Terms and Conditions for Material Purchases

TABLE OF CONTENTS

TERMS AND CONDITIONS FOR MATERIAL PURCHASES

1. DEFINITIONS

The following terms shall have the following meanings:

A. "Affiliate" means, with respect to any Person, each Person that directly or indirectly, controls or is controlled by or is under common control with such Person. For the purposes of this definition, "control" (including, with correlative meanings, the terms "controlled by" and "under common control with"), as used with respect to any Person, shall mean the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of such Person, whether through the ownership of voting securities, by contract or otherwise.

B. "Agreement" means these Terms and Conditions, the document(s) issued by Company called the "Purchase Order" and/or "Contract," the "Contract Documents" listed in either the Purchase Order and/or Contract, and all other documents that the Purchase Order and/or Contract specifically incorporate by reference into the Agreement.

C. "Change Order" means the document issued by the authorized Company Representative that modifies the Agreement.

D. "Company" means the DTE Energy Company entity stated on the first page of the Purchase Order and/or Contract.

E. "Company Representative" means the Company representative(s) identified in the Purchase Order and/or Contract.

F. "Laws" means all applicable federal, state and local laws, ordinances, industry standards, codes, regulations and executive.

G. "Materials" means the materials, goods, equipment, stock, other tangible items or non-stock, and/or services covered by the Agreement, and includes all parts, portions, items, attachments, repairs, replacements and substitutions thereof.

H. "Seller" means the person or legal entity with whom Company has entered into the Agreement.

I. "Third Party Work" means any original works of authorship or inventions or designs created or owned by a third party and used in performing any Work under the Agreement, as identified in writing in sufficient detail in the Agreement so as to distinguish such Work from Work Product developed or created under the Agreement.

J. "Warranty Period" means the applicable warranty length specified in the Purchase Order or, if the Purchase Order does not specify a warranty length, the first to occur of 1) 18 months after the Materials are first used for the purposes intended by Company, or 2) four years after the date Company accepts the Materials.

K. "Work Documents" means all manuals, designs, specifications, technical descriptions, drawings, plans, reports, calculations, summaries and other items to be delivered by Seller to Company under the Agreement.

L. "Work Product" means all materials, notes, reports, documentation, computer programs in object code and fully-commented source code, literary works, graphical works, performances or displays and any derivatives, inventions, formulae, processes, machines, manufacturers, composition of matter devices or any portions thereof and Work Documents, and any improvements on any of them, prepared or developed by Seller for Company in the performance of the Agreement.

2. SCOPE OF SALE AND PURCHASE

Seller agrees to sell to Company the Materials identified in the Agreement at the stated price, quantity, ship to location and other specifications. Company is not obligated to purchase any minimum quantity or dollar amount of Materials from Seller.

3. INGREDIENTS AND HAZARDOUS MATERIALS

A. Prior to delivery, Seller shall promptly furnish to Company a Material Safety Data Sheet ("MSDS") for any chemicals or hazardous materials or products to be delivered to Company, which includes at a minimum: (1) a list of all ingredients in the products and materials to be brought by Seller or its subcontractor or supplier to Company's property, (2) the quantity of all such ingredients and (3) information concerning any changes in or additions to such ingredients. Company shall require the immediate removal of any substance from its property if Seller fails to provide an MSDS. Any damage or delays caused by the removal of such substance shall be at Seller's expense.

B. Prior to and during the shipment of any Materials, Seller shall furnish Company and any carriers with sufficient written warnings and notices (including appropriate labels on the products, materials, containers and packaging) of any hazardous material that is an ingredient or a part of any of the Materials, together with all special handling instructions, safety measures and precautions necessary to comply with all applicable laws, to inform Company and any carriers of any applicable legal requirements and prevent bodily injury or property damage in the handling, transportation, processing, use or disposal of the Materials, containers and packaging.

4. DELIVERY OF MATERIALS

A. All Materials shall be properly packed and secured during shipment and delivered according to the time period stated in the Purchase Order and/or Contract and in accordance with the Supply Chain Management Packaging Requirements Standard, SCM-MM-001, the terms of which are hereby incorporated by reference. To the extent anything in the Supply Chain Management Packaging Requirements Standard, SCM-MM-001, conflicts with these Terms and Conditions, the Purchase Order, Contract, or Change Order, the applicable term in these Terms and Conditions, the Purchase Order, Contract, or Change Order will control. Time is of the essence for this Agreement and Seller shall at all times achieve one hundred percent (100%) on-time delivery. Company may from time to time change such quantities and delivery times, or direct temporary suspension of the scheduled deliveries.

B. In the event Seller delivers the Materials prior to their scheduled delivery date, Company may, at its option, (i) refuse to accept the Materials and return them at Seller's expense or (ii) accept the Materials but defer payment until the time when payment would have been due had the Materials been shipped according to schedule.

C. If delivery of the Materials is not completed by the time period stated in the Agreement, Company reserves the right, without liability and in addition to other rights and remedies, to (1) terminate the Purchase Order and or Contract with written notice to Seller with respect to the stated quantities of Materials not yet delivered and (2) purchase substitute Materials from third parties and Seller shall be responsible for any increased cost.

5. TITLE AND RISK OF LOSS

A. Except as otherwise stated in the Agreement, title to all Materials subject to the Agreement shall remain with Seller until delivery.

B. Except as otherwise stated in the Agreement, risk of loss shall pass to Company upon delivery of the Materials by Seller.

C. Notwithstanding a contrary Incoterm or other shipping term, Seller shall be responsible for any loss or damage occurring during transit to the extent that such loss or damage is attributable to an act or omission of Seller or Seller's failure to adhere to the express shipping instructions of Company.

6. INSPECTION, REJECTION, ACCEPTANCE AND REVOCATION OF ACCEPTANCE OF GOODS

A. Seller shall provide and maintain a quality assurance system which shall assure that all Materials delivered to Company conform to Company's requirements as specified in the Agreement, whether manufactured or processed by Seller or by Seller's suppliers. Seller shall maintain adequate records of all inspections and tests that shall indicate the nature and number of observations made, the number and type of nonconforming or defective Materials, the quantities approved and rejected, and the corrective action taken.

B. Notwithstanding payment, passage of title of Materials to Company, or prior inspection or testing by Seller, all Materials are subject to final inspection and acceptance or rejection by Company.

C. At all reasonable times during the period of Seller's performance under the Agreement, including the period of manufacture, Company may inspect and/or test the Materials to be furnished under the Agreement at the locations where the Work is being performed, including those of Seller's suppliers and Seller shall provide, without additional charge, reasonable facilities and assistance for safe and convenient inspection and testing. Company may conduct one hundred percent (100%) inspection of the Materials or any lot of the Materials or, at Company's option, Company may select and inspect samples thereof. Neither Seller nor Seller's suppliers shall change the location where the Materials are being manufactured, without the prior written consent of Company Representative.

D. In the event that Company determines that any Materials are nonconforming in any manner prior to acceptance, after giving Seller a reasonable time to cure, Company may, in addition to rejecting the Materials and all other remedies available, either itself or through others, rework, correct or otherwise alter any such Materials for the purpose of making them conforming, and all reasonable costs, charges and expenses associated therewith shall be the responsibility of Seller and may be deducted by Company from any amount due Seller. The parties further agree that Company may return to Seller any nonconforming Materials that are delivered to Company and not rendered conforming through Company's efforts (although Company shall be under no obligation to undertake such efforts) and receive full credit for the price of such Materials together with all reasonable costs, charges and expenses associated therewith. Any acceptance by Company is not a release or waiver of any of its rights under this Agreement.

7. WORK DOCUMENTS

Seller shall deliver all Work Documents to Company upon request, delivery of Materials or termination of this Agreement. All Work Documents or Work Product furnished by Seller in connection with this Agreement are the property of Company and, notwithstanding any markings or notices to contrary included on such Work Documents or Work Product, there shall be no restrictions upon Company's use thereof.

8. ELECTRONIC SUBMISSIONS

A. Seller warrants that 1) it has established and adheres to cyber security standards and processes during all equipment and product development and testing procedures, 2) software and related electronic documentation provided to Company does not contain any computer code that would cause a product vulnerability, unauthorized access, loss of functions, malware intrusion, or any other compromise to confidentiality, integrity, or availability, 3) Seller has implemented failsafe features for all products that protect the product's critical functionality, even when the product's security has been compromised, and 4) Seller and Seller's products comply with

all applicable required cyber-security guidelines and standards. Upon Company's request, Seller shall provide Company or Company's authorized representative with a written copy of its development security standards. Upon Company's request, Seller shall provide a third party assessment confirming Seller's product development complies with the requirements in this Section.

B. Without limiting any other rights Company may have under the Agreement, if such virus or other contaminant is brought into Company's computer environment, by or through Seller, Seller shall reimburse Company for all labor and material costs (whether internal or third party) incurred by Company to identify, contain and correct the effects of such virus.

9. CHANGES

A. Company may make changes to the Agreement, including without limitation, changes to any one or more of the following: (1) the specifications of the Materials, (2) the addition or deletion of Materials; (3) the method of shipment of the Materials and (4) the place or time of inspection, delivery or acceptance of the Materials. If such change causes an increase or decrease in the cost of, or time required for performance of, the Agreement, an equitable adjustment may be made by Change Order. Notwithstanding the foregoing, nothing in this Section shall excuse Seller from proceeding with performance of the Agreement as changed. No price increases, costs, charges or other amounts, extensions of time for delivery or other changes shall be binding on Company unless evidenced by a Change Order. Payments made under this Section shall not exceed the aggregate price specified in the Agreement, less payments otherwise made or to be made. The provisions of this Section shall not apply if Company terminates all or any portion of the Agreement due to the default of Seller.

B. No claim by Seller for adjustment hereunder shall be considered unless made in writing within ten calendar days from the date notice of any such change is received by Seller.

10. PRICE AND PAYMENT

A. Company shall pay Seller the prices indicated in the Agreement for all Materials purchased under this Agreement. Unless otherwise agreed to by a Change Order, Seller shall not increase the price stated in the Agreement. Invoices for Materials delivered shall be submitted on a timely basis, in the manner, frequency and form, and with such supporting documentation, as required by the Agreement (including the Supply Chain Management Packaging Requirements Standard, SCM-MM-001, the terms of which are hereby incorporated by reference). Seller shall promptly pay its subcontractors and/or suppliers upon receipt of each payment, the respective amounts owed to the extent of each such subcontractor and/or supplier's interest therein. Company shall pay approved invoices in accordance with the payment terms specified in the Agreement or shall notify Seller of its reasons for disapproval of such invoices. All payments are subject to adjustment for shortage or rejection.

B. Seller, as directed by Company, shall, at its own expense, obtain a prompt discharge of any lien or liens that may be filed on the Material or against Company's property in connection with the Materials. If any lien is filed, Company may withhold payment for the Materials or amounts due under this Agreement (or any other agreement between Seller and Company) until Seller provides proof that said lien has been removed. Company may, at its option, make payments directly to Subcontractors, Suppliers or other lien claimants with notice of such payment to Seller, and deduct such amounts from any payment to Seller or withhold, without interest, any payments otherwise due by Company to Seller because of any claim arising out of this or any other transaction with Company.

C. Seller shall defend, indemnify and hold harmless Company from any and all claims, demands, causes of action and/or costs, including reasonable attorney fees, attributable to Seller's failure to make any payments to Seller's Subcontractor or Suppliers, or any payment required by this Agreement. Nothing in the Agreement shall imply or infer an obligation of Company to make payment to any party other than Seller.

11. GENERAL REPRESENTATIONS

Seller represents and warrants that:

A. Execution, delivery and performance by Seller of this Agreement have been authorized by all necessary action on behalf of Seller.

B. The execution, delivery and performance by Seller under this Agreement does not conflict or result in the breach of any applicable laws, any judgment or decree of any court, or any agreement to which Seller is a party.

12. SELLER COVENANTS

Seller shall keep itself fully informed of and shall comply with all applicable federal, state and local laws, ordinances, industry standards, codes, regulations and executive orders or decrees (collectively, "Laws"), including but not limited to (1) the applicable Laws set forth on the Schedules to these Terms and Conditions and attachments to this Agreement, (2) environmental and pollution control laws, (3) Laws of bodies or tribunals having any jurisdiction or authority over the Materials, and (4) any rules or regulations of Company relating to health, safety or performance of the Agreement which in any manner affect those engaged or employed on any work, the Materials used in any work, or the performance of the Agreement. If any discrepancy or inconsistency should be discovered between the Agreement and any such Laws, Seller shall immediately report the same in writing to Buyer. Seller shall be responsible for the compliance by its subcontractors and suppliers of all tiers with the above provisions and shall be liable for all fines levied in violation of any Laws. Seller shall immediately notify Company Representative if Seller receives any notifications from governmental agencies alleging non-compliance with Laws.

13. CONFIDENTIALITY

A. Seller acknowledges and agrees that all information Company discloses to Seller or to which Seller may have access during Seller's performance of the Agreement is considered proprietary and confidential by Company, unless designated otherwise. This information is and shall, at all times, remain the property of Company. Seller shall disclose such information to its employees, subcontractors or suppliers only to the extent necessary to provide the Materials or perform other obligations under the Agreement. Seller shall advise such persons of the existence of this Agreement, of the confidential nature of the information and of Seller's obligations regarding same under this Agreement. Seller, its employees, subcontractors and suppliers and their employees shall not, without permission of Company, disclose such proprietary or confidential information to any third party for any reason or purpose whatsoever. In the event of a breach or threatened breach of this Section by Seller or those under its control, Company shall be entitled to an injunction restraining such conduct. Nothing herein shall be construed as prohibiting Company from pursuing any other remedies available to Company for such breach or threatened breach.

B. Seller and its employees shall not be required to protect or hold in confidence any such information which (1) becomes known to the public through no act or omission of Seller or its employees; (2) is ordered to be disclosed by a court or administrative agency; or (3) is thereafter developed independently by Seller. In the event that Seller is requested or required under compulsion of legal process to disclose such information, Seller shall not, unless required by law, disclose the information until Company has first (i) received prompt written notice of such request or requirements to disclose and (ii) had an adequate opportunity to obtain a protective order or other reliable assurance that confidential treatment shall be accorded to the Information. Seller shall not oppose actions by Company to assure such confidential treatment.

C. No publications or advisements concerning the subject matter of the Agreement, Company's name and/or logo, or photographs of Company property and materials or portions thereof shall at any time be made by or on behalf of Seller, its subcontractors, or suppliers, unless prior written authorization therefore is obtained from Company Representative.

14. INTELLECTUAL PROPERTY

A. Seller represents and warrants that it has authority to grant, and hereby grants Company, a permanent, assignable, nonexclusive, royalty free license to use, maintain and modify (except for software) any Third Party Work that is required for the performance of this Agreement.

B. All Work Product shall become the sole and exclusive property of Company, whether delivered to Company or not, and shall be delivered to Company in hard copy in electronic native file format as well as Adobe Portable Format (PDF) upon request or upon expiration, termination or completion of this Agreement.

C. Company and Seller agree that all Work Product is a Work-Made-For-Hire under the copyright, patent and trademark laws (as applicable) of the United States. In addition, if any Work Product is not Work-Made-For-Hire, Seller agrees to assign and does hereby expressly assign to Company for all time, all right, title and interest to all Work Product, including any and all intellectual property rights it may have in any whole or part of the Materials. Seller agrees to obtain any assignments of rights from other parties, including its employees, it requires to comply with this Section.

D. During and after the expiration or termination of this Agreement, Seller shall do whatever is necessary, at Company's cost, to obtain patents or copyrights on any concepts, process, products or writings conceived, developed or produced by Seller for the purpose of performing services. Seller shall execute all documents as may be necessary or requested by Company to implement and carry out the provisions of this Section.

E. Notwithstanding the foregoing, Seller shall retain ownership of all its pre-existing know-how embodied in the Work Product, provided that the Company shall have a transferable license to use such pre-existing know-how to the fullest extent necessary to realize the benefits of the Work Product and/or Materials.

F. Seller represents and warrants that all materials, equipment and processes used or supplied and Work Product are free from infringement of any patent, trademark or other intellectual property right. Seller shall pay all royalties and license fees necessary for the performance of this Agreement or use of the Materials.

G. Seller shall indemnify and defend any action brought against Company based on a claim or allegation that any process or method used, equipment or material supplied pursuant to the Agreement constitutes an infringement or violation of any patent, trademark or other proprietary right. Company shall at Seller's expense give such information and assistance as it may deem appropriate for the defense of same, and Seller shall pay all of Company's actual costs and expenses of such action, including any damages awarded. If an infringement or violation is determined or held to exist and the use of such process, method, equipment, material or service is enjoined, Seller shall at its own expense and at Company's option either (1) procure for Company the right to continue using said process, equipment, material or service; (2) replace it with non-infringing process, equipment, materials or service acceptable to Company; or (3) modify it in a manner acceptable to Company so that it becomes non-infringing.

15. WARRANTY

A. Seller represents and warrants that:

(1) all materials and equipment furnished by it and its subcontractors or suppliers shall be (a) free from defects in design, material and workmanship, (b) fit for the purpose intended, (c) new and conform to the specifications, drawings, samples and other descriptions as set forth in the Agreement and, (d) where not specified, of the highest quality and best grade of its respective kind for its intended use,

(2) it has good and marketable title to all materials at the time the materials are loaded for delivery to Company and that title to all materials and equipment furnished by it shall pass to Company free and clear of all liens, claims, security interests or encumbrances, and

(3) all engineering, drafting or other technical services provided as part of the Materials shall be performed by qualified and competent personnel in accordance with industry practice and the high standards of care, skill, diligence and practice appropriate to the nature of the services rendered and shall conform in all respects to any specifications.

B. Seller acknowledges and agrees that Company will be relying on the accuracy, competence and completeness of the technical services to be performed and will use the results of such services as input data for Company projects (as described in the applicable Purchase Order). If at any time during the Warranty Period it appears that the Materials or any part thereof do not conform to these warranties, Company shall notify Seller within a reasonable time after such discovery and Seller, at its sole expense and after obtaining Company's concurrence, shall promptly correct such defects as follows:

(1) Seller shall provide any redesign, repair, replacement and testing services as necessary to correct any nonconforming materials or workmanship. The warranty for redesigned, repaired or replaced Materials shall be of equal duration and scope as the original warranty and commence upon Company's acceptance of such corrected Materials.

(2) Seller shall defend and hold harmless Company, its successors and assigns from and against any liens, charges, claims or encumbrances in breach of the foregoing warranty; this provision of this clause B2 shall survive termination or expiration of this Agreement.

C. If Seller fails to fulfill its obligations under this Section, Company may revoke acceptance and cover by purchasing substitute Materials or may proceed to make corrections or accomplish Seller's work by the most expeditious means available. Seller shall be liable for the cost of cover or correction performed by Company, including all damages proximately caused by the breach of the foregoing warranties, such as removal and reinstallation costs, inspection costs and all shipping costs.

D. Seller shall promptly provide Company Representative (a) notice of any defects (latent or otherwise) in the Materials; (b) any warnings concerning defects (latent or otherwise) in the Materials; (c) any recall notices or safety bulletins related to the Materials; and (d) details including corrective action requirements. The provisions of this clause D shall survive termination or expiration of this Agreement.

E. In addition to, and without limiting, Seller's warranty, Seller shall obtain and extend to Company any manufacturer's warranty for products or processes utilized during, or incorporated into, the Material and procured by Seller.

16. TERMINATION FOR CONVENIENCE

Company may at any time, upon ten calendar days-notice without cause, terminate this Agreement in whole or in part. Upon such termination, Seller agrees to waive all claims for damages, including without limitation claims for loss of profits, and to accept as its sole remedy for termination the cost of all Materials delivered prior to the date of termination, including reasonable overhead and profit thereon and reasonable cost incurred by Seller in terminating the Agreement. Company shall have no liability whatsoever for goods which are Seller's standard stock. Termination shall not relieve Seller of any of its obligations for Materials delivered hereunder.

17. TERMINATION FOR CAUSE

A. Seller shall be in default hereunder if (1) Seller refuses, neglects or fails in any respect to prosecute the Agreement hereunder or any portion thereof with promptness, diligence or in accordance with any of the provisions set forth herein, (2) Seller refuses, neglects, or fails to perform any other obligations under this Agreement or provide adequate assurance of performance, (3) Seller makes an assignment for the benefit of creditors or bankruptcy or insolvency proceedings are instituted by or against Seller, or (iv) at any time in Company's sole judgment, Seller's financial or other condition or progress on the Agreement shall be such as to endanger timely performance.

B. Upon any default hereunder, in addition to all other remedies hereunder, under applicable law or in equity, Company may (1) terminate all or any portion of the Agreement without liability, except the obligation to pay the purchase price for conforming Materials received by Company prior to termination that were accepted in accordance with the Agreement and not previously paid for, (2) require Seller to repair or replace any or all Materials, at Company's option and at Seller's sole expense at the location designated by Company, (3) require Seller to pay all transportation and other charges arising from delivery, storage and return of Materials, (4) purchase replacement Materials from a third party and charge the same to Seller, (5) recover from Seller any and all increased costs and other damages relating to such default and/or (6) recover attorneys' fees and costs of suit, plus interest.

C. No delay by Company in the enforcement of any provision of the Agreement shall constitute a waiver thereof, and no waiver thereof shall constitute a waiver of any other provision.

D. Upon termination, Seller shall deliver all Materials in progress under the Agreement and provide Company with all intellectual rights in any Work Product.

18. INDEMNIFICATION

A. Seller covenants and agrees that it shall defend, indemnify and hold Company and all of its officers, agents and employees (each, a "Company Indemnitee") harmless for any claim, loss, damage, cost, charge, expense, lien, settlement or judgment, including interest thereon, whether to any person, including employees of Seller, its subcontractors and suppliers, or property or both, arising directly or indirectly out of or in connection with Seller's or any of its subcontractor's or supplier's performance of the Agreement or in connection with the provision of Materials, to which any Company Indemnitee may be subject or put by reason of any act, action, neglect or omission on the part of Seller, any of its subcontractors or suppliers or any Company Indemnitee. Without limiting the foregoing, said obligation includes claims involving Seller's, supplier's or subcontractor's employees injured while going to and from the Project. If the Agreement is one subject to the provisions MCL 691.991, then Seller shall not be liable under this Section for damage to persons or property directly caused or resulting from the sole negligence of any Company Indemnitee.

B. In the event any suit or other proceedings for any claim, loss, damage, cost, charge or expense covered by Seller's foregoing indemnity should be brought against any Company Indemnitee, then upon Company's request Seller hereby covenants and agrees to assume the defense thereof and defend the same at Seller's own expense and to pay any and all costs, charges, attorney's fees, and other expenses, and any and all judgments that may be incurred by or obtained against any Company Indemnitee in such suits or other proceedings. In the event of any judgment or other lien being placed upon the property of Company in such suits or other proceedings, Seller shall at once cause the same to be dissolved and discharged by giving bond or otherwise.

19. LIQUIDATED DAMAGES

This Section applies only if liquidated damages are specified in the Agreement. If Seller fails to deliver the Materials, or any severable portion thereof, or comply with this Agreement, within the time specified in this Agreement, the damages to Company as a result of such delay shall be substantial. However, the amount of such damages is difficult and impractical to determine and, as such the parties agree that the amount set forth as liquidated damages in the Agreement is a reasonable estimate of Company's damages for such delay. The amount of any liquidated damages may be withheld from any payments due Seller or shall be paid by Seller, or its sureties, if any, to Company. If liquidated damages are withheld during performance and Seller subsequently remedies its delay, such liquidated damages shall be refunded.

20. LIMITATION OF LIABILITY

Except as may be expressly stated elsewhere in this Agreement, neither party shall be liable to the other party for incidental, indirect, or consequential damages, including, but not limited to, loss of profits or revenue.

21. SET OFF

Company shall be entitled at any time to set off any sums owing by Seller or any of Seller's affiliated companies, to Company or any of Company's affiliated companies, against sums payable by Company.

22. RECORDS AND AUDITS

Company or its authorized representative shall have access to Seller's records to review, audit, and verify any information connected with this Agreement for a period of three years after completion of the Agreement. Seller will provide Company or its authorized representatives with access to all personnel, property, books, and records necessary to effectuate such audit. Seller shall keep all records in an electronic format and be able to transmit them to Company in an electronic native-file format as well as Adobe Portable Document Format (PDF). All documents and records shall be provided to Company at no additional cost. Company has the right to use general audit software and other reporting tools to analyze the data.

23. ASSIGNMENT

No assignment of this Agreement or any of its rights or obligations hereunder shall be made by Seller without first obtaining the written consent of Company. This Agreement shall be binding upon and inure to the benefit of the respective successors and permitted assigns of the parties hereto.

24. FORCE MAJEURE

A. Except as otherwise provided herein, Seller shall not be liable for a reasonable delay or default in furnishing Materials hereunder and Company shall not be liable for failure to perform any of its obligations hereunder, to the extent due to fire, flood, storm, other natural disaster, national emergency or war, and not due to labor problems, inability to obtain financing, negligence or other similar condition of such party, provided that either party has given the other prompt notice of such occurrence.

B. Within seven calendar days of the commencement of any excusable delay, Seller must notify Company Representative in writing of the nature, cause, date of commencement and expected impact of the event. Seller must exercise due diligence in proceeding to meet its performance obligations hereunder, notwithstanding the delay. Upon Seller satisfying these conditions, Company may extend the schedule for the period of time equal to the time actually lost by reason of the delay.

25. NON-WAIVER
None of the provisions of the Agreement shall be considered waived by either party unless such waiver is given in writing by the other party. No such waiver shall be a waiver of any past or future default, breach or modification of any of the terms, provisions, conditions or covenants of the Agreement unless expressly set forth in such waiver.

26. NOTICES
Notices and other written communications are to be made in writing to the address stated in the Agreement. Such notices and other written communications must reference the Purchase Order and/or Contract Number appearing in the Agreement.

27. SAVING CLAUSE-INDEPENDENT TERMS
Each term and condition of this Agreement is deemed to have an independent effect and the invalidity of any partial or whole paragraph or section shall not invalidate the remaining paragraphs or sections. The obligation to perform all of the terms and conditions shall remain in effect regardless of the performance of any invalid term by the other party.

28. SURVIVAL
All of the terms of this Agreement which by their nature extend beyond (a) the termination or cancellation of this Agreement or (b) the completion of the delivery of Materials shall survive and remain in full force and effect and apply to respective successors and assigns.

29. NON-EXCLUSIVITY
It is agreed that this Agreement is not exclusive, and that nothing herein shall be deemed to prevent Company from engaging others to provide any of the Materials or to prevent Company from providing any of the Materials through its own employees or agents.

30. CONSTRUCTION OF TERMS
The terms of this Agreement have been arrived at after mutual negotiation and the parties agree that its terms shall not be construed against any party by reason of the fact that this Agreement was prepared by one of the parties. References to laws refer to such laws as they may be amended from time to time. The words “shall” and “will” have equal force and effect. The words “include”, “including” or “includes” shall be read to be followed by the words “without limitation”. The section headings contained in this Agreement are for convenience of reference only and shall not affect the meaning or interpretation hereof. All references to day(s) shall mean calendar day(s), unless otherwise expressly specified.

31. GOVERNING LAW AND JURISDICTION
The Agreement, and the rights, obligations and liabilities of the parties hereto shall be construed in accordance with the law of the State of Michigan, without regard to its conflict of law principals. The parties agree that any action with respect to this Agreement shall be brought in a court of competent subject matter jurisdiction located in the State of Michigan and the parties hereby submit themselves to the exclusive jurisdiction and venue of such court for the purpose of such action.

32. ENTIRE AGREEMENT
A. The Agreement represents the entire agreement between Company and Seller. No modification of the Agreement shall be effective unless made by a Change Order. Any agreements, negotiations or understandings of the parties prior or contemporaneous to the date of the Agreement, whether written or oral, are superseded hereby.

B. Any document submitted by Seller (including any Seller document referenced in the Agreement) is used solely for the purpose of describing the Materials and, to the extent containing any terms in addition to or inconsistent with the terms of the Agreement, or a rejection of any terms of the Agreement, shall be deemed to be a counter offer to Company and shall not be binding upon Company unless specifically accepted in writing by Company Representative. In the absence of written acceptance of such counteroffer by Company, commencement of performance by Seller shall be deemed to be an agreement by Seller to perform in accordance with the terms of the Agreement and an acceptance hereof, notwithstanding any prior dealings or usage of trade.

33. ON-SITE SERVICES
If the Agreement requires Seller to be physically present on any Company site, Seller shall also comply with the provisions set forth in the attached On-Site Services Schedule.

34. NUCLEAR POWER PLANT ADDITIONAL TERMS
If Seller is providing Materials for delivery to or use at a Company nuclear power plant, Seller shall abide by the additional terms and conditions set forth in the attached Nuclear Terms Schedule, which may be modified by Company from time to time to conform to any change in law.

35. FEDERAL CONTRACTING REQUIREMENTS
Seller agrees to comply with the Federal Contracting Requirements and Foreign Corrupt Practices Act as set forth on the attached Federal Requirements Schedule. Seller agrees that Company may modify Federal Requirements Schedule at any time to conform to any change in law, without notice to Seller.

36. BACKGROUND INVESTIGATION REQUIREMENTS
Seller shall comply with the requirements set forth on the attached Background Investigations Requirements Schedule, which may be modified by Company from time to time to conform with any change in law.

37. VENDOR REMOTE ACCESS SECURITY AND/OR NERC CIP 013

If Contractor will either have access to Company's computer or electronic communications network or sell products to Company that impact the availability or reliability of Company's BES Cyber Assets, Company shall abide by the attached Terms and Conditions for Remote Access and NERC CIP 013 Schedule, which may be modified by Company from time to time to conform with any change in Law.

38. DIVERSITY, EQUITY, AND INCLUSION

Company is committed to utilizing a diverse supplier base, which includes businesses that are owned and operated by: Women, Minorities (African Americans, Hispanic Americans, Native Americans, Asian-Pacific Americans, or Subcontinent Asian Americans), Veterans, Service-Disabled Veterans, and members of the LGBT Business Community. Company expects Contractor will have similar values and work toward a goal of sourcing at least 20% spend with diverse businesses. Company requests that, upon invitation by Company's Supply Chain representative, Contractor submit Tier II* diversity subcontracting spend into Company's third-party reporting platform. Contractor must provide an annual subcontracting plan that identifies spend goals with diverse businesses.

*Tier II spend is defined as work subcontracted by a Prime supplier to a diverse supplier. Spend could be "direct" or "indirect". Direct spend is defined as materials or services directly related to the Company deliverable, for example engineering services or a component for equipment. Indirect spend is defined as services utilized by the Prime supplier that are not directly related to the Company deliverable. For example, if Prime supplier utilizes a diverse supplier to perform landscaping services at their headquarters, Company would track percentage of spend contributing to the Prime supplier's revenue (e.g., if Company represents 20% of Prime supplier's revenue and Prime supplier spent $100,000 with diverse supplier, Company would recognize $20,000 as indirect purchasing spend).

When Scorecards are utilized to monitor Contractor's performance, Company will track Contractor's commitment to achieving Tier II spend goals established for scope of work. In addition, Contractor shall report participation in the following (which may include, but not be limited to):

- In-house "Trades-related" training that Contractor provides to local communities
- "Michigan-based" participation with student programs and mentoring
- Community outreach programs

In support of Diversity, Equity and Inclusion, Contractors are encouraged to hire a diverse workforce to gain new perspectives. Diversity includes hiring people across the spectrum of age, race, gender, ethnicity, sexual orientation, cultural backgrounds and more.

ON-SITE SERVICES SCHEDULE

SAFETY AND SECURITY

A. Seller shall take all necessary precautions for the protection of the health and safety of its employees, its subcontractors and suppliers, Company, the public and other third parties and shall at all times comply with Company's health, safety and security rules and procedures applicable to the site (which are subject to change from time-to-time) and appropriate for the Materials. As required by the Agreement, Seller shall comply with the DTE Energy Contractor Safety Requirements and applicable Safety Handbooks.

B. Company may furnish security personnel at the site to control access, patrol yards and buildings, maintain order, and enforce regulations. The presence or absence of such security personnel shall not modify the responsibility of Seller for loss and/or damages to persons or property.

REPORTING OF ACCIDENTS

Seller shall notify Company Representative and shall comply with the following telephone reporting procedure in the event that its employee(s) or its subcontractor's or supplier's employee(s) sustain a serious personal injury (any injury which requires admittance to a hospital) or a fatality occurs arising out of the Agreement.

1. Between the hours of 8:00 a.m. and 5:00 p.m. eastern time, Monday through Friday, the Legal Investigations Division of Company's Legal Department (313-235-7705) shall be notified immediately.

2. Between the hours of 5:00 p.m. and 8:00 a.m. eastern time, Monday through Friday, weekends and holidays, the Company switchboard (313-235-8000) shall be notified. It shall in turn relay the report to the Legal Department representatives on call. In addition to this telephone reporting procedure, Seller shall also submit to the Legal Investigations Division of Company's Legal Department a written follow-up accident report form (available from the Company Representative) within 24 hours after the occurrence, as well as a written accident report in all other cases requiring more than first aid treatment. Seller shall also furnish Company with a copy of all claims submitted to its insurance companies.

INSURANCE

A. Seller shall provide Company with Certificate(s) of Insurance evidencing that insurance coverage of the types, amounts and conditions as specified in Appendix A, "Insurance provided by Contractor" are in effect. Such insurance coverage shall remain in effect at all times that Seller is present on Company property.

B. Seller shall require its subcontractors to carry insurance in the amount, type and form of insurance required by the Agreement. If its subcontractors do not obtain such coverage, Seller shall insure the activities of its subcontractors.

NUCLEAR TERMS SCHEDULE

PROTECTION AND INSPECTION OF MATERIALS

If Seller is providing goods for delivery to or for use at a Company nuclear power plant, Seller shall establish cleanliness control and foreign material exclusion practices that shall ensure that: (i) the Materials when delivered are free from oil or grease (not being used as a preservative or protective coating), machine tailings, dirt, mill scale, weld splatter, residue, broken or loose parts, contaminants, loose fasteners, tags and labels (not permanently affixed to internals) or other foreign material that may adversely affect the operation of the Materials or may be introduced into interfacing equipment and systems; (ii) if the Materials are shipped with other parts (such as seals, gaskets, lubricants, mounting hardware), precautions should be taken to ensure smaller items cannot be introduced into openings or cavities of larger parts and equipment; (iii) where appropriate, every item included with a shipment should be identified in the packing list or by other means; (iv) if necessary, clearly visible protective devices such as caps, plugs or covers (protective devices shall be validated for material compatibility to guarantee no impact to the Materials provided (for example, protective devices containing halogens or heavy metals should not be used on stainless steel items)); and (v) if desiccants or other preservatives are used to protect the Materials, the affected part of equipment shall be clearly labeled or tagged with information including the type of preservative, its location, and any special instructions pertaining to its removal prior to installation or other applicable information such as quantity of desiccant packages.

Prior to shipping any radioactive material to any Company Site, Seller must notify Radiation Protection (734-586-5302) no less than 48 hours in advance and inform them of what is being shipped, curie content, purchase order number and estimated time of arrival. Prior to receiving any material at any Company Site that might have been used at another nuclear facility, Seller must contact Radiation Protection Department to survey the material prior to entering the protected area.

DELIVERY OF SUSPECT/COUNTERFEIT ITEMS

The delivery of suspect/counterfeit Materials is of special concern to Company. If any Materials specified in the Agreement are described using a part or model number, a product description, and/or industry standard referenced in the Agreement, Seller shall assure that the Materials supplied by Seller meet all requirements of the latest version of the applicable manufacturer data sheet, description, and/or industry standard unless otherwise specified. If the Seller is not the manufacturer of the Materials, the Seller shall make reasonable efforts to assure that the Materials supplied under this Agreement are made by the original manufacturer and meet the applicable manufacturer data sheet or industry standard. Should Seller desire to supply an alternate item that may not meet the requirements of this paragraph, Seller shall notify Company of any exceptions and receive Company's written approval prior to shipment of the alternate Materials to Company.

If suspect/counterfeit Materials are furnished under this Agreement or are found in any of the Materials delivered hereunder, Company may dispose of or return such Materials to Seller in accordance with the warranty provisions applicable to the Agreement. The Seller shall promptly replace such suspect/counterfeit Materials with items meeting the requirements of the Order. In the event the Seller knowingly supplied suspect/counterfeit Materials, the Seller shall be liable for reasonable costs incurred by the Company for the removal, replacement and reinstallation of such Materials in accordance with the warranty provisions applicable to the Agreement.

FEDERAL REQUIREMENTS SCHEDULE

. Company, as a federal seller, requires that Seller agree to be bound by and comply with the following clauses which are incorporated by reference herein and have the same force and effect as if set forth in full text.

(1) The following Federal Acquisition Regulation ("FAR") and Code of Federal Regulations ("CFR") clauses, as amended, are incorporated by reference in these terms and conditions unless Seller is exempt thereunder: Equal Opportunity, FAR 52.222-26 (applies to all orders); Prohibition on Segregated Facilities, FAR 52.222-21 (applies to all orders); Anti-Kickback Procedures, FAR 52.203-7 (applies to all orders over $100,000); Restrictions on Subcontractor Sales to the Government, FAR 52.203-6 (applies to all orders); Anti-kickback Procedures FAR 52.203-7 (applies to orders of $150,000 or more); Combat Trafficking in Persons, FAR 52.222-50(applies to orders of $500,000 or more) , Equal Opportunity for Veterans, FAR 52.222-35 (applies to orders of $150,000 or more); Equal Opportunities for Workers with Disabilities, FAR 52.222-36 (applies to orders of $15,000 or more) and Privacy Training, FAR 52-224-3 (applies if Seller's (or subcontractor's) employee(s) will have access to personally identifiable information (PII) or a system of records on individuals. . To the extent not exempt, Seller shall abide by the requirements of 41 CFR 60-300.5(a) (applies to orders of $100,000 or more) and 60-741.5(a) (applies to orders of $10,000 or more). These regulations prohibit discrimination against qualified individuals on the basis of protected veteran status or disability, and require affirmative action by covered prime seller's and subcontractors to employ and advance in employment qualified protected veterans and individuals with disabilities. The terms "Contractor," "Government" and "Contracting Officer" as used in the FAR clauses shall be deemed to refer to "Seller," "Company" and "Company Representative", respectively.

(2) Except to the extent that this Agreement is exempt from any of these requirements, Seller agrees to be bound by and comply with the clauses set forth at 48 CFR 52.2-8 (Utilization of Small Business Concerns) and 48 CFR 52.219-9 (Small Business Subcontracting Plan) (only if this Agreement exceeds $700,000 and if Company requests submission of a Small Business Subcontracting Plan).

B. Seller does hereby represent, warrant and covenant that:

(1) Seller shall not cause Company or its affiliates to be in violation of the Foreign Corrupt Practices Act (15 U.S.C. Section 78dd-1, et. seq.) as amended (the "FCPA") or any other applicable law.

(2) With respect to its performance under the Agreement, Seller and its owners, directors, officers, employees, and agents will not, directly or indirectly through third parties, pay, promise or offer to pay, or authorize the payment of, any money or give any promise or offer to give, or authorize the giving of anything of value to any individual, entity, or government for purposes of corruptly obtaining or retaining business for or with, or directing business to, any person, including, without limitation, Company or its affiliates.

(3) Seller shall ensure that no part of any payment, compensation, reimbursement or fee paid by Company to Seller will be used directly or indirectly as a corrupt payment, gratuity, emolument, bribe, kickback or other improper benefit.

(4) Seller shall provide to Company and/or its representatives and advisors all supporting documents requested by Company pertaining to any expenses incurred, products provided, and/or services performed by Seller and its agents pursuant to the Agreement to ensure compliance with the FCPA. Seller understands and acknowledges that, notwithstanding any other provision contained in the Agreement, none of Company or any of its affiliates shall be obligated to reimburse any expense incurred or pay for any Work, in Company's reasonable opinion, (1) Seller has failed to provide adequate documentation or information to confirm that an expense or charge did not violate the FCPA, or (2) an expense reimbursement or product/service payment would cause Company or any of its affiliates to be in violation of the FCPA.
A

BACKGROUND INVESTIGATIONS REQUIREMENTS

A. Seller must conduct a background check (as set forth herein) on all of its workers assigned to provide services to Company, prior to that respective worker starting work on Company's project.

B. In performing the background checks, Seller agrees to comply with all applicable local, state and federal laws, including the Fair Credit Reporting Act and agrees that such background check will be performed by a National Association of Professional Background Screeners Accredited Company.

C. Background checks will include, but not limited to:

- Social Security Number (SSN) Trace;
- Criminal history check in all federal, state, and county jurisdictions as revealed by address history on social security trace. Criminal search shall also include any name variations and/or aliases located on the social security trace. County records must be searched at the court level to maintain maximum possible accuracy. Automated county searches, commonly referred to as Bots, may not be used unless guaranteed to be equivalent by county court clerk.
- US Patriot Act Watch Lists.
- National Criminal Index Search to include State Sex Offender Registries; Office of Foreign Asset Control (OFAC).
- Verification of Immigration Status, including valid I-9 Form where applicable. Note the Company expressly prohibits any Seller from employing any person on Company premises who does not have valid authorization to work in the United States.
- U.S. law requires companies to employ only individuals who may legally work in the United States – either U.S. citizens, or foreign citizens who have the necessary authorization. Seller must validate eligibility through E-Verify.
- Driving History (where permitted by law and if Seller is required to operate a Company motor vehicle).

D. Unless restricted by applicable law, all convictions for misdemeanors or felonies shall be reviewed by Seller to determine whether the criminal conviction disqualifies the worker from working on Company's project.

E. Examples of convictions that shall be carefully reviewed by Seller for possible disqualification include, but are not limited to: crimes of dishonesty (i.e. theft, embezzlement, fraud, forgery, etc.) and violence (i.e. murder, rape, kidnapping, assault, robbery, stalking, harassment, etc.).

F. In evaluating the results of background checks, Seller shall consider factors such as the nature and severity of the crime, the length of time that has passed since the offense occurred, how the crime relates to the worker's proposed job responsibilities, truthfulness and completeness of the worker's disclosure of convictions, and evidence of rehabilitation and subsequent job history.

G. Seller provides Company an ongoing representation and warranty that it has conducted background checks consistent with the requirements set forth in this Schedule. Further, if Seller breaches this warranty, it agrees that it will make Company whole for any cost, claim, fine, or penalty that Company may incur as a result, directly or indirectly, from a breach of this warranty.

H. Seller covenants and agrees that it shall defend, indemnify and hold Company, its parent, and all of their officers, agents and employees (each a, "Company Indemnitee") harmless for any claim, loss, damage, cost, charge, expense, lien, settlement or judgment, including interest thereon, including employees of Seller, its subcontractors and suppliers, or property or both, arising directly or indirectly out of or in connection with Seller's or any of its subcontractor's or supplier's breach of the warranty and representation set forth in this Schedule. In the event any suit or other proceedings for any claim, loss, damage, cost, charge or expense covered by Seller's foregoing indemnity shall be brought against any Company Indemnitee, Seller hereby covenants and agrees to assume the defense thereof and defend the same at Seller's own expense and to pay any and all costs, charges, attorney's fees, and other expenses, and any and all judgments that may be incurred by or obtained against any Company Indemnitee's in such suits or other proceedings.

I. Federal and state laws and/or regulations may require Seller to conduct periodic background checks for Temporary Personnel assigned to certain positions (e.g., positions requiring Nuclear, NERC or TWIC access). Company may also require Seller or Seller employees be subject to additional background investigative activities completed by the Company or other 3rd party vendors, to satisfy the federal regulations for access to a nuclear facility or other NERC / TWIC regulated assets. Company will notify Seller of any assignments requiring periodic updates or re-completion of background check activities. If any worker moves from one assignment to another, Seller shall verify with Company whether a re-analysis is required.

Terms and Conditions for Remote Access and NERC CIP013

Table of Contents

1. Definitions

a. "Access" refers to any privilege or authority, which Company makes available to Contractor to view, download, create or modify Company sensitive, confidential, or proprietary information via any software or hardware.

b. "BES" means Bulk Electric System, as defined by NERC and approved by FERC, and as may change from time to time.

c. "BES Cyber Asset" means a cyber asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the BES. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact.

d. "Company Computing Resources" refers to any Company computer or electronic communications resource that processes, stores or transmits Company data or information.

e. "Company Information" means for purposes of these terms and conditions, any and all information concerning Company and its business in any form, including, without limitation, the products and services provided under this Agreement that is disclosed to or otherwise learned by Contractor during the performance of this Agreement.

f. "Computer" refers to any personal computer, laptop, or other device that is owned or used by the Contractor to access the Company Computing Resources.

g. "Disclosed" means any circumstance when the security, integrity, or confidentiality of any Company Information has been compromised, including but not limited to incidents where Company Information has been damaged, lost, corrupted, destroyed, or accessed, acquired, modified, used, or disclosed by any unauthorized person, by any person in an unauthorized manner, or for an unauthorized purpose.

h. "FERC" shall mean the Federal Energy Regulatory Commission.

i. "NERC" shall mean the North American Electric Reliability Corporation.

j. "NIST" shall mean the National Institute of Standards and Technology.

k. "Remote Session" refers to access that is established through either a dial-up connection, a wireless connection, or through a Virtual Private Network ("VPN").

l. "Security Incident" means any circumstance when (i) Contractor knows or reasonably believes that Company Information hosted or stored by the Contractor has been Disclosed; (ii) Contractor knows or reasonably believes that an act or omission has compromised or may reasonably compromise the cybersecurity of the products and services provided to Company by Contractor or the physical, technical, administrative, or organizational safeguards protecting Contractor's systems or Company's systems storing or hosting Company Information; or (iii) Contractor receives any complaint, notice, or communication which relates directly or indirectly to (A) Contractor's handling of Company Information or Contractor's compliance with the data safeguards in this Agreement or applicable law in connection with Company Information or (B) the cybersecurity of the products and services provided to Company by Contractor. This includes, but is not limited to:

   i. Attempts (either failed or successful) to gain unauthorized access to a system or its data,
   ii. Unwanted disruption or denial of service,
   iii. The unauthorized use of a system for processing data, storing data, or removing data from a system or network,
   iv. Changes to system hardware, firmware, or software characteristics (malicious code, etc.) without the owner's knowledge, instruction, or consent,
   v. Physical security breach that may have a cybersecurity impact,
   vi. Reportable cybersecurity incidents per NERC guidelines for threat and incident reporting.

2. Contractor Cybersecurity Policy

a. Contractor will provide to Company the Contractor's cybersecurity policy, which shall be consistent with NIST Special Publication 800-53 (Rev. 4), ISO 27001, and/or ISO 27002 as may be amended. Contractor will implement and comply with that cybersecurity policy. Any changes to Contractor's cybersecurity policy as applied to products and services provided to Company under the Agreement that are inconsistent with the security requirements of NIST Special Publication 800-53 (Rev. 4), ISO 27001, and/or ISO 27002, as may be amended, shall be subject to review and approval by Company prior to implementation by Contractor.

3. Notification of Incidents that Pose Cyber Security Risk

a. Contractor shall notify Company immediately, by calling the Company's Director of Compliance and Security at (313) 235-5100 and notifying Company's Cyber Security Defense Center ("CSDC"), by emailing csdc@dteenergy.com, and subsequently via written letter, whenever a Security Incident occurs.

b. Contractor agrees that Company will immediately terminate access to Company Computing Resources, until Company has re-authorized Contractor to access such Company Computing Resources.
c. The notice shall include the date and time of the Security Incident occurrence (or the approximate date and time of the occurrence if the actual date and time of the occurrence is not precisely known) and a detailed summary of the facts and circumstances of the Security Incident, including a description of (a) why the Security Incident occurred (e.g., a precise description of the reason for the system failure), (b) the amount of Company Information known or reasonably believed to have been Disclosed, (c) the IP address or computer name of affected system(s), (d) name of user(s) impacted and contact information, (e) screenshots and/or logs that may be helpful, and (c) the measures being taken to address and remedy the occurrence to prevent the same or a similar event from occurring in the future.
d. Contractor shall provide written updates of the notice to Company addressing any new facts and circumstances learned after the initial written notice is provided and shall provide such updates within a reasonable time after learning of those new facts and circumstances. Contractor shall cooperate with Company in Company's efforts to determine the risk to the BES posed by the Security Incident, including providing additional information regarding the Security Incident upon request from Company.

4. Incident Response

a. Development and implementation of a Response Plan
   i. Contractor shall have policies and procedures to address Security Incidents ("Response Plan") by mitigating the harmful effects of Security Incidents and addressing and remedying the occurrence to prevent the recurrence of Security Incidents in the future. Contractor shall provide Company access to inspect its Response Plan. The development and implementation of the Response Plan shall follow best practices that at a minimum are consistent with the contingency planning requirements of NIST Special Publication 800-61 Rev. 26, NIST Special Publication 800-53 Rev. 4, CP-1 through CP-137 and the incident response requirements of NIST Special Publication 800-53 Rev. 4, IR-1 through IR-10 as those standards may be amended, or ISO 27001, and/or ISO 27002, as may be amended.
   ii. Immediately upon learning of a Security Incident related to the products and services provided to Company, Contractor shall implement its Response Plan and, within 24 hours of implementing its Response Plan, shall notify Company of that implementation by contacting Company's CSDC.

b. Coordination of Incident Response with Company
   i. Within one (1) day of notifying Company of the Security Incident, Contractor shall recommend actions to be taken by Company on Company-controlled systems to reduce the risk of a recurrence of the same or a similar Security Incident, including, as appropriate, the provision of action plans and mitigating controls. Contractor shall coordinate with Company in developing those action plans and mitigating controls. Contractor will provide Company guidance and recommendations for long term remediation of any cyber security risks posed to Company Information, equipment, systems, and networks as well as any information necessary to assist Company in any recovery efforts undertaken by Company in response to the Security Incident.

c. Notification to Affected Parties
   i. Contractor shall, at its sole cost and expense, assist and cooperate with Company with respect to any investigation of a Security Incident, disclosures to affected parties, and other remedial measures as requested by Company in connection with a Security Incident or required under any applicable laws related to a Security Incident.
   ii. In the event a Security Incident results in Company Information being Disclosed such that notification is required to be made to any person or entity, including without limitation any customer, shareholder, or current or former employee of Company under any applicable laws, including privacy and consumer protection laws, or pursuant to a request or directive from a governmental authority, such notification will be provided by Company, except as required by applicable law or approved by Company in writing. Company will have sole control over the timing and method of providing such notification.

d. Prevention of Recurrence
   i. Within thirty (30) days of a Security Incident, Contractor shall develop and execute a plan that reduces the likelihood of the same or a similar Security Incident from occurring in the future consistent with the requirements of its Response Plan and NIST Special Publication 800-61 Rev. 2 and NIST Special Publication 800-184, ISO 27001, and/or ISO 27002, as may be amended, and shall communicate that plan to Company. Contractor shall provide recommendations to Company on actions that Company may take to assist in the prevention of recurrence, as applicable or appropriate.

e. Unrelated Security Incidents
   i. In the event (a) Contractor's confidential information has been corrupted or destroyed or has been accessed, acquired, compromised, modified, used or disclosed by any unauthorized person, or by any person in an unauthorized manner or for an unauthorized purpose; (b) Contractor knows or reasonably believes that an act or omission has compromised or may reasonably compromise the cybersecurity of the products and services provided by Contractor to an entity other than Company; or (c) Contractor receives any complaint, notice, or communication which relates directly or indirectly to (i) Contractor's handling of confidential information or Contractor's compliance with applicable law in connection with confidential information or (ii) the cybersecurity of the products and services provided by Contractor to an entity other than Company ("Unrelated Security Incident"), Contractor shall provide to Company a confidential report describing, to the extent legally permissible, a detailed summary of the facts and circumstances of the Unrelated Security Incident, including a description of (1) why the Unrelated Security Incident occurred, (2) the nature of the confidential information disclosed, and (3) the measures being taken to address and remedy the occurrence to prevent the same or a similar event from occurring in the future.

5. **Remote Access**

a. Restricted Access and Use

i. Contractor shall access and use Company Computing Resources only as necessary to perform work for Company. Contractor agrees it will not otherwise use or access Company Computing Resources for the Contractor's own use or for any other purpose.
ii. Contractor shall only access Company Computing Resources and Company data for which Contractor has been specifically granted access rights by Company.
iii. Contractor shall not attempt unauthorized access to Company Computing Resources.
iv. Contractor shall not access, or attempt to access, any third-party network or systems from Company Computing Resources, unless authorized in advance by Company.
v. Contractor shall not input, delete or otherwise modify data accessible via Company Computing Resources, except to the extent that Contractor is authorized to do so in advance by Company.
vi. Contractor shall not make any changes to Company Computing Resources, unless authorized by Company in advance.

b. Notification by Contractor when Remote or Onsite Access Should No Longer Be Granted to Contractor Representative

i. Development and Implementation of Access Control Policy: Contractor shall develop and implement policies and procedures to address the security of remote and onsite access to Company Information, Company systems and networks, and Company property (an "Access Control Policy") that is consistent with the personnel management requirements of NIST Special Publication 800-53 Rev. 4 AC-2, PE-2, PS-4, and PS-5 as may be amended, ISO 27001, and/or ISO 27002 and also meets the following requirements:
   1. Company Authority Over Access: In the course of furnishing products and services to Company under this Agreement, Contractor shall not access, and shall not permit its employees, agents, contractors, and other personnel or entities within its control ("Contractor Personnel") to access Company's property, systems, or networks or Company Information without Company's prior express written authorization. Such written authorization may subsequently be revoked by Company at any time in its sole discretion. Further, any Contractor Personnel access shall be consistent with, and in no case exceed the scope of, any such approval granted by Company. All Company authorized connectivity or attempted connectivity to Company's systems or networks shall be in conformity with Company's security policies as may be amended from time to time with notice to the Contractor.
   2. Contractor Review of Access: Contractor will review and verify Contractor Personnel's continued need for access and level of access to Company Information and Company systems, networks and property on a quarterly basis and will retain evidence of the reviews for three years from the date of each review.
   3. Notification and Revocation: Contractor will immediately notify Company in writing (no later than four (4) hours from the moment of termination or change set forth below) and will immediately take all steps necessary to remove Contractor Personnel's access to any Company Information, systems, networks, or property when:
      a. any Contractor Personnel no longer requires such access in order to furnish the services or products provided by Contractor under this Agreement,
      b. any Contractor Personnel is terminated or suspended or his or her employment is otherwise ended,
      c. Contractor reasonably believes any Contractor Personnel poses a threat to the safe working environment at or to any Company property, including to employees, customers, buildings, assets, systems, networks, trade secrets, confidential data, and/or employee or Company Information,
      d. there are any material adverse changes to any Contractor Personnel's background history, including, without limitation, any information not previously known or reported in his or her background report or record,
      e. any Contractor Personnel fails to maintain conduct in accordance with the qualification criteria set forth herein,
      f. any Contractor Personnel loses his or her U.S. work authorization, or
      g. Contractor's provision of products and services to Company under this Agreement is either completed or terminated, so that Company can discontinue electronic and/or physical access for such Contractor Personnel.
ii. Contractor will take all steps reasonably necessary to immediately deny such Contractor Personnel electronic and physical access to Company Information as well as Company property, systems, or networks, including, but not limited to, removing and securing individual credentials and access badges, RSA tokens, and laptops, as applicable, and will return to Company any Company-issued property including, but not limited to, Company photo ID badge, keys, parking pass, documents, or laptop in the possession of such Contractor Personnel. Contractor will notify Company at 313-235-7123 and csdc@dteenergy.com, once access to Company Information as well as Company property, systems, and networks has been removed.
iii. Upon notification of termination or change in access, Company will remove all Contractor Personnel's access to all Company Information, systems, networks, property, and physical locations.

c. Coordination of Controls

i. Contractor shall coordinate with Company on all remote access to Company's systems and networks, regardless of interactivity, and shall comply with any controls for interactive remote access and system-to-system remote access sessions requested by Company.
ii. Controls for Remote Access: Contractors that directly, or through any of their affiliates, subcontractors or service providers, connect to Company's systems or networks agree to the additional following protective measures:
    1. Contractor will not access, and will not permit any other person or entity to access, Company's systems or networks without Company's authorization and any such actual or attempted access will be consistent with any such authorization.
    2. Contractor shall implement processes designed to protect credentials as they travel throughout the network and shall ensure that network devices have encryption enabled for network authentication to prevent possible exposure of credentials.
    3. Contractor shall ensure Contractor Personnel do not use any virtual private network or other device to simultaneously connect machines on any Company system or network to any machines on any Contractor or third-party systems.
    4. Contractor shall ensure Contractor Personnel accessing Company networks are uniquely identified and that accounts are not shared between Contractor Personnel.
    5. Failure to comply with these requirements will result in the immediate removal of all access for Contractor Personnel.

d. Confidentiality of Information Accessed via a Company Computing Resource

Contractor agrees to follow the required controls for protection of authorized access to NERC CIP BES Critical System Information (BCSI).

i. BCSI information that will be stored and accessed from Contractor owned and managed electronic storage locations must identify the location to Company and provide all access entitlements and identify all Contractor Personnel that will require access to the storage location.
ii. Company will manage the authorization process to provide access to the Contractor managed BCSI storage location to ensure compliance with CIP004.
iii. Contractor will not provision access individuals to the Contractor Managed BCSI storage locations without express notification from Company
iv. Contractor will be responsible for performing the quarterly true-up process to comply with CIP-004 Part 4.2. Contractor must provide the current entitlement list of users with access to each managed BCSI storage location. This list will be compared with the list of authorized users with the matching entitlement(s) tracked by Company. Any discrepancies must be validated and resolved by following the *AGRTS to NERC Access Reconciliation and Remediation True-Up Process*.
v. At the close of the contract, Contractor must destroy all BCSI then document and provide evidence of the destruction of the BCSI. This is required for both electronic and physical versions of BCSI. The evidence may include, but is not limited to verification of the:
    1. Reformat of the storage location drive(s)
    2. Physical destruction of the BCSI or BCSI location
    3. Attestations of the destruction of the BCSI

e. Contractor Systems Accessing Company Computing Resource

i. Contractor computing resources, such as PCs and workstations, that access Company Computing Resources must:
    1. not be physically accessible by the general public,
    2. utilize security and password controls that restrict access to Company's Network to only authorized Contractor employees and contractors,
    3. not contain any loaded software or remote node connection which allows TCP/IP routing, unless such routing capability is disabled, and
    4. not utilize a function that automates passwords in the logon process, such as storing a password in a macro, logon script or function key, or checking the "save password" box.

f. Contractor Changes to Company Systems

i. This section applies to Contractors providing certain IT support, such as technical support for software
ii. For any changes that Contractor makes to Company's production systems, including, but not limited to programs, configuration, or environment, Contractor shall:
    1. functionally test all such changes in a test system which replicates the Company production system, (Note: If testing isn't possible, then Contractor must obtain approval from Company.)
    2. obtain prior Company approval and then schedule the change, except on an emergency exception basis, in which case, Contractor shall notify Company within four (4) hours of the change, and
    3. supply updated documentation and backout procedures, if pertinent, to Company at the time of the change.
    4. Create, maintain, and administer a written change log including: date/time, name of Company authorization personnel, and functional change, which shall be available for one year at Company's request within twenty-four (24) hours.

g. Contractor User Creation and Authentication

i. Company User ID Administration. Company shall administer the allocation of individual user IDs to Contractor. Contractor shall provide Company with the following:
   1. the full name and Date of Birth of each individual who will have access to Company's Network,
   2. the telephone number at which the individual user may be reached during business hours,
   3. prompt notification, as defined herein as no more than four (4) business hours, in writing, upon termination of employment or reassignment of personnel with access to Company's Network so that user logon IDs may be changed and other measures may be taken by Company to prevent unauthorized access,
   4. Contractor cannot transfer the logon username and password to another Contractor employee without prior approval from Company.

ii. Tracking Access and Use. In those unique situations where Contractor is a technical supplier authorized to perform only one or a series of remote sessions, Contractor will
   1. provide access and maintain a log of access authorizations for a period of one year.
   2. The log shall contain the following information for each remote session: date, user ID, first and last name of user, start of call, end of call, purpose, tests performed or actions completed.
   3. A single user ID cannot be assigned to or shared by multiple users.

iii. Protection of Credentials. Company may establish a mechanism for strong authentication credentials, such as digital certificates, tokens, smartcards, biometrics, etc. to provide access, accountability and revocation. Contractor will use the mechanism Company requires it to use.
   1. Company may administer or delegate to Contractor the administration of credentials for Contractor's operations. In either case, Contractor must validate the credential for each authorized Contractor user who will have access to Company Computing Resources.
   2. Credential attributes must provide for granular access controls within applications. Contractor will provide such information to Company at Company's request.
   3. Company will deliver credentials to Contractor in a secure manner. Contractor must disseminate credentials securely and protect them from unauthorized use.

iv. Passwords. Passwords used to authenticate Contractor user IDs or to restrict access to a resource, process or system, must comply with the following standards, which may be changed from time to time by Company with reasonable notice to Contractor:
   1. The password must have a minimum of 12 characters, with one numeric character.
   2. The password must be non-decipherable and non-associative.
   3. The password must be changed when the password has been or is suspected of having been made available to an unauthorized user.
   4. The password must be changed, at a minimum, every ninety (90) days.

v. Confidentiality of User IDs and Passwords.
   1. Contractor acknowledges that any user ID or password granted to Contractor is Company confidential information and is for Contractor's exclusive use in connection with the work.
   2. Contractor must encrypt all user IDs and passwords. Contractor shall not share, disclose or use in any unauthorized manner Company granted user IDs and passwords.
   3. Contractor is responsible for the actions of any individuals using the user IDs and passwords to access a Company Computing Resources. Contractor shall defend and hold Company harmless from any demands, claims, actions or causes of actions, losses, damages, costs, expenses, judgments, awards, fines, amounts paid in settlement and other liabilities arising out of Contractor's accessing a Company Computing Resources, and/or failure to maintain the security and confidentiality of its user IDs and/or passwords used to access a Company Computing Resources.

vi. Revocation by Company. Company may revoke such IDs and passwords at any time at Company's sole discretion, in which case the user ID or password will be deleted.

vii. Requirements to access NERC CIP Physical, Cyber, and BCSI assets. Company will require Contractor to comply with all requirements in NERC CIP004 needed to request and maintain access to Physical, Cyber, and BCSI assets owned by Company. Contractor must comply with:
   1. Contractor must complete and maintain a valid NERC PRA (Personnel Risk Assessment) as directed by NERC CIP004-6 for every individual (Party or Sub-Party) who will access Confidential information and provide evidence of the completed PRA, in the form of a completed attestation provided by Company, to Company prior to authorization to access Company cyber systems, physical security perimeters (PSPs), or BCSI documentation.
   2. Contractor will complete assigned DTE Energy NERC CIP training, as directed by CIP004-6 and designated by Company as required for electronic access to Confidential Information, cyber system access, and PSP access.

h. Contractor User Obligations

i. User Obligations. Each individual having access through Contractor to a Company Computing Resources must:
   1. Have their respective information added to the Security Schedule, which is on last page of these Terms and Conditions;
   2. use only their assigned user ID when logging on to a Company Computing Resources;
   3. log-off any Company Computing Resources before leaving their computing resources with such access unattended;
   4. not allow unauthorized individuals to access Company's Network, data or information;
   5. keep strictly confidential the logon ID, password, and all other information that enables such access;
   6. not replicate or store Company information in a way which unnecessarily exposes the information; and

ii. Contractor User Notification. Contractor must ensure that all Contractor Personnel comply with this Security Schedule, and Contractor is liable for any breach of this Schedule by Contractor Personnel. Contractor must provide security awareness training to enforce the obligations under this Security Schedule
iii. User Violation. If any Contractor Personnel violates any provision of this Security Schedule, then such employee or contractor shall not be eligible to perform services for Company through Contractor.

i. Company Computing Resources Addresses

i. Information on Company Computing Resources addresses shall not be published on any external network to which Contractor is connected.

j. Transmission of Information from Contractor

i. Encryption. Company may provide Contractor with an approved encryption mechanism for use in all electronic business transactions with Company. If provided such a mechanism, Contractor must use the Company approved encryption methodology for any electronic sharing of information with Company.
ii. Communication software. Contractor will use only Company-approved network communication programs for interactions with Company Computing Resources.
iii. Personal Firewall software. Contractor shall take all reasonable precautions to prevent potential hackers that may threaten to expose, destroy, or steal, Company's private data and personal records while interfacing directly with Company Computing Resources. Internet access broadcasts personal computer addresses to others and a personal firewall will close off the computer system to scanning and entry by blocking certain ports, prevent information from leaving the PC, and block non-trusted services or applications from accessing the computer.
    1. Contractor shall use a personal firewall on all devices used to communicate with Company Computing Resources.
    2. Contractor shall notify Company immediately if any device used to communicate with Company Computing Resources becomes vulnerable to internet exposures.
    3. List the Personal Firewall software and version that is actively running on the computers that will directly connect to the Company Computing Resources
iv. Operating System Patches. Contractor shall be responsible for preventing potential vulnerabilities that may compromise Company systems while directly connecting with Company Computing Resources.
    1. Contractor shall ensure that all computers directly connecting to the Company Computing Resources are kept up-to-date with the latest operating system security patches.
    2. Contractor shall notify Company immediately if any device used to communicate with Company Computing Resources becomes vulnerable to an operating system vulnerability.
    3. List the operating system software and version that is running on the computers that will directly connect to the Company Computing Resources

k. Remote Access Audit and Monitoring of Access and Compliance

i. Access Monitoring. Contractor, while accessing Company Computing Resources, may have its use of such network monitored and recorded by Company or its agent. Contractor expressly consents to such monitoring and recording.
ii. Remote Access Audit. Company may, upon reasonable notice, audit Contractor's compliance with the security requirements in this Security Schedule. Upon notice to Contractor, Company will have the right to visit Contractor's site to review Contractor's security measures and controls.

l. Trademarks and Notices of Intellectual Property

i. Contractor shall not remove or alter copyright or trademark notices or notices of confidentiality from any material accessed via a Company Computing Resources.

m. Disclaimers and Limitations on Liability

i. Disclaimers. Company is providing access to its network and its contents on an "as is" basis and makes no representations or warranties of any kind with respect to the Company Computing Resources or its contents. Company disclaims all such representations and warranties, whether express, implied or statutory, including, for example, warranties of merchantability and fitness for a particular purpose. Without limiting the foregoing, Company does not represent or warrant that the information accessible via its network is accurate, complete or current. The Company Computing Resources must not be relied upon in connection with any investment decision. Company does not warrant that the operation of the Company Computing Resources will be uninterrupted or error-free. Contractor is responsible for taking appropriate precautions against damage to its operations that could be caused by defects, interruptions, or malfunctions of the Company Computing Resources and assumes the risk of such occurrences. Changes are made periodically to the information contained in the Company Computing Resources. Company reserves the right to make improvements and/or changes to its Company Computing Resources or to discontinue operation of any part of it at any time.

ii. Limitations on liability. Company is not responsible for technical, hardware or software failures of any kind; lost or unavailable network connections; incomplete, garbled or delayed computer transmissions. Under no circumstances shall Company or its suppliers be liable for any damages or injury that result from the use of the materials on the Company Computing Resources.

iii. By accessing the Company Computing Resources, the Contractor agrees that neither Company nor any of its directors, employees or other representatives shall be liable for any direct or indirect loss or damages arising out of or in connection with the use of the Company Computing Resources, or the information contained in the Company Computing Resources, even if Company has been advised of the possibility of such damages. This is a comprehensive limitation of liability that applies to all damages of any kind, including (without limitation) direct, indirect, compensatory, incidental, consequential, special or exemplary damages, loss of data, income or profit, loss of or damage to property, and claims of third parties.

6. Disclosure and Remediation of Known Vulnerabilities

a. Contractor shall develop and implement policies and procedures to address the disclosure and remediation by Contractor of vulnerabilities and material defects related to the products and services provided to Company under the Agreement including the following:

i. Prior to the delivery of the procured product or service, Contractor shall provide summary documentation of publicly disclosed vulnerabilities and material defects related in the procured product or services, the potential impact of such vulnerabilities and material defects, the status of Contractor's efforts to mitigate those publicly disclosed vulnerabilities and material defects, and Contractor's recommended corrective actions, compensating security controls, mitigations, and/or procedural workarounds.

ii. Contractor shall provide summary documentation of vulnerabilities and material defects in the procured product or services within thirty (30) calendar days after such vulnerabilities and material defects become known to Contractor. This includes summary documentation on vulnerabilities that have not been publicly disclosed or have only been identified after the delivery of the product. The summary documentation shall include a description of each vulnerability and material defects and its potential impact, root cause, and recommended corrective actions, compensating security controls, mitigations, and/or procedural workarounds.

iii. Contractor shall disclose the existence of all known methods for bypassing computer authentication in the procured product or services, often referred to as backdoors, and provide written documentation that all such backdoors created by Contractor have been permanently deleted or disabled.

iv. Contractor shall implement a vulnerability detection and remediation program consistent with NIST Special Publication 800-53 Rev. 4 RA-5, SA-11, and SI-2, as may be amended.

b. Disclosure of Vulnerabilities by Company

i. Whether or not publicly disclosed by Contractor and notwithstanding any other limitation in this Agreement, Company may disclose any vulnerabilities or material defects in the products and services provided by Contractor to (a) the Electricity Information Sharing and Analysis Center, the Industrial Control Systems Cyber Emergency Response Team, or any equivalent entity, (b) to any entity when necessary to preserve the reliability of the BES as determined by Company in its sole discretion, or (c) any entity required by applicable law.

7. Software Integrity

a. Hardware, Firmware, Software, and Patch Integrity and Authenticity

i. Contractor shall establish, document, and implement risk management practices for supply chain delivery of hardware, software (including patches), and firmware provided under this Agreement. Contractor shall provide documentation on its: chain-of-custody practices, inventory management program (including the location and protection of spare parts), information protection practices, integrity management program for components provided by sub-suppliers, instructions on

how to request replacement parts, commitment to ensure that for seven (7) years, spare parts shall be made available by Contractor.

ii. Contractor shall specify how digital delivery for procured products (e.g., software and data) including patches will be validated and monitored to ensure the digital delivery remains as specified. If Company deems that it is warranted, Contractor shall apply encryption to protect procured products throughout the delivery process.
    1. If Contractor provides software or patches to Company, Contractor shall publish or provide a hash conforming to the Federal Information Processing Standard (FIPS) Security Requirements for Cryptographic Modules (FIPS 140-2) or similar standard information on the software and patches to enable Company to use the hash value as a checksum to independently verify the integrity of the software and patches and avoid downloading the software or patches from Contractor's website that has been surreptitiously infected with a virus or otherwise corrupted without the knowledge of Contractor.

iii. Contractor shall identify the country (or countries) of origin of the procured product and its components (including hardware, software, and firmware). Contractor will identify the countries where the development, manufacturing, maintenance, and service for the product are provided. Contractor will notify Company of changes in the list of countries where product maintenance or other services are provided in support of the procured product. This notification shall occur 180 days prior to initiating a change in the list of countries.

iv. Contractor shall use trusted channels to ship procured products, such as U.S. registered mail or as instructed by Company.

v. Contractor shall demonstrate a capability for detecting unauthorized access throughout the delivery process.

vi. Contractor shall demonstrate chain-of-custody documentation for procured products as determined by Company in its sole discretion and require tamper-evident packaging for the delivery of this hardware.

b. Patching Governance

i. Prior to the delivery of any products and services to Company or any connection of electronic devices, assets or equipment to Company's electronic equipment, Contractor shall provide documentation regarding its patch management and vulnerability management/mitigation programs and update process (including third-party hardware, software, and firmware) for products, services, and any electronic device, asset, or equipment required to be connected to the assets of Company during the provision of products and services under this Agreement. This documentation shall include information regarding:
    1. the resources and technical capabilities to sustain this program and process such as Contractor's method or recommendation for how the integrity of a patch is validated by Company; and
    2. Contractor's approach and capability to remediate newly reported zero-day vulnerabilities.

ii. Unless otherwise approved by the Company in writing, current or supported version of Contractor products and services shall not require the use of out-of-date, unsupported, or end-of-life version of third-party components (e.g., Java, Flash, Web browser, etc.).

iii. Contractor shall verify and provide documentation that procured products (including third-party hardware, software, firmware, and services) have appropriate updates and patches installed prior to delivery to Company.

iv. In providing the products and services described in this Agreement Contractor, shall provide appropriate software and firmware updates to remediate newly discovered vulnerabilities or weaknesses within thirty (30) days. Updates to remediate critical vulnerabilities shall be provided within a shorter period than other updates, within seven (7) days. If updates cannot be made available by Contractor within these time periods, Contractor shall provide mitigations and/or workarounds within seven (7) days.

v. When third-party hardware, software (including open-source software), and firmware is provided by Contractor to Company, Contractor shall provide appropriate hardware, software, and firmware updates to remediate newly discovered vulnerabilities or weaknesses within ninety (90) days. Updates to remediate critical vulnerabilities shall be provided within a shorter period than other updates, within thirty (30) days. If these third-party updates cannot be made available by Contractor within these time periods, Contractor shall provide mitigations and/or workarounds within thirty (30) days.

c. Viruses, Firmware and Malware

i. Contractor will use reasonable efforts to investigate whether computer viruses or malware are present in any software or patches before providing such software or patches to Company.

ii. Contractor warrants that it has no knowledge of any computer viruses or malware coded or introduced into any software or patches, and Contractor will not insert any code which would have the effect of disabling or otherwise shutting down all or a portion of such software or damaging information or functionality.

iii. When install files, scripts, firmware, or other Contractor delivered software solutions are flagged as malicious, infected, or suspicious by an anti-virus vendor through open source solutions like "Virus Total," Contractor must provide technical proof as to why the "false positive" hit has taken place to ensure their code's supply chain has not been compromised.

iv. If a virus or other malware is found to have been coded or otherwise introduced as a result of Contractor's breach of its obligations under this Agreement, Contractor shall immediately and at its own cost:
    1. Take all necessary remedial action and provide assistance to Company to eliminate the virus or other malware throughout Company's information networks, computer systems, and information systems, regardless of whether such systems or networks are operated by or on behalf of Company; and
    2. If the virus or other malware causes a loss of operational efficiency or any loss of data (A) where Contractor is obligated under this Agreement to back up such data, take all steps necessary and provide all assistance required by Company and its affiliates, and (B) where Contractor is not obligated under this Agreement to back up such data, use commercially reasonable efforts, in each case to mitigate the loss of or damage to such data and to restore the efficiency of such data.

d. End of Life Operating Systems

i. Contractor delivered solutions will not be required to reside on end-of-life operating systems, or any operating system that will go end-of-life six (6) months from the date of installation.
ii. Contractor solutions will support the latest versions of operating systems on which Contractor-provided software functions within twenty-four (24) months from official public release of that operating system version.

e. Cryptographic Requirements

i. Contractor shall document how the cryptographic system protects the confidentiality, data integrity, authentication, and non-repudiation of devices and data flows in the underlying system as specified by Company. This documentation shall include, but not be limited to, the following:
   1. The cryptographic methods (hash functions, symmetric key algorithms, or asymmetric key algorithms) and primitives (*e.g.*, Secure Hash Algorithm [SHA]- 256, Advanced Encryption Standard [AES]-256 or greater, RSA, and Digital Signature Algorithm [DSA]-2048) that are implemented in the system, and how these methods are to be implemented.
   2. The preoperational and operational phases of key establishment, deployment, ongoing validation, and revocation.
ii. Contractor will use only "approved" cryptographic methods as defined in the FIPS 1402 Standard when enabling encryption on its products.
iii. Contractor shall provide an automated remote key-establishment (update) method that protects the confidentiality and integrity of the cryptographic keys.
iv. Contractor shall ensure that:
   1. The system implementation includes the capability for configurable cryptoperiods (the life span of cryptographic key usage) in accordance with the Suggested Cryptoperiods for Key Types found in Table 1 of NIST 800-57 Part 1, as may be amended.
   2. The key update method supports remote re-keying of all devices within ninety (90) days as part of normal system operations.
   3. Emergency re-keying of all devices can be remotely performed within thirty (30) days.
v. Contractor shall provide a method for updating cryptographic primitives or algorithms.

8. Return or Destruction of Company Information

a. Upon completion of the delivery of the products and services to be provided under this Agreement, or at any time upon Company's request, Contractor shall return to Company all hardware and removable media provided by Company containing Company Information. Company Information in such returned hardware and removable media shall not be removed or altered in any way. The hardware should be physically sealed and returned via a bonded courier or as otherwise directed by Company. If the hardware or removable media containing Company Information is owned by Contractor or a third-party, a notarized statement detailing the destruction method used and the data sets involved, the date of destruction, and the entity or individual who performed the destruction will be sent to a designated Company security representative within fifteen (15) calendar days after completion of the delivery of the products and services to be provided under this Agreement, or at any time upon Company's request. Contractor's destruction or erasure of Company Information pursuant to this Section shall be in compliance with best industry practices (e.g., Department of Defense 5220-22-M Standard, as may be amended).
b. Contractor agrees that upon request of Company, it shall return to Company or destroy all items containing Company's confidential information, including all copies, abstractions and compilations. Company may further require that Contractor certify in writing that it has fulfilled its obligations under this Section.

9. Audit Rights

a. Company or its third-party designee may, but is not obligated to, perform audits and security tests of Contractor's IT or systems environment and procedural controls to determine Contractor's compliance with the system, network, data, and information security requirements of this Agreement. These audits and tests may include coordinated security tests, interviews of relevant personnel, review of documentation, and technical inspection of systems and networks as they relate to the receipt, maintenance, use, retention, and authorized destruction of Company Information. Contractor shall provide all information reasonably requested by Company in connection with any such audits and shall provide reasonable access and assistance to Company upon request. Contractor will comply, within reasonable timeframes at its own cost and expense, with all reasonable recommendations that result from such inspections, tests, and audits. Company reserves the right to view, upon request, any original security reports that Contractor has undertaken or commissioned to assess Contractor's own network security. If requested, copies of these reports will be sent via bonded courier to Company security contact. Contractor will notify Company of any such security reports or similar assessments once they have been completed. Any regulators of Company or its affiliates shall have the same rights of audit as described herein upon request.
b. These audit rights are additional to those that Company may be entitled to in regard to other aspects of the Agreement.

10. Regulatory Examinations

a. Contractor agrees that any regulator or other governmental entity with jurisdiction over Company and its affiliates may examine Contractor's activities relating to the performance of its obligations under this Agreement to the extent such authority is granted to such entities under the law. Contractor shall promptly cooperate with and provide all information reasonably requested by the regulator or other governmental entity in connection with any such examination and provide reasonable assistance and access to all equipment, records, networks, and systems reasonably requested by the regulator or other governmental entity. Contractor agrees to comply with all reasonable recommendations that result from such regulatory examinations within reasonable timeframes at Contractor's sole cost and expense. The foregoing cooperation and assistance will be rendered at Contractor's then-current time and materials rates, subject to Company's prior written authorization.

11. Contractor Personally Identifiable Information

a. For any Personally Identifiable Information ("PII") of Contractor that is disclosed to Company, Company agrees that it will treat the PII in the same manner it treats like information of its own and exercise a reasonable degree of care for preventing unauthorized disclosures of the PII. Company will not make copies of PII, disclose, disseminate or distribute PII, except for use by Company's agents, employees, or consultants with a need to know. If Company is required or requested by administrative or judicial process to disclose PII, Company shall notify Contractor so that Contractor may seek an appropriate protective order. Company may disclose PII to the extent required or compelled by administrative or judicial process, or as requested or required by the Michigan Public Service Commission or the Federal Energy Regulatory Commission.

Vendor Remote Access Security Schedule (the “Security Schedule”)

<u>Please provide the following information for all users that require access:</u>

First Name	Last Name	Phone Number	Email Address	Job Title

Contractor NERC CIP Compliance Requirements Schedule

All Contractors performing Work that requires physical or cyber access to areas containing BES Cyber Assets shall comply with the following requirements:

1. Contractor Personnel shall comply with and at all time conduct themselves in accordance with North American Electric Reliability Corporation ("NERC") Critical Infrastructure Protection ("CIP") Standards and NERC Standard NUC-001, as applicable and as amended from time to time, as well as the Company cyber security policies (OP 20 and EM 22) when providing services or performing work on Company BES Cyber Assets (Company will provide Contractor a copy of its cyber security policies and any updates as necessary).

2. Contractor shall, promptly upon Company's request, provide Company with information about Contractor Personnel necessary for Company to maintain the required records regarding personnel with authorized cyber or unescorted physical access to BES Cyber Assets, including their specific electronic and physical access rights (in compliance with NERC CIP-004). Contractor shall ensure that Contractor and its Subcontractors maintain employee access list(s) as required in CIP-004 (specifically part R4 thereof). Contractor must also notify Company within four business hours (or immediately if the applicable Contractor Personnel were terminated for cause) after any Contractor Personnel no longer requires unescorted physical or authorized cyber access to Company BES Cyber Assets to perform Work.

3. Contractor agrees that under no circumstances may authorization for unescorted physical access or authorized cyber access to Company BES Cyber Assets, or any related access badge, be transferred between Contractor Personnel.

4. Contractor Personnel who are designated by Contractor as potentially performing work for Company that would require authorized cyber or authorized unescorted physical access to BES Cyber Assets must be provided training, and be enrolled in an ongoing security awareness program, consistent with the requirements of CIP-004. All such Contractor Personnel must receive such training and be enrolled in such program within the timeframe required under CIP-004 as then currently effective. Contractor may either (1) certify that it trains Contractor Personnel using training materials provided by Company and provides a security awareness program to its employees consistent with this requirement; (2) certify that Contractor Personnel have taken or will be required to take Company -led training and are enrolled in a Company -provided program consistent with this requirement; or (3) certify that it trains Contractor Personnel using its own training materials and provides a security awareness program to its employees consistent with this requirement. Company may require additional site-specific training as it deems necessary in its sole discretion.

Contractor must conduct personnel risk assessments of all Contractor Personnel who are designated by Contractor as potentially requiring authorized cyber or unescorted physical access to Company BES Cyber Assets, and must execute a Background Screening Verification Form (which Company will provide) with respect to each such individual.