and Services.

"Services" means all work performed, and labor, actions, recommendations, plans, research, customizations, modifications, documentation, and maintenance and support provided by the Contractor necessary to fulfill that which the Contractor is obligated to accomplish under this Contract.

"SOW" means Statement of Work.

"State" means the State of Wisconsin.

"Subcontract" means an agreement, written or oral between the Contractor and any other party to fulfill the requirements and performance obligations of this Contract.

"Subcontractor" means an entity that enters into a Subcontract with the Contractor for the purpose of delivering Deliverables or rendering Services to the State.

2. **APPLICABLE LAW.** This Contract shall be governed by the laws of the State of Wisconsin. Venue for any action brought under this Contract shall lie in Madison, Dane County, Wisconsin.

3. **TERMINATION FOR CAUSE.** The State may terminate this Contract after providing the Contractor with thirty (30) Days' written notice of the Contractor's right to cure a failure of the Contractor to perform under the terms of this Contract.

   The Contractor may terminate this Contract after providing the State with ninety (90) Days' written notice of the State's right to cure a failure of the State to perform under the terms of this Contract.

4. **TERMINATION FOR CONVENIENCE.** The State may terminate this Contract at any time, without cause, by providing a written notice to the other party at least ninety (90) Days in advance of the intended date of termination.

   Contractor may terminate this Contract at any time, without cause, by providing a written notice to the other party at least ninety (90) Days in advance of the intended date of termination.

   In the event of a termination, the Contractor shall be entitled to receive compensation for any completed or partially completed Services rendered or Deliverables provided under the Contract up to the date of termination. Compensation for partially completed Services shall be no more than the percentage of completion of the Services requested, as determined by the State in its sole discretion, multiplied by the corresponding payment for completion of such Services as set forth in the Contract. Alternatively, at the sole discretion of the State, the Contractor may be compensated for the actual Service hours provided up to the date of termination. The State shall be entitled to a refund for Deliverables or Services paid for but not received or rendered, such refund to be paid within 30 Days of written notice to the Contractor requesting the refund.

5. **CONTRACT CANCELLATION:**

   (a) The State reserves the right to cancel this Contract in whole or in part without penalty, and without prior notice, if the Contractor:

   - Files a petition in bankruptcy, becomes insolvent, or otherwise takes action to dissolve as a legal entity
   - Makes an assignment for the benefit of creditors
   - Fails to maintain and keep in force all required insurance, permits and licenses as provided in this Contract;
   - Fails to maintain the confidentiality of the State's information that is considered to be Confidential Information, or
   - Performs in a manner that threatens the health or safety of a State employee, citizen, or customer.

   (b) The State reserves the right to cancel this Contract in whole or in part without penalty, with 30 Days' notice, if the Contractor:

   - Fails to follow the sales and use tax certification requirements of s. 77.66 of the Wisconsin Statutes;
   - Incurs a delinquent Wisconsin tax liability;
   - Fails to submit a non-discrimination or affirmative action plan as required herein.

- Fails to follow the non-discrimination or affirmative action requirements of subch. II, Chapter 111 of the Wisconsin Statutes (Wisconsin's Fair Employment Law); or
- Becomes a state or federally debarred contractor.

(c) The State reserves the right to cancel this Contract in whole or in part without prior notice, penalty or liability, in accordance with the terms of no. 9, "Non-Appropriation."

6. **POST CONTRACT OBLIGATIONS.** Upon the termination of this Contract for any reason, or upon Contract expiration, each party shall be released from all obligations to the other party arising after the date of termination or expiration, except for those that by their terms survive such termination or expiration.

7. **CONTRACTOR COMPLIANCE AND RESPONSIBILITY FOR ACTIONS.** The Contractor shall at all times comply with and observe all federal, state, and local laws, ordinances, and regulations that are in effect during the term of this Contract that may affect the Contractor's work or obligations hereunder.

   The Contractor shall be solely responsible for its actions and those of its agents, employees, or Subcontractors. Neither the Contractor nor any of the foregoing parties has authority to act or speak on behalf of the State.

8. **DELAY AND REMEDY.** If the Contractor fails to remedy any delay or other problem in its performance of its Contract obligations after receiving thirty (30) day notice from the State to do so, the Contractor shall reimburse the State for all reasonable costs incurred as a direct consequence of the Contractor's delay, action, or inaction. This remedy shall be in addition to any other legal remedies available to the State

9. **NON-APPROPRIATION.** The State reserves the right to cancel this Contract in whole or in part without any penalty or liability whatsoever due to non-appropriation of funds or non-receipt of funds from the Legislature or federal government.

10. **CONTRACTOR'S INSURANCE RESPONSIBILITY.** The Contractor shall maintain the following insurance coverage:
    - Worker's compensation insurance, as required under Chapter 102 of the Wisconsin Statutes, for all of the Contractor's employees and Contracted Personnel engaged in the work performed under this Contract;
    - Commercial liability, bodily injury and property damage insurance against any claim(s) that may occur in carrying out the terms of this Contract, with a minimum coverage of one million dollars ($1,000,000) liability for bodily injury and property damage including products liability and completed operations; and
    - Motor vehicle insurance for all owned, non-owned and hired vehicles that are used in carrying out the terms of this Contract, with a minimum coverage of one million dollars ($1,000,000) per occurrence combined single limit for automobile liability and property damage.
    - Certificate of Insurance, showing up-to-date coverage, shall be on file in the Contracting Agency before the Contract may commence. (if applicable)

- Cyber Liability for two million dollars ($2,000,000). Cyber liability coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by supplier in this agreement and shall include, but not be limited to, claims involving system failure, data recovery, business interruption, cyber extortion, social engineering, infringement of intellectual property, including but not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, and alteration of electronic information. The policy shall provide security breach response costs, regulatory fines, and penalties as well as credit monitoring expenses. Such insurance shall be maintained in force at all times during the term of the agreement and for a period of two years thereafter for services completed during the term of the agreement

The State reserves the right to require higher or lower insurance limits, where warranted.

11. NONDISCRIMINATION AND AFFIRMATIVE ACTION. In connection with the performance of work under this contract, the contractor agrees not to discriminate against any employee or applicant for employment because of age, race, religion, color, handicap, sex, physical condition, developmental disability as defined in s. 51.01(5), Wis. Stats., sexual orientation as defined in s. 111.32(13m), Wis. Stats., or national origin. This provision shall include, but not be limited to, the following: employment, upgrading, demotion or transfer; recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training, including apprenticeship. Except with respect to sexual orientation, the contractor further agrees to take affirmative action to ensure equal employment opportunities.

11.1. Contracts estimated to be over fifty thousand dollars ($50,000) require the submission of a written affirmative action plan by the contractor. An exemption occurs from this requirement if the contractor has a workforce of less than fifty (50) employees. Within fifteen (15) working Days after the contract is awarded, the contractor must submit the plan to the contracting state agency for approval. Instructions on preparing the plan and technical assistance regarding this clause are available from the contracting state agency.

11.2. The contractor agrees to post in conspicuous places, available for employees and applicants for employment, a notice to be provided by the contracting state agency that sets forth the provisions of the State of Wisconsin's nondiscrimination law.

11.3. Failure to comply with the conditions of this clause may result in the contractor's becoming declared an "ineligible" contractor, termination of the contract, or withholding of payment.

11.4. Pursuant to s. 16.75(10p), Wis. Stats., contractor agrees it is not, and will not for the duration of the contract, engage in a prohibited boycott of the State of Israel as defined in s. 20.931(1)(b). State agencies and authorities may not execute a contract and reserve the right to terminate an existing contract with a company that is not compliant with this provision. This provision applies to contracts valued $100,000 or over.

11.5. Pursuant to 2019 Wisconsin Executive Order 1, contractor agrees it will hire only on the basis of merit and will not discriminate against any persons performing a contract, subcontract or grant because of military or veteran status, gender identity or expression, marital or familial status, genetic information or political affiliation.

12. STATE PAYMENT OFFSETS FOR CONTRACTOR'S DELINQUENCY. The State shall offset payments made to the Contractor under this Contract in an amount necessary to satisfy a certified or verifiable delinquent payment owed to the State, or to any state or local unit of government. The State also reserves the right to cancel this Contract as provided in Section 6, Contract Cancellation, if the delinquency is not satisfied by the offset or other means during the term of the Contract.

13. SECURITY OF PREMISES, EQUIPMENT, DATA AND PERSONNEL. During the performance of Services under this Contract, the Contractor may have access to the personnel, premises, equipment, and other property, including data files, information, or materials (collectively referred to as "data") belonging to the State**.** The Contractor shall preserve the safety, security, and the integrity of the personnel, premises, equipment, data and other property of the State, in accordance with the instruction of the State. Contractor shall ensure personnel with access to the State's IT Resources comply with Exhibit A: State's Acceptable Technology Use, Access and Security Policy, the Contractor's published security policy, and its ISO27001 certification**.**

The Contractor shall be responsible for damage to the State's equipment, workplace, and its contents, or for the loss of data, when such damage or loss is caused by the Contractor, Contracted Personnel, or Subcontractors, and shall reimburse the State accordingly upon demand. This remedy shall be in addition to any other remedies available to the State by law or in equity.

14. CONTRACTOR PERSONNEL.

(a) Identification. If requested by the State, the Contractor shall provide a list of the names and addresses of all Contractor's employees, Contracted Personnel, or Subcontractor's employees who may at any time require admission to the State's premises in connection with the rendering of Services, specifying each such person's connection to the Contractor, the role the person is to take in the performance of the Contract, and other particulars as the State may require.

The State reserves the right to refuse to admit to the State's premises any person employed or contracted by the Contractor whose admission, in the sole opinion of the State, would be undesirable.

(b) Right to Approve Changes of Contracted Personnel. The State shall have the absolute right to approve or disapprove a proposed replacement of Key or Contracted Personnel. The Contractor shall provide to the State, in each instance a resume of the proposed substitute and an opportunity to interview that person prior to giving its approval or disapproval. The State shall not unreasonably withhold this approval.

(c) Contracted Personnel Removal. The State may direct the Contractor to remove or reassign Key or Contracted Personnel at the State's discretion; however, the State's right to do so does not implicate the State as a party to any of the Contractor's obligations in the Contract. The State may request that a Contracted Personnel be replaced within ten (10) Business Days from such removal.

(d) Identification of Contracted Personnel. The Contractor shall furnish each Contracted Personnel with a means of identifying themselves as agents, Subcontractors, or employees of the Contractor assigned to perform Services under the Contract, and furnish the State with security credentials on these Contracted Personnel, if requested.

(e) Background or Criminal History Investigation. Prior to the commencement of any Services under this Contract, the State may request a background or criminal history

investigation of Contracted Personnel, and Subcontractor's employees, who will be providing Services to the State under the Contract. If any of the stated personnel providing Services to the State under this Contract is not acceptable to the State in its sole opinion as a result of the background or criminal history investigation, the State may either request immediate replacement of the person, or immediately terminate this Contract and any related Service Agreement.

15. **REMOVAL OF PROHIBITED FOREIGN PRODUCTS STANDARD.** Pursuant to Governor Evers' Executive Order #184, the Removal of Prohibited Foreign Products Standard is intended to provide standardization on the removal of prohibited foreign products and technologies from State of Wisconsin IT Systems. Therefore, Contractors providing Goods and Services under this Contract are prohibited from using the vendors and/or software identified in the Division of Enterprise Technology (DET) IT Security Standards Handbook 290 Removal of Prohibited Foreign Products Standard. Contractors must act as a Prime Contractor who will ensure the Subcontractors, and third parties meet the State of Wisconsin standards throughout the Contract term.

16. **TRANSITION SERVICES.** Upon cancellation, termination, or expiration of this Contract for any reason, the Contractor shall provide such reasonable cooperation, assistance and Services, and shall assist the State in the migration of the State's production operations to the State's control or to the control of an alternative contractor upon written notice to the Contractor at least thirty (30) Business Days prior to termination or cancellation, and subject to the terms and conditions set forth herein. This Contract shall automatically be extended by the number of Days that training or continued Services are necessary to be performed in order to complete the transition. The Contractor's Services required to complete the transition after the notice set forth herein shall be within this Contract's scope and shall not be the subject of any change order. Notwithstanding the foregoing, in no event shall the Contract extend beyond the number of Days permitted by the Master Agreement.

17. **INDEPENDENT CONTRACTOR.** The Contractor shall act as an independent contractor in rendering any and all Services under this Contract and, except as otherwise outlined herein, shall maintain complete control over its employees, Contracted Personnel, and Subcontractors, if any.

18. **COOPERATION WITH OTHER CONTRACTORS.** In the event that the State enters into a contract with another contractor for additional Services, the Contractor shall ensure that Contracted Personnel fully cooperate with such other contractor. Contracted Personnel shall not commit any act that interferes with the rendering of Services by any other contractor or by the State. Contracted Personnel shall cooperate with State personnel, hardware manufacture representatives, system software suppliers, and communications systems suppliers in the provision of Services to the State.

19. **STATE EMPLOYEES.** The Contractor may not contract with or employ a State employee or an individual retained as a full-time contractor by the State during the term of this Contract.

20. **REFUND OF CREDITS.** Within sixty (60) Days of the State's request, the Contractor shall pay to the State any credits resulting from an order that the State determines cannot be applied to future invoices.

21. **PROMPT PAYMENT.** The State shall pay the Contractor's Properly-submitted Invoices within thirty (30) Days of receipt, provided that the Deliverables or Services to be provided to the State

have been delivered, rendered, or installed, and accepted as specified in the solicitation document, Statement of Work (SOW) or this Contract.

If the State fails to pay a Properly-submitted Invoice within thirty (30) Days of receipt, it shall pay a late payment penalty as provided in §16.528, Wis. Stats. However, if the State declares a good faith dispute in regard to an invoice pursuant to §16.528 (3)(e), Wis. Stats., it may pay any undisputed portion of said invoice, and will be exempt from the prompt payment requirement for the disputed portion.

22. STATE TAX EXEMPTION. The State is exempt from payment of Wisconsin sales or use tax on all purchases.

23. CONTRACT DISPUTE RESOLUTION. In the event of any dispute or disagreement between the parties under this Contract, whether with respect to the interpretation of any provision of this Contract, or with respect to the performance of either party hereto, each party shall appoint a representative to meet for the purpose of endeavoring to resolve such dispute or negotiate for an adjustment to such provision. No legal action of any kind, except for the seeking of equitable relief in the case of the public's health, safety or welfare, may begin in regard to the dispute until this dispute resolution procedure has been elevated to the Contractor's highest executive authority and the equivalent executive authority within the Contracting Agency, and either of the representatives in good faith concludes, after a good faith attempt to resolve the dispute, that amicable resolution through continued negotiation of the matter at issue does not appear likely.

(a) No Termination or Suspension of Services: If any problem or dispute arises between the parties, in no event nor for any reason and unless and until authorized by a court of competent jurisdiction, shall Contractor interrupt the performance of the Services or any other obligation hereunder, disable any equipment used in the Services, or perform any other action that prevents, slows down, or reduces in any way the performance of the Services or the State's ability to conduct its business**.**

24. NO GUARANTEE OF QUANTITY. The State may obtain related Deliverables and Services from other sources during the term of this Contract. The State makes no express or implied warranties whatsoever that any particular quantity or dollar amount of Deliverables or Services will be procured through this Contract.

25. TERMINATION OF PURCHASE ORDER. The State may terminate a specific Purchase Order issued under this Contract if it determines that the Contractor is unable to render the Services or provide the Deliverables required in a timely manner, in order to meet the business needs of the State.

26. FORCE MAJEURE. Neither party shall be in Default by reason of any failure in performance of this Agreement in accordance with reasonable control and without fault or negligence on their part. Such causes may include, but are not restricted to, acts of nature or the public enemy, acts of the government in either its sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, freight embargoes and unusually severe weather, but in every case the failure to perform such must be beyond the reasonable control and without the fault or negligence of the party.

27. NO AGENCY RELATIONSHIP. The Contractor shall not take any action, or make any omission, that may imply, or cause others reasonably to infer that the Contractor is acting as the State's agent in any matter or in any way not expressly authorized by this Contract.

28. DISCLOSURE. If a state public official (as defined in §19.42 (14) of the Wisconsin Statutes) or an organization in which a state public official holds at least a 10% interest is or becomes a party to this Agreement, it shall be voidable by the State unless appropriate disclosure is made to the State of Wisconsin Government Accountability Board, 212 East Washington Avenue, Madison, Wisconsin 53703 (Telephone 608-266-8005).

29. WEB CONTENT ACCESSIBILITY GUIDELINES

29.1. Contractor shall comply with the Americans with Disabilities Act (ADA) in a manner consistent with the W3C Web Content Accessibility Guidelines (WCAG), version 2.1 ("WCAG 2.1"), at conformance levels A and AA for all Goods and Services provided under the Contract.

29.2. If during the term of the Contract, the Contractor fails to maintain compliance with WCAG 2.1 A and AA, or the State of Wisconsin identifies an accessibility barrier in the Goods or Services that renders it inaccessible or unusable to people with disabilities, the State of Wisconsin shall notify the Contractor of non-compliance. If conformance is not reached within 30 Days of the Contractor receiving the notification of non-compliance the Contractor and the State of Wisconsin shall meet and mutually agree upon an appropriate timeline for resolution of the accessibility barrier(s). Should Contractor: (i) fail to acknowledge receipt of the notification within 30 Days of receipt, or (ii) fail to materially resolve the accessibility barrier(s) within the agreed-upon timeline, Contractor agrees to indemnify and hold harmless the State of Wisconsin from any claims arising out of its failure to comply with the aforesaid requirements. Failure to comply with these requirements throughout the Contract term may be grounds for cancellation of the Contract by the State of Wisconsin.

29.3. The State of Wisconsin may also require the Contractor to provide an Accessibility Conformance Report (ACR) or Voluntary Product Accessibility Template (VPAT) upon request to demonstrate compliance with this requirement.

30. HIGH-RISK CONTRACTS. Pursuant to Wis. Stat. 16.973(13), The Contractor is required to submit, via the Contracting Agency, to the Department of Administration for approval any order or amendment that would change the scope of the contract and have the effect of increasing the Contract price. The Department of Administration shall be authorized to review the original Contract and the order or amendment to determine whether the work proposed in the order or amendment is within the scope of the original Contract and whether the work proposed in the order or amendment is necessary. The Department of Administration may assist the Contracting Agency in negotiations regarding any change to the original Contract price.

31. OTHER DOCUMENTS. The parties to this Contract understand and agree that standard forms or templates may be used for various purposes, including but not limited to, purchase orders, invoices, quotes, 'Website Terms and/or Conditions' or 'click to accept' agreement(s), some of which may contain boilerplate or standard terms and conditions ("Other Documents"). However, any use of Other Documents are not a part of this Contract and are deemed to be for administrative convenience only and the terms therein are of no effect, have no force of law and do not modify the terms of this Contract.

State of Wisconsin – Acceptable Technology Use, Access, and Security Policy

Effective Date: March 10, 2025

Information for Agency IT:

Legal Authority for, and Applicability of, Policy:

Pursuant to the legal authority and mandates set forth in Wis. Stat. §§ 16.971-16.975, the State of Wisconsin Department of Administration (DOA)'s Division of Enterprise Technology (DET), must, among other duties and responsibilities: 1) ensure that information technology (IT) services and resources are available to all executive branch agencies; 2) prescribe policies, standards, procedures, and safeguards for the security and privacy of the information and data contained within those State-managed IT Resources; and 3) ensure that all executive branch agencies develop and operate with clear guidelines. *See, e.g.,* Wis. Stat. § 16.971(2)(a); §§ 16.973(3), (4), and (5); § 16.974(3).

Accordingly, this enterprise-wide Acceptable Technology Use, Access, and Security Policy shall apply to all executive branch agencies, as defined by Wis. Stat. §§ 16.97(5m) and 16.70(4). This shall not apply to the following: Wisconsin Department of Justice, Wisconsin Department of Military Affairs, State of Wisconsin Investment Board, University of Wisconsin System Board of Regents, and the Wisconsin Technical College System Board.

Policy Exceptions:

With respect to the scope outlined in this policy, these are the minimum DET-established policies, standards, and procedures that all executive branch agencies are required to follow. Agency IT Directors are permitted to develop and implement policies, standards, procedures, or requirements for their users that are more stringent than are set forth in this enterprise policy. Agencies that do so should seek guidance and approval from agency legal counsel before developing and implementing those agency policies, standards, procedures, or requirements, to ensure compliance with any laws or standards applicable to the agency's work.

However, agencies are prohibited from developing or implementing policies, standards, procedures, or requirements that directly conflict with this enterprise policy without first requesting and receiving an exception from DET through established DET processes. Before making the request to DET for an exception, agencies are required to receive approval from their legal counsel to ensure the exception can be implemented consistently with the legal requirements applicable to an agency's work.

Questions regarding the risk exception procedures should be directed to the agency's IT Director (through the agency's service request [SR] process or other established IT processes), or to agency legal counsel.

Information for All Users:

Policy Statement:

The State of Wisconsin uses and manages a variety of IT Resources for its operations. Those State-managed IT Resources (as defined below) include, but are not limited to, information, data, equipment, systems, platforms, applications, and facilities. Users' usage of and access to these State-managed IT Resources has significant benefits for the State's operations and for users themselves (*e.g.,* remote/hybrid work), but also can create significant risks to the State, including IT security risks, as well as other legal, operational, audit, privacy, and financial risks.

Therefore, users' use of State-managed IT Resources comes with the expectation that these resources will be used in a manner consistent with stated policies, laws, and regulations. Using State-managed IT Resources in a manner inconsistent with this policy creates liability, security, privacy, and accountability risks which compromise the services that we provide to the public.

Questions about this policy can be directed to the user's supervisor, agency Human Resources, agency IT Director (through the agency's service request [SR] process or other established IT processes), or agency legal counsel.

Scope of Policy:

The responsibilities outlined in this policy apply to all users who are granted rights to access State-managed IT Resources, including all employees and all other non-employee users who are granted rights to use or access State-managed IT Resources through a contractual relationship or other relationship with the State.

A complete listing of authorized State-managed IT Resources, information, equipment, systems, platforms, applications, and facilities is not feasible or desirable, given that technology, data, and access across the State varies and technology rapidly evolves and changes. However, this policy outlines the authorized access and uses of, and applies to, all State-managed IT Resources used in conducting State business.

This Acceptable Technology Use, Access, and Security Policy primarily pertains to policies, standards, and procedures related to State-managed IT Resources, pursuant to DET's statutory authority. However, it also may include references to work rules,

laws/regulations, and other policies. This policy is not intended to supplant, supersede, or replace other policies; users must ensure that they abide by all relevant work rules, laws/regulations, and other policies that are stated elsewhere.

Definitions:

"*Appropriate Security Measures*" means reasonable technical, physical, and procedural controls to protect data against destruction, loss, alteration, unauthorized disclosure, and unauthorized access, whether by accident or otherwise, by employees or other authorized users including contractors. The State of Wisconsin IT Security Policy Handbook has been developed to provide a baseline of executive branch IT security policies and controls, and can be found here: DET Policies, Standards, and Procedures.

"*Artificial intelligence*" (or "AI") means any IT system or part of an IT system able to perform specific tasks that normally require human intelligence. A complete listing of all such technologies or capabilities is not feasible or desirable, but at present includes capabilities such as visual perception, speech recognition, decision-making, creation of new content, documentation and/or data, and language translation.

"*Authorization*" means the security process that an agency uses to determine a user's or service's level of access, as well as legal authority to access. Agencies have staff defined within their organization to determine the appropriate permissions, access privileges, and/or authorizations to access certain kinds of Non-Public Information (as defined below), or to perform particular actions. Users should direct all questions about authorizations, permissions, access privileges, and security processes to their supervisor, agency Human Resources, agency IT Director (through the agency's service request [SR] process), or agency legal counsel.

"*Enterprise Service Desk*" means the 24x7x365 IT support center providing users with a single point of contact for any Division of Enterprise Technology (DET)-managed or supported IT service.

"*Non-Public Information*" means any sensitive or confidential information whose use, dissemination, disclosure, or re-disclosure is protected, restricted, or prohibited from being disclosed by federal or state laws or regulations, or else should be treated confidentially or restricted pursuant to industry standards, policies, and procedures. Examples of "non-public information" include, but are not limited to, personally identifiable information ("PII"), protected health information ("PHI"), student

educational records or information, financial records or information, social security numbers, driver's license information, federal or state tax information, trade secrets, proprietary information, or attorney-client privileged information.

"*PHI*" or "*Protected Health Information*" has the meaning given in Wis. Stat. § 146.816(1)(f) and 45 C.F.R. § 160.103.

"*PII*" or "*Personally Identifiable Information*" has the meaning given in Wis. Stat. § 19.62(5). PII can also include information that, by itself, is not identifying, but when combined with other information could identify a specific individual.

"*Record*" has the meaning given in Wis. Stat. §§ 16.61(2)(b) and 19.32(2).

"*State*" means the State of Wisconsin.

"*State Credentials*" or "Security Credentials" means a proof of identity, such as passwords, biometrics, X.509, digital certificates, key cards, and USB tokens, which control access to information systems.

"*State-managed IT Resources*" include but are not limited to:

- Any State-provided or State-managed information technology device, which may include a computer, computer monitor, fax machine, copy machine, scanner, multi-function device, printer, camera, cellular telephone, tablet, mobile hotspot, or any other State-provided electronic or mobile device which can send, receive, display, or record data, text, pictures, video, or audio through any medium.

- Any State-provided or State-managed e-mail address or other similar State credentials used to access State-managed IT Resources, software, hardware, information system, cloud computing service, social media platforms, other services connected to or hosted on the State network, or other technology provided by the State to a user, or managed by the State, for work purposes.

- The use of voice or data connectivity through any State-provided or State-managed resource, which includes but is not limited to a wired network, wireless network, mobile hotspot, cellular telephone (including voicemail and other

similar Voice over IP [VoIP] systems), remote desktop or virtual desktop, virtual private network, or any other State-provided or State-managed service.

General Usage:

Users of State-managed IT Resources must abide by the following general provisions while using State-managed IT Resources:

- You shall not knowingly or intentionally use State-managed IT Resources to violate any federal, state, or local laws, regulations, or policies, including the State Employee Code of Ethics.

- You shall not use State-managed IT Resources in a manner inconsistent with the terms and conditions governing their use.

- You acknowledge that State-managed IT Resources are constantly monitored by the State for cybersecurity purposes.

- You acknowledge that you have no expectation of privacy associated with the use of State-managed IT Resources. Any information you send, receive, store, or view on State-managed IT Resources is subject to management review and may be monitored, including websites visited and personal communications, both during and outside of work hours.

- You acknowledge that State-managed IT Resources are the property of the State, including all communications sent or received on behalf of the State. As discussed below, all communications sent or received by users are presumed to be public records subject to release under the Wisconsin Public Records Law.

- You may only access data, documents, correspondence, and other records and information that you have been authorized to access and that are necessary to complete your work for the State of Wisconsin.
    - Access to data, documents, correspondence, and other records and information without authorization or for any other purpose is prohibited.

- You acknowledge that all State-managed IT Resources are subject to intellectual property laws, including patents, copyrights, trademarks, and trade secrets, and shall be used in accordance with relevant laws and regulations.
    - When using State-managed IT Resources with content that may be subject to intellectual property protection (*e.g.,* photos, graphics, recordings,

documents, and other information), you must ensure that you have the necessary permission from the owner to use it.

- You shall only communicate using State-managed IT Resources in a manner that is respectful and professional. Harassment, discriminatory conduct, hate speech, and other offensive behavior are prohibited while using State-managed IT Resources.
    - This also applies if you are using State-managed IT Resources to engage on social media, or if you are engaging on social media using a personal device or account in a way that could be attributed to the State of Wisconsin. *See* Wisconsin Human Resources Handbook Chapter 480 (Social Media Usage in State Government) and other applicable enterprise or agency social media policies.

- You are prohibited from using State-managed IT Resources to download, view, solicit, seek, display, or distribute any obscene, pornographic, offensive, or excessively violent material, unless specifically authorized to perform your work responsibilities for the State of Wisconsin.

Regarding Non-Public Information:

Users of State-managed IT Resources acknowledge that the information, data, and knowledge made available for State-related business purposes must be kept safe, and Non-Public Information must be treated as confidential or sensitive. This is necessary to preserve the integrity of State of Wisconsin operations and services.

- You are prohibited from using, disclosing, communicating, or transmitting Non-Public Information without proper authorization, including but not limited to:
    - Copying or transferring Non-Public Information to any form of removable media (*e.g.,* external hard drives, flash drives) without proper authorization.
    - Revealing Non-Public Information on newsgroups, forums, mailing lists, websites, chat rooms, or other similar public/semi-public forums.
    - Accessing or disclosing Non-Public information for any purpose not related to State business, or for any other non-authorized purpose.

- You shall utilize appropriate security measures for all authorized uses, disclosures, communications, transmissions, copies, or transfers of Non-Public Information.
    - You shall immediately contact your agency IT help desk or the Enterprise Service Desk, as soon as you become aware of any suspected or actual unauthorized use, disclosure, communication, transmission, copy, or transfer of Non-Public Information, including the loss or theft of removable media (*e.g.,* external hard drives, flash drives) which may contain Non-Public Information.
    - You must provide this notification even if the unauthorized use or disclosure was inadvertent or accidental. This will allow the agency to determine whether it needs to initiate any legally required mitigation or notification actions, pursuant to each agency's incident response plan. *See* DET's Standard 170 Incident Response Standard.

- You acknowledge that shared files, groups of files, or folders must have proper security configurations, encryptions, and permissions/access rights to comply with legal and regulatory requirements related to Non-Public Information.

- You should avoid disclosing Non-Public Information over text and other non-encrypted or non-secure messaging platforms. Doing so not only creates public records that must be retained and produced, if requested, but may also create unnecessary security and privacy risks.

Public Records and Records Retention:

A comprehensive description of users' public records and records retention obligations is outside the scope of this policy. However, users should assume that any records and other electronic content on State-managed IT Resources (*and* content on personal devices) that are created or being kept in connection with the official purpose or function of the agency are "records" that: 1) should be evaluated by the agency's legal counsel before disclosure to the public, pursuant to the agency's normal public records request processes; and 2) should be retained for the time periods set forth in the applicable General Records Retention Schedule (GRS) or agency-specific Records Retention/Disposition Authorization (RDA).

Users should follow these general records guidelines, in addition to any agency-specific policies or guidelines, to assist in ensuring compliance with public records and

records retention responsibilities and obligations while using State-managed IT Resources:

- The definition of "record" includes but is not limited to electronic records (*e.g.,* emails, Teams chats, text messages), content on virtual platforms (both during meetings and outside of meetings), data, social media content, voicemails, and audio/video recordings, generative AI output, etc., that are created or being kept in connection with State business.
    - If you are using State-managed IT Resources to engage on social media, or if you are engaging on social media using a *personal* device or *personal* account in a way that could be attributed to the State of Wisconsin, you must abide by Wisconsin Human Resources Handbook Chapter 480 (Social Media Usage in State Government) and other applicable enterprise or agency social media policies.

- In addition to applicable records retention schedules, other laws and circumstances may require some records to be retained for longer, such as when a public records request has been made for a record, or if the record pertains to a complaint, investigation, or ongoing litigation.
    - Those retention timeframes may extend beyond the user's period of employment or contractual or other connection with the State.
    - Therefore, before deleting any records, users should consult their supervisor, agency legal counsel, or agency records officer.

Questions about these affirmative records responsibilities, duties, and obligations can be directed to the user's supervisor, agency records officer, or agency legal counsel.

Use of Personal Devices and Personal Accounts:

Users should also follow these general guidelines, in addition to any agency-specific guidelines, to assist in ensuring compliance with public records and records retention responsibilities and obligations:

- You acknowledge that all work-related records (including but not limited to data, communications, pictures, audio, video, or other information) housed on personal *devices* and on personal *accounts* are considered records and are subject to disclosure under the Wisconsin Public Records Law. Such records must also be retained, maintained, and safeguarded per relevant records retention schedules.

  - You are encouraged to always use State-managed IT Resources, including State email, Teams, and text messaging on State-issued mobile devices to conduct State business. Doing so will help ensure proper records retention on State-managed IT systems and help protect State-managed IT Resources, information, and data through proper security practices.

- The use of personal *accounts* (*e.g.,* Gmail for emails, personal text messaging *accounts*, and other similar instant messaging-type *accounts* like WhatsApp, etc.) for State business is strongly discouraged. You should not use personal *accounts* to conduct State business, except in very limited circumstances where it is not possible to use State-managed IT Resources.
  - If you use a personal account to conduct State business and create any records using that personal account, you are responsible both for the proper retention of such records, and for making such records available if requested by the public, as well as compliance with any other legal requirements and enterprise or agency policies applicable to the records.
  - With respect to certain types of Non-Public Information (*e.g.,* PII, PHI), the use of personal accounts may also violate other aspects of this policy, other applicable laws or regulations, or enterprise or agency policies. In most instances, users should not use personal accounts to transmit or store Non-Public Information.

- When using personal *devices* or personal *accounts* to conduct State business, you must also ensure that all other security and usage requirements are being met. This includes but is not limited to:
  - Logging into State accounts using State Credentials.
  - Utilizing a secure VPN connection to access State-managed IT Resources when not connected to a State network (*e.g.,* when not connected by state ethernet or Wi-Fi, but when using public or non-secure Wi-Fi).
  - Enabling multi-factor authentication to access Non-Public Information on non-State-issued devices or non-State-managed IT Resources.
  - Not conducting any State business on personal devices or personal accounts using prohibited vendors and technologies, pursuant to DET Standard 290 Removal of Prohibited Foreign Products Standard.
  - Ensuring that any other agency or enterprise policies are followed when using personal devices (*e.g.,* agency Bring Your Own Device policies).

Transcriptions and Recordings:

Information for Agency IT:

Regarding transcriptions and recordings, a comprehensive enterprise-wide policy is neither feasible nor desirable. Each State-managed IT Resource may have its own functionality regarding whether a transcription and/or recording can be made from audio, video, or both (*e.g.,* virtual meetings). Each agency may also have its own needs, policies, and legal requirements regarding permissible uses of transcription and recording functionality. Some transcription and recording functionality may also be enabled by default. Moreover, some State-managed IT Resources may require transcriptions or recordings to be enabled in order to access AI-enabled functionality (*e.g.,* meeting summaries), including AI-enabled functionality that is not yet widely available or not yet in use enterprise-wide. Therefore, agencies are responsible for creating their own policies regarding transcriptions and recordings, and must abide by all relevant DET policies, standards, and procedures if transcription/recording functionality is enabled.

Agency policies must follow all applicable laws, regulations, standards, and procedures to ensure that such recordings or transmissions are not prohibited by law, do not contain Non-Public Information, and do not use Non-Public Information to train a large language model (LLM) contained within AI-enabled technology.

Information for Users:

When deciding whether to transcribe or record a meeting or conversation, users should follow these general guidelines, in addition to any agency-specific guidelines, to assist in ensuring compliance with any applicable laws, regulations, policies, and other requirements related to transcriptions and recordings:

- Unless there is an agency policy expressly permitting such recordings or transcriptions, *and* a business need to record/transcribe, you are strongly discouraged from recording or transcribing any conversations or meetings that occur in audio or video messaging applications, including but not limited to Teams and audio recorders on electronic devices.
    - Transcriptions often contain errors and may not accurately reflect the communication made by the caller or the meeting participant(s).
    - Video and audio recordings are also expensive to retain.

- Before recording or transcribing a meeting or conversation, you must obtain authorization from your supervisor, and you must also notify all attendees or participants that the meeting or conversation is being recorded or transcribed.

- If you have received authorization to record or transcribe meetings, and if such transcriptions or recordings are permissible by agency policy, you must retain the audio/video recording and/or the transcription securely for the relevant records retention period mandated by law.
    - Transcriptions and recordings are distinct records, and both must be retained under relevant records retention periods.
    - Other records created from a transcription and/or recording (*e.g.,* meeting minutes, interview summaries) are also records, and distinct from the transcription/recording. Both should be retained under relevant records retention periods.
    - Transcriptions and recordings are subject to disclosure under the public records law and may be released to the public, if requested.

Users should direct any questions about transcriptions and recordings to their supervisor, agency IT Director, or agency legal counsel.

Closed Captioning:

This transcription/recording policy does not apply to live closed captioning, which may be enabled by anyone during a meeting or call and does not create a record. If a user needs to record or transcribe a meeting as a reasonable accommodation for a disability-related need, please contact your agency's medical coordinator to obtain that accommodation.

IT Security:

The security and safety of State-managed IT Resources is of the utmost importance. In addition to any agency security standards, all users must comply with the following security standards, processes, and practices:

- You should keep all usernames, passwords, multi-factor authentication codes, and other information used to access State-managed IT Resources confidential and never share with others.

  - State of Wisconsin agency IT help desk and Enterprise Service Desk staff will never ask for a user's passwords or codes.
  - If you believe your passwords or codes have been compromised, you should immediately contact your agency IT help desk or the Enterprise Service Desk.

- You shall not use any software, tools, or services that permits another user to remotely access or control another system on any State-managed IT Resource without authorization from your supervisor.
  - This prohibition does not apply to authorized remote access by DET or agency IT personnel for authorized purposes (*e.g.,* help desk).

- You shall not reroute traffic on, scan, probe, or attack a network without authorization.

- You shall not intercept or attempt to intercept any data or other information without authorization.

- You shall not use unauthorized peer-to-peer (P2P) networking, file sharing, instant messaging, or Internet Relay Chat (IRC) applications or services.

- You shall not install or attach any equipment to State-managed IT Resource without your agency's authorization (*e.g.,* wireless access points, modems, disk drives, external hard drives, networking devices, personal mobile devices or computers, monitors, keyboards, mice, printers, etc.). Any unauthorized equipment may be confiscated.
  - This applies to equipment being used, installed, or attached anywhere (*e.g.,* in the office, at home, at remote work location sites, in the community, etc.).
  - For additional information about equipment being used for remote work, *see* Wisconsin Human Resources Handbook, Chapter 748 Remote Work and any applicable agency remote work policies.

- You shall not intentionally modify, damage, repurpose for personal use, or remove State-managed IT Resources without authorization.

- You shall not modify, disable, test, or circumvent any State-managed IT Resource security controls, safeguards, or access controls without authorization.

- You shall not intentionally cause a security incident resulting in a loss of data confidentiality or integrity, or a disruption or denial of availability.
    - This includes using State-managed IT Resources to obtain, or to attempt to obtain, unauthorized access to another computer, to make unauthorized modifications to data, computer programs or supporting documentation, to improperly disrupt the operation of another computer, or to commit any crime.

- You shall not circumvent user authentication or compromise the security of a host, network, or account.

- You shall not compromise, modify, or cause damage to State-managed IT Resources.

- You shall not disrupt or interfere with the normal operation of any State-managed IT Resource.

- You shall not download, install, configure, or modify software or hardware without authorization.

- You shall not store data, records, or other information in public storage services or removable devices, without authorization.

- You shall not use or share any program, disk image, archive, or any form of executable files without authorization.

Suspected Unauthorized Use/Security Incidents:

Users must stop using a State-managed IT Resource when they become aware that it may have been involved in a suspected or actual security incident, data breach, or unauthorized use or disclosure.

- You must use alternative communication methods to report the suspected incident, pursuant to each agency's incident response plan. *See* DET's Standard 170 Incident Response Standard.

- Wait for further instructions prior to doing anything further with the State-managed IT Resource.

- You must not delete anything related to such suspected security incident, data breach, or unauthorized use/disclosure, as such information may legally be required to be kept and/or may assist in a later investigation.

State Credentials/Security Credentials:

Users must take precautions to not disclose information related to State Credentials or Security Credentials. As noted above, users should keep all usernames, passwords, multi-factor authentication codes, and other information used to access State-managed IT Resources confidential and never share with others.

In addition, to prevent information and security compromises, users must adhere to the following:

- Do not provide your State of Wisconsin issued email address, or the email address of other State of Wisconsin employees or contractors, to others on a public forum or while using artificial intelligence (AI) tools without authorization to do so as a State of Wisconsin representative.
  - If you are using State-managed IT Resources to engage in a public forum (including but not limited to social media), or if you are engaging in a public forum using a *personal* device in a way that could be attributed to the State of Wisconsin (including but not limited to using your State of Wisconsin issued email address), you must abide by Wisconsin Human Resources Handbook Chapter 480 (Social Media Usage in State Government) and other applicable enterprise or agency social media policies.
  - If you are using State-managed IT Resources while using artificial intelligence (AI) tools (including but not limited to generative AI tools), or if you are using AI tools using a *personal* device in a way that could be attributed to the State of Wisconsin, you must abide by the requirements for use of AI as stated elsewhere in this policy, along with any other applicable enterprise or agency AI policies.

- Do not re-use passwords from State-managed IT Resources for use on any non-State-managed IT Resources.

- Do not reveal or allow anyone to know or use your State Credentials.

- Do not access State-managed IT Resources with Administrator Credentials or administrator authority unless authorized. If administrator authority is necessary to run an application or perform a task, only approved agency processes may be used to grant that administrator authority.

Workstation/Device Usage:

Users of State-managed IT Resources are expected to keep State-managed IT Resources safe and take all necessary steps to ensure protection from unauthorized use or unauthorized modification, and to ensure that those State-managed IT Resources are maintained within authorized and secure locations.

These State-managed IT Resources are supplied to assist users in providing State services, and as such, must be used and maintained according to this policy and other relevant state and federal laws, policies, regulations, and guidelines. Users must take the following precautions to protect State-managed IT Resources:

- You must lock or log off State-managed IT Resources when unattended.

- Do not use State-managed IT Resources or access State data outside the boundaries of the United States.
    - Use of State-managed IT Resources and access of State data outside the United States is strictly prohibited, except in very limited circumstances and in accordance with DET's International Travel Procedures.
    - International use of State-managed IT resources causes an unacceptable level of cybersecurity risk that in many cases cannot be mitigated.
    - Any use case exceptions for international use must be submitted through DET's risk exception process and pre-approved by both the agency IT director and the agency head before users use State-managed IT Resources outside of United States.
    - This prohibition also includes all State-provided or State-managed IT Resources housed on personal devices (*e.g.,* applications including but not limited to Teams and Outlook).

- Do not bypass or circumvent VPN, firewall, antivirus, or other security measures.

- Non-State Wi-Fi access is inherently not secure, and you should use appropriate security measures when using any State-managed IT Resources that are not connected to a State system or network (*e.g.,* when not connected by state ethernet or Wi-Fi, when using public or non-secure Wi-Fi). Those security measures include but are not limited to:
    - Logging into State accounts using State-provided Credentials.
    - Utilizing a secure VPN connection to access State-managed IT Resources.

- Only devices authorized by your agency may be attached, plugged into, connected with, docked with, paired to, or otherwise provided access to State-managed IT Resources.
    - This includes external hard drives, USB flash drives, memory cards, Bluetooth devices, RFID devices, NFC devices, docks, monitors, keyboards, and mice.

- Removing any State-managed IT Resource other than a State-provided devices, including but not limited to laptops, headsets, webcams, cellular telephone, mobile hotspot, payment processing equipment, or tablet from a user's workspace, including a home office, is prohibited without proper authorization.

- You are responsible for all State-managed IT Resources that have been assigned access and/or issued to you. Damage, loss, or theft of State-issued or State-managed equipment should be immediately reported to your agency IT help desk or the Enterprise Service Desk.

- Repairs to State-issued or State-managed equipment shall be completed only by authorized agency employees, vendors, or contractors.

Personal Use of State-managed IT Resources:

Users of State-managed IT Resources must protect those resources from unauthorized access and misuse. Access is given to assist you in providing State services and to perform State business. To accomplish this, any State-managed IT Resources must only be used in support of approved and authorized State business activities and must not be put at risk by unauthorized access or activity.

Regarding any personal use of State-managed IT Resources, users must abide by the following provisions:

- Do not use State-managed IT Resources for any political or commercial purpose.
    - "Political purpose" is defined in DPM Bulletin DPM-0580-MRS.
    - "Commercial purpose" is defined as any activity for which an employee receives payment or compensation other than through their employment or other contractual relationship with the State of Wisconsin.

- Consistent with State of Wisconsin work rules, you are at all times prohibited from using State-managed IT Resources for engaging in unauthorized activities, including but not limited to gambling, operating a personal business, soliciting, playing games, or any other conduct that is disruptive, decreases the user's productivity, or increases agency costs.

- You acknowledge that any personal use of State-managed IT Resources should be incidental or minimal, including storage of non-work-related files or data on State-managed IT Resources.
    - If you download or store non-work-related files or data on State-managed IT Resources, you must ensure that doing so does not create a security or data privacy risk.
    - It is also recommended that you label any personal files or data housed on State-managed IT Resources, and/or place personal files or data in clearly marked personal folders, especially on shared network drives.

- If using State-managed IT Resources for incidental personal use, you shall not disrupt or interfere with the normal operation of any State-managed IT Resource, including but not limited to causing unnecessary network congestion or application delays within State-managed IT Resources (*e.g.,* streaming video or audio during work hours).

Network Usage:

- Do not bypass or circumvent any State of Wisconsin cybersecurity measure or disrupt the operation of any computer or information system.

- Do not connect any non-State-managed device to a State-managed network unless authorized.

- Do not attempt to bypass State-managed firewalls, routers, or other security systems.

- Do not attempt to access any State-managed IT Resource that you have not been given access to or have not been authorized.

- Do not share any network information such as IP addresses, Wi-Fi passwords, jack location, or other details with anyone unless explicitly requested by approved agency support personnel.

Artificial Intelligence (AI) Usage:

Information for Agency IT:

The State of Wisconsin may seek to use Artificial Intelligence (AI) platforms to leverage their capabilities in gaining unique insights, problem solving, and enhancing productivity at state agencies. It is important to note that each agency and each State-managed IT Resource may have access to its own AI functionality, and needs, policies, and legal requirements regarding its permissible uses of AI technology. AI technology is evolving and developing rapidly; at this time, it is not possible to anticipate all possible uses of AI technology, or risks of those uses.

Therefore, until such time when enterprise frameworks, policies, standards, and procedures are in place, agencies are responsible for creating their own AI policies regarding evaluation and use of AI technology within their agency. Agency AI policies must be reviewed and approved by DOA. Such policies must be consistent with all relevant DET policies, standards, and procedures where AI functionality is enabled or used within State-managed IT Resources. DOA may require agencies to submit additional information, including information from agency legal counsel, as part of the approval process. Once approved, an agency may implement the AI policy to approve AI functionality for purchase and/or use by employees.

Information for Users:

Safeguarding sensitive or confidential information from unauthorized access, use, or disclosure is of utmost importance. Before using AI technology, particularly open-source or publicly available generative AI technology (*e.g.,* Chat GPT, Gemini, etc.), users should review their agency AI policy for any agency-specific requirements. This will help ensure that AI platforms and any associated data handling processes complies with applicable confidentiality and data protection laws and regulations, contractual or legal

obligations. This will also help ensure that the use of AI platforms aligns with existing agency, DET, and enterprise policies that concern but are not limited to data privacy, confidentiality, security, and intellectual property protection. At minimum, users must follow these general guidelines to assist in ensuring safe use of AI and proper compliance:

- You must only use AI platforms and functions that have been authorized for use at your agency and that you have received authorization to use for a specific use case or business purpose.

- You should familiarize yourself and comply with any applicable agency policies, all terms and conditions of the AI platform itself, and any other laws and regulations, including public records and records retention laws.

- You are prohibited from using State Credentials when engaging with AI technology in a personal capacity or on a personal device, unless you have received prior authorization to do so. However, when using an authorized AI tool on State-managed IT resources, you should use your State Credentials to engage with the AI tool.

- You are strictly prohibited from sharing Non-Public Information with any internal or external generative AI platform that has not been authorized for use at your agency.
    - You should be vigilant in using generative AI tools and should report to your supervisor or IT staff the appearance of, or others' unauthorized use of, Non-Public Information in generative AI input or output.
    - You should take care to avoid including specific project details, proprietary information, internal jargon, or any other information that could potentially compromise confidentiality, privacy, or data security, or infringe upon the State's or others' intellectual property rights.

- As a user of State-managed IT Resources, you are responsible for using any AI tools ethically, transparently, and in a manner that minimizes bias and discrimination.
    - Given the known risk of factual errors and algorithmic bias in AI-generated output, you must exercise critical judgment and verify the completeness and accuracy of all information from any AI platform, especially generative AI.

        - You should report to your supervisor or IT staff any erratic or inaccurate behavior of the authorized AI tool.
    - You are prohibited from using AI tools in a way that would violate State of Wisconsin work rules, laws/regulations, and other policies that are stated elsewhere. This includes a prohibition creating or distributing content that is defamatory, discriminatory, malicious, deceptive, or infringes on the rights of others. Any such misuses of AI tools may result in termination of access or disciplinary action.
    - All uses of generative AI and predictive AI must be guided by "human-in-the-loop" principles to ensure that critical thinking and good judgment is exercised. Therefore, you must not deploy an AI output in your work on behalf of the State without conducting an appropriate level of review of such output. For example:
        - If authorized by your agency to create content using generative AI, (e.g., letter or email or memo), you must not use such content without first reviewing and revising it for accuracy, usefulness, and appropriateness of tone and substance;
        - You must not use a generative AI tool to assist with research without conducting independent checks of the content created for accuracy;
        - You must not instruct nor prompt generative AI tools or models to create content in the style of others, and you should clearly attribute any output solely created by AI for State business through a footnote or other means visible to the reader; and
        - Unless using an AI tool expressly authorized by your agency for an expressly authorized purpose, you must not solely use predictive AI for decision-making without also reviewing those predictions, decisions, or outputs, and exercising critical judgment about those predictions, decisions, or outputs.
    - Permissible uses of generative AI may include such uses as brainstorming or generating ideas. If a use case is not included in your agency's AI policy, or if you are unsure whether a use is permissible, you should ask your supervisor before proceeding.

Internet Usage:

The internet enables users to access and leverage non-State-managed IT Resources, systems, and services, including cloud services. Users of these services must

be cautious and ensure that State security policies are not violated. You must also take the following precautions to protect State interests:

- State agencies have blocked many internet sites that are not appropriate for work purposes.
    - However, you should not assume that a website is appropriate simply because it is not blocked. Certain un-blocked internet sites may also be inappropriate for work purposes or prohibited by other policies.
    - You must abide by all other policies, work rules, and laws related to appropriate internet use.

- Do not use internet services for purposes other than those needed in support of your work duties, with limited, incidental personal use exceptions as outlined by this policy or related agency or enterprise policies.

- Do not share, exchange, transfer, reveal, or otherwise distribute data contained on State-managed IT Resources with any internet site without proper authorization.

- Do not import or download data or information from any internet sources directly into State-managed IT Resources without proper authorization.

- Do not copy, repost, or share information from internet sources unless the source is known, reliable, trustworthy, legal, accurate, public (*i.e.,* not Non-Public Information, sensitive, restricted, or otherwise protected), and properly credited or attributed to the original source.
    - You must also abide by all relevant intellectual property laws when copying, reposting, or sharing information.

Remote Work:

Users of State-managed IT Resources and technology may be allowed or required to work remotely (outside of a State-managed facility). Remote work has many advantages but also creates a unique set of risks and obligations that must be managed to ensure that State-managed systems and data are protected.

Users must abide by all the provisions of this Acceptable Use Policy described herein, as well as applicable human resources policies about remote work, *see*

Wisconsin Human Resources Handbook, Chapter 748 Remote Work and any applicable agency policies.

In addition, users must also take all the following precautions to protect State-managed IT Resources while engaging in remote work:

- The State will provide a computer for employees working from home and may provide other State-managed IT Resources and equipment at its discretion, but you must provision, configure, support, patch, and maintain any personal equipment and services that are needed to enable your remote work.
    - The State will only provide technical support for State-managed IT Resources and will not provide technical support for personal IT equipment and services.
- You must take appropriate steps to secure all State-managed IT Resources and work to prevent unauthorized access or unauthorized use:
    - You shall secure physical documents, lock screens when not in use, and use encryption or password protection for digital files and communications, as required by enterprise or agency policies.
    - You shall not share State-managed IT Resources with unauthorized individuals.
    - You shall not share or disclose Non-Public Information with unauthorized individuals.

Policy Violations:

Users must follow all relevant agency IT policies and procedures, in addition to this enterprise policy. All users must also understand and accept that violating any of these policies exposes the State of Wisconsin to unnecessary risk.

Accordingly, all users must acknowledge that violating any of these policies can constitute work rule violations. The potential consequences for violations include:

- Disciplinary actions, which can include warnings, suspension, or termination of employment, depending upon the severity and frequency of the behavior or violation of work rule.
- Criminal prosecution, if the behavior constitutes a criminal offense.
- Civil liability for behaviors outside the scope of employment.
- Restricted access or termination of access to State-managed IT Resources for users who violate this policy or pose a risk to the security, privacy, and integrity of State systems, networks, or data.

STATE OF WISCONSIN SECURITY RIDER

The terms and conditions of the State of Wisconsin Security Rider (hereinafter "Rider") shall apply to all Products or Services provided under the Participating Addendum, 505ENT-O26-NASPOITRSRC-02, unless otherwise agreed to by the parties. This Rider shall apply to all environments (e.g., cloud-SaaS, IaaS, PaaS, AI, on-premises, and hybrid); all computing elements performed, provided, occupied, or utilized; and any access to State resources related to the delivery of Products or Services under the Master Contract.

In the event of a conflict between the terms of this Rider, the Master Contract or any other Service Level Agreements (SLA) or agreements between the State and Contractor, this Rider shall control.

1 Definitions

1.1 **"Agency" or "State Agency"** means an office, department, agency, institution of higher education, association, society, or other body in State of Wisconsin government created or authorized to be created by the State Constitution or any law, which is entitled to expend moneys appropriated by law, including the legislature and the courts, but not including an authority, as defined in Wis. Stat. § 16.70(2).

1.2 **"Artificial Intelligence" or "AI"** means a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. (Source: NIST SP800-218A). Artificial Intelligence (AI) applies advanced analysis and logic-based techniques, including machine learning (ML), to interpret events, support and automate decisions, and take actions. (Source: Gartner Glossary)

1.3 **"Authorization"** means the official decision by management, typically an Authorizing Official (AO), to permit an information system to operate after implementing appropriate security controls and accepting the associated risk to organizational operations and assets.

a) **"Authorization to Operate" or "ATO"** means a formal management decision by a State Agency to authorize an information system to operate and to explicitly accept the risk to Agency operations, assets, individuals, and the State that results from its use

b) **"Authorization to Use" or "ATU"** means a formal management decision by a State Agency to approve the use of an information system that has an existing Authorization. An ATU acknowledges that the Agency has reviewed the associated security authorization package or attestation, accepted the system's risk posture, and authorized its use to support the Agency's mission and business purposes.

1.4 **"Authorized User"** means any appropriately provisioned individual with a requirement to access an information system.

1.5 **"Baseline" or "Security Control Baselines"** means the minimum set of security and privacy controls, as defined by the National Institute of Standards and Technology (NIST) in NIST Special Publication 800-53, Revision 5 and NIST Special Publication 800-53B, that are required for information systems categorized as Moderate Impact under Federal Information Processing Standard (FIPS) 199. These controls provide protection where the loss of confidentiality, integrity, or availability could reasonably be expected to have a serious adverse effect on operations, assets, individuals, or the State.

For cloud-based systems, the baseline includes the FedRAMP Moderate Security Control Baseline, which incorporates the NIST Moderate controls plus additional FedRAMP-defined control enhancements, parameters, and continuous monitoring requirements necessary to safeguard Controlled Unclassified Information (CUI) and other federal or State Data hosted in cloud environments.

1.6 **"Breach"** means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: a person other than an Authorized User accesses or potentially accesses Personally Identifiable Information; or an Authorized User accesses Personally Identifiable Information for an unauthorized purpose. The determination of whether a Breach has occurred is within the sole discretion of the State.

1.7 **"Confidential Data"** means any type of data that presents a high or moderate degree of risk if released, disclosed, modified, or deleted without authorization from the State. There is a high degree of risk when unauthorized release or disclosure is contrary to a legally mandated confidentiality requirement. There is a moderate risk when an Agency has discretion under the law to release data, particularly when the release must be made only according to Agency policy or procedure. Confidential Data includes, but is not limited to:

a) Personally Identifiable Information; and

b) Individually Identifiable Health Information; and

c) Federal Tax Information (FTI) under IRS Publication 1075 and bank or other financial account numbers; and

d) Criminal Justice Information under the Federal Bureau of Investigation's Criminal Justice Information Services Security Policy and the Law Enforcement Automated Data System (LEADS) Policy, substance use disorder records under 42 C.F.R. Part 2, and crime victim information; and

e) Certain information not associated with individuals such as State building specifications, security and infrastructure records, and trade secrets; and

f) Information covered by the Children's Online Privacy Act and Federal Educational Rights and Privacy Act, and other information concerning minors, such as child critical incident records and other juvenile records.

1.8 **"Continuous Monitoring" or "CM"** means maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

1.9 **"Contractor"** means the person or entity who is required to provide Products or Services to the State pursuant to the Master Contract.

1.10 **"Encrypt" or "Encryption"** means encryption that complies with NIST's Federal Information Processing Standard 140-3 as demonstrated by a valid FIPS certificate number (or 140-2 until retirement per NIST transition guidance) and configured to use approved modes and algorithms, unless otherwise approved by the State CISO or designee in writing.

1.11 **"Individually Identifiable Health Information"** means information covered by the Health Insurance Portability and Accountability Act (HIPAA), including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual. Individually Identifiable Health Information also includes patient health care records and other protected health information as defined by Wis. Stat. §§ 146.81 and 146.816.

1.12 **"Infrastructure as a Service (IaaS)"** means the capability provided to the State to provision processing, storage, networks, and other fundamental computing resources where the State can deploy and run arbitrary software, which can include operating systems and applications. In IaaS environments, the State does not manage or control the underlying cloud infrastructure, but the State has control over operating systems, storage, and deployed applications. The State may also have limited control of select networking components (e.g., host firewalls).

1.13 **"Large Language Model (LLM)"** means a class of language models that use deep-learning algorithms and are trained on extremely large textual datasets that can be multiple terabytes in size. LLMs can be classed into two types: generative or discriminatory. Generative LLMs are models that output text, such as the answer to a question or even writing an essay on a specific topic. They are typically unsupervised or semi-supervised learning models that predict what the response is for a given task. Discriminatory LLMs are supervised learning models that usually focus on classifying text, such as determining whether a text was made by a human or AI. (Source: NIST AI 100-3: The Language of Trustworthy AI). A LLM is a specialized type of AI trained on vast amounts of text to understand existing content and generate original content. (Source: Gartner Glossary)

1.14 **"Master Contract"** means the Participating Addendum between the Contractor and the State covering the Products and Services to be performed.

1.15 **"Personal Data" or "Personally Identifiable Information"** means information that can be associated with a particular individual through one or more identifiers or other information or circumstances. Such information can include but is not limited to an individual's last name and the individual's first name or first initial, in combination with and linked to any of the following elements, if the element is not publicly available information and is not encrypted, redacted, or altered in any manner that renders the element unreadable: (a) the individual's Social Security number; (b) the individual's driver's license number or State

identification number; (c) the individual's date of birth; (d) the number of the individual's financial account, including a credit or debit card account number, or any security code, access code, or password that would permit access to the individual's financial account; (e) the individual's DNA profile; or (f) the individual's unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation, and any other information protected by State or federal law.

1.16 **"Platform as a Service (PaaS)"** means the capability provided to the State to deploy onto the State's cloud infrastructure or acquired applications developed by using programming languages and tools supported by the Contractor. In PaaS environments, the State does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

1.17 **"Products"** means any combination of software, hardware, facilities, and/or Services that deliver a value to a customer segment.

1.18 **"Recovery Point Objective" or "RPO"** means the point in time that data can be recovered and/or systems restored when Service is restored after an interruption. The Recovery Point Objective is expressed as a length of time between the interruption and the most proximate backup immediately preceding the interruption.

1.19 **"Recovery Time Objective" or "RTO"** means the period within which information technology services, systems, applications, and functions are to be recovered following an unplanned interruption.

1.20 **"Risk Assessment"** means an assessment that (1) documents and categorizes the systems and types of information the Contractor processes, stores, and transmits; (2) identifies threats and vulnerabilities to the system and determines the potential harm from a Breach and Security Incident; and (3) reviews supply chain risks associated with the Contractor's systems.

1.21 **"Security Incident"** means an occurrence that actually or reasonable degree of certainty, jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. The determination of whether a Security Incident has occurred is within the sole discretion of the State.

1.22 **"Service" or "Services"** means an intangible product, including actions, recommendations, plans, research, customizations, modifications, documentation, and maintenance and support, including all related material necessary to fulfill that which the Contractor is obligated to accomplish or to provide under the Master Contract.

1.23 **"Service Level Agreement" or "SLA"** means a written agreement between the State and the Contractor that is subject to the terms and conditions in this document that unless otherwise agreed to includes but is not limited to (1) the technical service level performance promises (i.e. metrics for performance and intervals for measure), (2) description of service quality, (3) identification of roles and responsibilities, (4) security responsibilities and notice requirements, (5) how disputes are discovered and addressed, and (6) any remedies for performance failures.

1.24 **"Software as a Service" or "SaaS"** means the capability provided to the State to use the Contractor's applications on a cloud infrastructure. The applications are owned, delivered, and managed remotely by the Contractor and accessible by the State through a thin-client interface or a program interface. The Contractor delivers software based on one set of common code and data definitions that is consumed in a one-to-many model by the State at any time on a pay-for-use basis or as a subscription based on use metrics. The State does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage, or individual application capabilities, except for limited user-specific application configuration settings.

1.25 **"State"** means the State of Wisconsin.

1.26 **"State Data"** means all information that State officers, agents, employees, or end users upload, create, or modify pursuant to the Master Contract or this Rider, including Confidential Data, and any items or materials originated or prepared for the State under the Master Contract or this Rider. State Data also includes metadata that contains information from which State Data may be ascertainable.

1.27 **"State IT Security Policies and Standards"** means the policies and standards available at https://det.wi.gov/Pages/policies.aspx.

1.28 "**System Security Plan" or "SSP"** means a formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements. SSP should use FedRAMP or equivalent templates. SSP includes:

- system boundary; and
- system description; and
- roles and responsibilities; and
- Security categorization (FIPS 199 impact levels); and
- Implementation of each of the NIST 800-53r5 moderate baseline controls; and
- Inheritance from external providers (e.g., AWS, Azure, GCP); and
- Data flows (typically a diagram); and
- Interconnections; and
- Rules of behavior.

SSP is accompanied by a

a) "Security Assessment Report" or "SAR" means a document that details the findings of the independent security assessment conducted by a Third-Party Assessment Organization (3PAO) or equivalent.
b) "Plan of Action and Milestones" or "POA&M" means a document that details that tracks known weaknesses, vulnerabilities, or deficiencies found during the SAR, ongoing operations, or as part of continuous monitoring.
c) "Continuous Monitoring Strategy" or "ConMon" means a document that details process of maintaining ongoing awareness of security control effectiveness, vulnerabilities, and threats to support risk management decisions to ensure the system remains in compliance after Authorization.

1.29 **"Subcontractor"** means a third-party entity or individual that enters into an agreement with the Contractor for the purpose of providing Products or Services to the State pursuant to the Master Contract.

1.30 **"Trade Secret"** means information, including a formula, pattern, compilation, program, device, method, technique, or process to which all the following apply:

a) The information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other people who can obtain economic value from its disclosure or use.

b) The information is the subject of efforts to maintain its secrecy that are reasonable under the circumstances.

2 Data Ownership

2.1 The State will own and retain all rights, title, and interest in the State Data related to the Products or Services provided under the Master Contract, provided, however, that Contractor may use, reproduce, display and distribute excerpts and data from the deliverables, either alone or together with other material, in the ordinary course of Contractor's business, so long as such excerpts and data do not identify State by name or contain any of the State's confidential or proprietary information, and provided further that Contractor retains all right, title and interest in and to its processes, benchmarking data and data collection tools, assessment models and pertinent methodologies such as Strategic Planning, Contractor's copyrighted proprietary research and other pre-existing materials and data, such as Data Collection Templates and Survey Tools for Applications and Infrastructure, and benchmark comparisons ("Preexisting Intellectual Property")..

2.2 The Contractor shall not collect, access, or use State Data, State user accounts, AI input or output containing or created by State Data, or State search history information, except as necessary to fulfill the terms of the Master Contract; respond to Service or technical issues; or upon written permission from the State designee and shall remain the property of the State. These provisions also apply to all data or information stored or accessed by the Contractor that is the result of any processing of State Data.

2.3 The Contractor shall not acquire rights or licenses including, but not limited to, intellectual property rights or licenses, to State Data unless permitted under the terms of the Master Contract.

2.4 The Contractor shall enable and assist the State in transferring State Data at any time and disclose the necessary tools to complete the transfer. If costs are associated with the transfer, the amount will be negotiated and agreed upon by both parties before State Data is transferred.

3 Disclosing State Data to Third Parties

3.1 The Contractor shall not directly or indirectly disclose, provide, rent, sell, transfer, or otherwise provide access to State Data, State user accounts, AI input or output containing or created by State Data, or State search history information, except upon written permission from the State designee, by an order of a court of competent jurisdiction, or as provided within this Rider. If the Contractor engages in such prohibited actions, the State may invoke its cancellation rights under the Master Contract or SLA, and the procedures provided in Section 8 of this Rider.

3.2 The Contractor shall contact the State designee upon receipt of any electronic discovery, litigation holds, discovery searches, or expert testimonies related to State Data, or which in any way might reasonably

require access to or disclosure of State Data. The Contractor shall not respond to subpoenas, service of process, or any other legal requests related to the State without first notifying and obtaining approval from the State designee, unless the Contractor is prohibited by law from providing such notice.

3.3 Upon the Contractor's receipt of any other request for State Data, the Contractor shall promptly notify the State designee and direct the request to the State. The Contractor shall cooperate with the State to provide the information requested to third parties.

3.4 Except as provided within this Rider, the Contractor shall not use, copy, or disclose State Data, State user accounts, AI input or output containing or created by State Data, or State search history information, or any other information the Contractor may collect from providing Products or Services under the Master Contract, in any transaction that does not include the State, except as strictly necessary to fulfill the obligations of the Master Contract or as expressly permitted by the State designee in writing.

3.5 **No later than 30 days** of signing this Rider, the Contractor shall provide a list of all AI products, Services, or companies, third party or otherwise, that the Contractor will use or reasonably anticipates using to provide the Products or Services under the Master Contract. Annually, until the Master Contract ends or is cancelled, the Contractor shall provide an updated list in writing to the State designee. The State may prohibit the use or involvement of any AI product, Service, or company providing the Products or Services under the Master Contract to the State.

3.6 Except as provided in Section 3.5, these obligations shall survive and extend beyond the term of this Rider.

4 Data Protection

4.1 The Contractor shall not process, store, transmit, or otherwise use State data, nor provide Services for State business purposes, on any information system until such system has been formally authorized and secured in accordance with State requirements. Authorization shall be granted only after the following conditions are met:

a) Authorization to Operate (ATO): A formal decision by the State Authorizing Official to authorize the system to operate and to explicitly accept the risk associated with its use; or

b) Authorization to Use (ATU): A formal decision by the State Authorizing Official to approve the State's use of a system that already holds a valid Authorization (e.g., FedRAMP authorization, or another recognized authorization framework), based on review of the associated Authorization package and acceptance of the system's risk posture; and authorized its use to support the Agency's mission and business purposes.

4.2 The Contractor shall provide the State with evidence in the form of external audit certifications of all required security documentation:

- Certificates of external audits where applicable e.g., ISO 27001 certificate
- Answers to an industry-standard SIG questionnaire
- Tables of contents for all relevant data security policies or standards

The Contractor shall not permit State Data to reside in, or be processed by, any system until the State has formally reviewed and accepted the system's Authorization package and security baseline compliance.

4.3 The Contractor shall implement and maintain appropriate physical, administrative, technical, and organizational security measures to safeguard against Security Incidents and Breaches. Where not defined in this Rider, such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Contractor applies to its own data of a similar kind and shall be periodically reviewed and updated, as needed.

4.4 The Contractor shall implement and maintain security and privacy controls meeting NIST SP 800-53 Rev.5 Moderate baseline or equivalent industry standards, with evidence in an SSP, SAR, POA&M, and Continuous Monitoring Strategy. The Contractor shall perform authenticated vulnerability scanning of networks, hosts, containers, and applications at regular intervals (and after material changes), track findings in the POA&M, and meet the remediation timelines.

For cloud-based systems, the baseline includes the FedRAMP Moderate Security Control Baseline, which incorporates the NIST Moderate controls plus additional FedRAMP-defined control enhancements

4.4.1 The Contractor shall maintain a cybersecurity governance program aligned to NIST Cybersecurity Framework v2.0 or equivalent industry standard, including the GOVERN function. The program will define risk appetite, roles, and decision rights; maintain a risk register; track POA&M.

4.4.2 The Contractor will (a) track and remediate CISA KEV items within mandated timelines; (b) perform automated asset discovery and vulnerability enumeration at regular intervals for all in-scope assets; (c) enforce controls to eliminate or harden internet exposed management interfaces.

4.4.3 If agreed to by both Parties, for any cloud service components, The Contractor will provide FedRAMP equivalent artifacts using FedRAMP templates (SSP, SAR, POA&M) and submit **monthly** continuous monitoring packages (including authenticated vulnerability scans, inventory, and POA&M updates) to the State designee in writing.

4.5 Upon identification of a potential issue with using or maintaining State-provided infrastructure, the Contractor shall identify and communicate the nature of the issue to the State designee in writing without delay, and, if feasible, outline potential remedies for the State's consideration.

4.6 The Contractor acknowledges that it may create, receive from or on behalf of the State, or have access to, information and records that are subject to data protection laws or otherwise exempt from public disclosure under State or federal laws or regulations.

4.7 The Contractor shall not use or disclose State Data except as permitted to provide the Products and Services under the Master Contract and pursuant to this Rider, as required by law, or as otherwise authorized by the State designee in writing.

4.8 The Contractor shall implement commercially reasonable non-disclosure agreements and shall limit knowledge of State Data to those personnel necessary to provide the Products or Services under the Master Contract.

4.9 The Contractor shall encrypt all Confidential Data at rest and in transit with controlled access and is FIPS validated (140-2 or -3)or equivalent industry standards. Any stipulation of encryption responsibilities will identify the specific roles and responsibilities of the State and the Contractor.

4.10 The Contractor shall utilize data redundancy techniques to prevent data loss. The Contractor shall perform offsite replication or backups in a secure, environmentally controlled facility.

4.11 The Contractor shall not allow Confidential Data on mobile devices, portable computing devices, or portable storage components, except as strictly necessary to provide the Products or Services under the Master Contract or SLA, or as expressly permitted by the State designee in writing.

4.12 Where the State allows the Contractor to access Confidential Data on mobile devices, portable computing devices, or portable storage components, the Contractor shall implement security measures that address physical security and appropriate encryption, as well as a restriction on viewing Confidential Data in public or common areas.

4.13 The Contractor must maintain an accurate inventory of all devices that are allowed to access State Data and the individuals to whom they are assigned or who have access to such devices.

4.14 The Contractor must maintain and keep up-to-date antivirus and firewall software, firewall session tracking, and system password protection on any systems or devices (including mobile devices, portable computing devices, and portable storage components) that access State Data.

4.15 The Contractor must maintain and update system software patches on the systems and devices (including mobile devices, portable computing devices, and portable storage components) that access State Data.

4.16 The Contractor must maintain strong password security and multifactor authentication when accessing State Data. This will include ensuring accounts have cryptographically strong passwords and storing passwords in a hashed or encrypted format.

4.17 If applicable, the Contractor shall integrate with the State's identify management process by either (a) extending the State's trust boundary into the Contractor's domain using an identity management system with role-based user authentication and Authorization and synchronizing with the State's active directory using federation or single sign-on technology; or (b) using a password sign-on for application-level security which aligns with industry standards for password strength.

4.18 The Contractor will apply industry standard frameworks (e.g., NIST security frameworks) for Application Program Interfaces (APIs), authentication, and Authorization tasks.

4.19 The Contractor is strictly prohibited from using State Data to train AI or LLMs except if permitted by the State designee in writing and if for the exclusive purpose of providing Products or Services to the State.

4.20 Where the use of AI is allowed by the State, the Contractor shall have safeguards in place to prevent State Data from being exposed to public or external information systems. This restriction extends to Subcontractors.

4.21 **No later than 30 days** after signing this Rider, the Contractor shall provide the documents outlined below to the State designee in writing. Each of these shall be updated and provided to the State designee (1)

annually in writing, (2) when major changes, upgrades, or updates occur to the Products or Services provided under the Master Contract, and (3) following a Security Incident or Breach. The State and Contractor shall work to understand each other's roles and responsibilities with regards to intrusion protection.

- Certificates of external audits where applicable e.g., ISO 27001 certificate
- Answers to an industry-standard SIG questionnaire
- Tables of contents for all relevant data security policies or standards

5 Contractor Access to State Network Systems and Data

5.1 The Contractor shall maintain a robust boundary security capability that incorporates generally recognized system hardening techniques.

5.2 The Contractor shall determine which of their ports are required to support access to systems that hold State Data and shall limit their access to only these ports, disabling all others.

5.3 The Contractor's system network architecture shall separate internal systems from external information systems.

5.4 The Contractor shall use a demilitarized zone for handling public traffic, host-to-host management, Internet protocol specification for source and destination, packet filtering, and activity logging.

5.5 The Contractor shall maintain appropriate access control and Authorization policies, plans, and procedures. The Contractor must use multifactor authentication to access State network systems or Contractor network systems that store, transmit, or otherwise contain State Data.

5.6 The Contractor shall have security policies, plans, and procedures for the handling, storage, backup, access, and, if appropriate, destruction of State Data. These must be commensurate with the moderate security baselines defined in NIST Special Publication (SP) 800-53 or equivalent industry standards, unless provided otherwise in this Rider or agreed to by the State designee in writing.

5.7 The Contractor shall employ appropriate intrusion and attack prevention and detection capabilities. Those capabilities must track unauthorized access and attempts to access State Data, as well as attacks on the Contractor's infrastructure associated with State Data.

5.8 The Contractor shall maintain event profiles to reduce false positives and rapidly detect active access.

5.9 The Contractor shall design and execute reports, **at regular intervals**, to identify anomalies in system logs.

5.10 The Contractor shall ensure logs are written to central log aggregation with 12-month online retention minimum for security logs, and with integrity controls and immutability for all servers.

5.11 The Contractor must use encryption to protect the confidentiality and integrity of transmitted information.

6 Data Centers and Location of Data

6.1 Consistent with Wis. Stat. § 16.705(1r), the Contractor shall provide its Services under the Master Contract solely from within the United States.

6.2 The Contractor shall use data centers located in the United States and shall access data only from the United States. The Contractor shall ensure the transmission and storage of State Data at rest is at data centers located in the United States. The Contractor shall not allow its personnel to provide Services, store, or access State Data on desktops, mobile devices, or portable computing devices from Contractor's data centers while its personnel are located outside of the United States.

6.3 The Contractor shall perform physical security functions including, but not limited to, 24/7 controlled access, identification badge controls, and alarm responses, at any data centers housing State Data that are under the Contractor's control.

7 Security Incidents and Breaches

7.1 The Contractor shall notify the State **no later than 72 hours** of confirming a compromise that impacts confidentiality, integrity, or availability of State Data. Initial notice may include, to the extent reasonably available at the time, the following data elements:

- Identify the current level of impact on Agency functions or Services (Functional Impact).
- Identify the type of information lost, compromised, or corrupted (Information Impact).
- A preliminary assessment summary to be provided when recovered from the incident (Recoverability).
- Identify when the activity was first detected.
- An estimate of potential impact, if known.
- Summary of technical details, when confirmed and appropriate.
- Identify point of contact information for additional follow-up.

Important: Please refrain from adding sensitive personally identifiable information (PII) to incident submissions

7.2 Upon request, The Contractor shall provide updates until containment.

7.3 The Contractor shall notify the State designee of any confirmed or suspected to a reasonable degree of certainty Security Incidents or Breaches within **72 hours**, for the State to take any actions it deems necessary.

7.4 The Contractor must notify the State designee of any of the Contractor's disclosures of the Security Incident or Breach to law enforcement, news media, or any other third parties.

7.5 The Contractor must notify or assist the State designee in notifying regulatory or other governmental organizations and any affected individuals or entities the State deems appropriate or as required by federal or state law including, but not limited to, Wis. Stat § 134.98.

7.6 The Contractor shall preserve sufficient evidence to ensure accurate Security Incident or Breach records, facilitate any investigations internally, and determine the extent of the Security Incident or Breach.

7.7 The Contractor shall cooperate fully with the State and, without delay, by providing a Security Incident or Breach summary report to the State designee. At a minimum, the report will include the following:

- The data elements involved, the extent of the State Data involved, and the identities of any affected individuals or entities.
- The persons or entities known or reasonably believed to have improperly used or disclosed State Data and/or were responsible for the Security Incident or Breach.
- Where the Contractor believes the State Data was improperly transmitted, sent, or utilized.
- The probable causes of the Security Incident or Breach.

7.8 A proposed risk remediation and prevention plan for future Security Incidents or Breaches.

- The corrective actions the Contractor has taken or plans to take, including temporary workarounds and permanent fixes.
- Whether the Contractor believes any federal or State laws requiring notifications to individuals were triggered including, but not limited to, Wis. Stat § 134.98.

7.9 The Contractor must provide periodic follow-up reports to the State designee in writing until the Contractor's investigation of the Security Incident or Breach is complete. In the final follow-up report, the Contractor shall identify the root cause of the Security Incident or Breach.

7.10 The State may conduct an independent investigation of the Security Incident or Breach with which the Contractor shall cooperate by providing written incident summaries and responding to reasonable security questionnaires. An independent investigation may be conducted by a State Agency or a third party acting on behalf of the State. The State may require the Contractor to cover the cost of that investigation.

7.11 In the event of a Breach of Confidential Data the State, the Contractor shall provide a written incident summary (facts, impact to State data/services, root cause when known, remediation) and, upon request no more than annually, an industry-standard SIG questionnaire response, ISO 27001 certificate, and security whitepaper.

7.12 Upon request from the State, the Contractor shall provide one or more of the following corrective action steps to limit the exposure of State Data and respond to the Security Incident or Breach:

a) Credit monitoring.

b) Toll free number for impacted customers.

c) Liability of the Contractor for a certain amount (up to the level of their cyber insurance policy).

d) Participation of all Contractor employees in incident breach drills.

e) All other deliverables the State deems necessary to remediate the Security Incident or Breach.

8 Cancellation and Suspension of Service

8.1 During any period of Service suspension, the Contractor shall not intentionally erase or otherwise dispose of State Data regardless of its format.

8.2 Upon cancellation of the Master Contract, the Contractor shall implement an orderly return of State Data in a mutually agreeable format and at a mutually agreeable time, or the Contractor shall allow the State to extract the State Data itself. Only after the State Data is returned and the State designee confirms receipt of the State Data in writing may the Contractor securely dispose of it.

8.3 The Contractor shall ensure no State Data is deleted in violation of the Wisconsin Public Records Law and the record retention requirements from the Master Contract.

8.4 Upon cancellation of the Master Contract, unless legally prohibited, the Contractor shall securely dispose of all State Data regardless of its format unless stipulated otherwise by the State designee in writing. State Data shall be permanently destroyed and shall not be recoverable, in accordance with NIST 800-88 Revision 1. Certificates of destruction shall be provided to the State designee upon completion.

8.5 The State shall be entitled to any assistance post cancellation of the Master Contract that the Contractor would generally make available with respect to the provided Products and Services.

9 Security Audits

9.1 Upon the agreement of both Parties the State may perform a security audit to review the Contractor's conformance to this Rider. A State Agency may perform this audit, or the State may contract with a third party as its authorized representative, at the State's discretion and expense. The State or its authorized representatives will have access to anything necessary to review the Contractor's compliance with this Rider or pertaining to any facts related to any claim against the Contractor that may be chargeable to the State or its property. The Contractor shall cooperate with the State and its authorized representative in performance of a security audit.

9.2 As part of the security audit, the State or its authorized representative may conduct vulnerability scans and full penetration testing. Penetration testing may be conducted internally or externally on the hardware, software, or firmware components of a system, and may test both physical and technical controls.

9.3 As part of the security audit, the State or its authorized representative may require that the Contractor provide information regarding the security and access of State Data, but not limited to, latency statistics, user access, user access IP address, user access history, and security logs. The Contractor will also provide the following information and services to the State or its authorized representative, upon its request:

a) A review on the Contractor's hardware and software assets. This may include, but is not limited to, information regarding deviations from the hardware baseline, an inventory of information types by hardware device, a software inventory compared against State purchased licenses, and the software versions and scans of the software against patches distributed and applied.

b) A review of the Contractor's boundary defenses. This may include, but is not limited to, working with the State to support the denial of communications to and from known malicious IP

addresses, ensuring that the system network architecture separates internal systems from external information systems and that multifactor authentication is used when required under this Rider, cooperating with the State's monitoring and management of devices remotely logging into the internal network, and ensuring sufficient configuration of firewall session tracking mechanisms.

c) An audit log review. This may include, but is not limited to, validating the audit log settings for hardware and software, ensuring that all systems and environments have adequate space to store logs, creating and implementing profiles of common events to reduce false positives and rapidly identify active access, configuring operating systems to log access control events, creating periodic reports of anomalies in system logs, and ensuring audit logs are written to write-only devices for all servers or a dedicated server managed at an alternative storage site.

d) A review of application software security. This may include, but is not limited to, performing a configuration review of operating system, application, and database settings; and training for software development personnel in secure code development.

e) A review of system administrator access. This may include, but is not limited to, providing an inventory of all administrative passwords (application, database, and operating system level), configuring accounts to require regular password changes, ensuring user and service level accounts have cryptographically strong passwords and that they are stored in a hashed or encrypted format, and reviewing administrative privileged functions.

f) A review of account management and access privileges. This may include providing an inventory of user IDs and passwords; updating the processes for establishing and revoking system access; disabling unnecessary, unauthorized, or dormant accounts; creating a daily report on locked out accounts and disabled accounts; ensuring users are automatically logged off after three (3) unsuccessful log-in attempts after 120 minutes and after a period of inactivity; monitoring access attempts to deactivated accounts; profiling typical account usage; and properly maintaining security profiles.

9.4 The Contractor will bear the cost and responsibility for resolving any issues that exist in the Products or Services provided to the State pursuant to the Master Contract, except if an issue exists in the resources furnished by the State (e.g., code, systems, computer hardware and software). The State may elect to work with the Contractor under mutually agreeable terms for resolution of any found issues, or the State may elect to address the issues independently of the Contractor.

9.5 Any issues found during the security audit must be resolved to the State's satisfaction. Unless the Contractor receives the State's approval, the Contractor will not proceed with Contract work until the State tests and approves the Contractor's resolution.

9.6 Results of the security audit shall be sent to the Contractor and the State, if performed by a third party, within **seven (7) business days** of completion. The results shall include a complete copy of any certifications, scans, and tests conducted.

10 Data Center Audits

10.1 Upon both Parties agreement to conduct, annually, and upon request by the State in response to a Breach of Confidential Data, the Contractor shall perform and bear the cost of an independent audit of its data centers. FedRAMP ATO and Service Organization Control (SOC) 2 audit report, or an equivalent approved by the State CISO or designee in writing, shall set the minimum requirements of the audit. The Contractor shall provide the unredacted audit report to the State designee in electronic format within **seven (7) business days** of completion. The report shall include a complete copy of any certifications, scans, and tests conducted. The Contractor may only remove its Trade Secret from the un-redacted audit report before providing it to the State.

11 Support Responsibilities and Uptime Guarantee

11.1 The Contractor shall be responsible for the acquisition and operation of all hardware, software, and network support related to the Products or Services provided under the Master Contract. The Contractor shall also be responsible for the technical and professional activities required for establishing, managing, and maintaining the environments. All systems shall be available and accessible to customers and the State, except when agreed to by the State designee and Contractor in writing for maintenance downtime.

12 Subcontractor Disclosure

12.1 The Contractor shall maintain and provide to the State, a current roster of all Subcontractors and personnel with access to State systems, data, or facilities and involved in providing Products or Services pursuant to the Master Contract or the Rider. The roster shall include the Subcontractor's name, personnel's name, role, access level, and Authorization status. The Contractor shall provide the roster before the start of work and as a **monthly** update. The Contractor shall also ensure that only rostered Subcontractors and personnel are granted access.

12.2 The Subcontractors providing Products of Services to the State pursuant to the Master Contract shall be subject to the terms of this Rider. The State shall assess and manage granting access to these Subcontractors. These Subcontractors shall not be permitted to access State Data unless needed to provide Products or Services under the Master Contract.

12.3 The Contractor shall be responsible for the actions of the Subcontractors when related to providing Products or Services pursuant to the Master Contract.

13 Annual Review

13.1 The Contractor must meet with the State designee at least annually to review the requirements of this Rider and any of the Contractor's related documents, plans, policies and/or updates. These reviews will include, but are not limited to:

a) Reviewing the Contractor's list of AI Services, Products, and companies annually provided to the State per Section 3.5 of this Rider.

b) Certificates of external audits where applicable e.g., ISO 27001 certificate

c) Answers to an industry-standard SIG questionnaire

d) Tables of contents for all relevant data security policies or standards

e) Ensuring the Contractor remains in compliance with the State's Acceptable Technology Use, Access and Security Policy or Contractor's ISO 27001 certified policy for personnel with access to the State's IT resources.

13.2 The Contractor must perform an annual disaster recovery test and correct any issues detected during the test within the time per Contractor policies. Upon the State's request, the Contractor shall provide the test's result confirmation, test type, scope, date of test.

14 Notification process

14.1 All notifications or other communications required under this Rider shall be provided to the contact listed below:

State designee:

To be determined by Agency at time of purchase order.

Contractor designee:

Will McGuire, Contract Manager
will.mcguire@gartner.com
571-683-4482