Terms and Conditions for Consulting Services

TABLE OF CONTENTS

TERMS AND CONDITIONS FOR CONSULTING SERVICES

1. DEFINITIONS

The following terms 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. "Background Technology" means all materials and information, developed or acquired by Contractor independently of the Agreement, and any derivative works made thereto in connection with this Agreement, including documents, data, know-how, ideas, methodologies, specifications, Licensed Software, Third Party Works, content, and technology, in any form or media, directly or indirectly provided or made available to Company by or on behalf of Contractor in connection with this Agreement, whether or not the same: 1) are owned by Contractor, a third party, or in the public domain, or 2) qualify for or are protected by any intellectual property rights.

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

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

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

G. "Contractor" means the person or legal entity with whom Company has entered into the Agreement.

H. "Contractor Personnel" means Contractor's employees, agents, Subcontractors and Suppliers (and their respective employees and agents), and any other personnel used by Contractor in performing Work under the Agreement.

I. "Customized Software" means the software Contractor is required to or otherwise does create for Company in connection with the Services. Customized Software does not include any Background Technology.

J. "Licensed Software" means the computer program(s), including programming tools, scripts, and routines, the Contractor provides under the Agreement, as described more fully in a scope of work and governed by Exhibit A (Software Licensing Agreement), including all updates, upgrades, new versions, new releases, enhancements, improvements, and other applicable modifications made or provided.

K. "Services" means the specific service(s) performed by Contractor as set forth in the Agreement.

L. "Subcontractor" is any person or legal entity doing all or any portion of the Work on behalf of Contractor. Except as expressly set forth in Sections 3 & 4, nothing in the Agreement shall create any contractual relationship between Company and any Subcontractor.

M. "Supplier" is any person or other entity supplying material, equipment or goods in connection with the Work on behalf of Contractor. Except as expressly set forth in Section 3, nothing in the Agreement shall create any contractual relationship between Company and any Supplier.

N. "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 Services under the Agreement, including any software (including open source software) owned by a third party, and documents, data, content, specifications, products, equipment, or components of or relating to such software, 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.

O. "Work Documents" mean all manuals, design, specifications, technical descriptions, drawings, plans, reports, calculations, summaries and other items identified as deliverables from Contractor to Company pursuant to the Agreement and other documentation necessary for Company to realize the benefits of the Services.

P. "Work Product" means all materials, notes, reports, documentation, Customized Software, literary works, graphical works, performances or displays and any derivatives, inventions, formulae, designs, processes, machines,

manufactures, composition of matter devices, or any portions thereof and any improvements on any of them prepared or developed by Contractor for Company in the performance of the Agreement. For purposes of clarity, Work Product shall not include Licensed Software, Third Party Work, or any derivatives thereto.

Q. "Laws" means all applicable federal, state and local laws, ordinances, industry standards, codes, regulations and executive orders or decrees.

2. SCOPE OF WORK

Contractor agrees to provide the Services as specified in the Agreement. Except as otherwise provided herein, Contractor may not perform extra services except pursuant to a Change Order.

3. INDEPENDENT CONTRACTOR

A. Contractor and all its employees, Subcontractors and Suppliers are, with respect to Company, independent contractors. Except as otherwise expressly provided in the Agreement, Contractor shall furnish all labor and supervision and provide all equipment, materials, tools and supplies as are necessary or incidental to the complete performance of its obligations as required and described in the Agreement. Contractor shall be solely responsible for the performance, general direction, supervision and efficient administration of the Services of Contractor Personnel. Any rights to inspect, reject, approve or otherwise oversee the Services, or other similar provisions regarding the conduct of the Services, including safety rules and practices, are for Company's benefit only (and not for any other person or entity) and do not relieve Contractor of its responsibilities.

B. Contractor shall be solely responsible for and have control over the means, methods, techniques, sequences, procedures and coordination of all portions of the Services under the Agreement. Contractor shall be solely responsible for 1) payment of any and all wages, taxes, or benefits that are due and owing to Contractor Personnel, 2) computation of compensation, unemployment compensation, overtime and fringe benefits, and 3) performance of such other duties and obligations as are required to comply with all applicable federal, state and local laws, ordinances, rules and regulations.

4. HIRING AND SUBCONTRACTING

A. For Services performed within the U.S., Contractor shall not hire aliens who are unauthorized or ineligible for U.S. employment at Contractor, pursuant to the Immigration and Nationality Act as amended (INA). Contractor shall comply with the INA verification and retention requirements for its employees hired after November 6, 1986, and with such other applicable requirements of employers as have been or will be issued, pursuant to the INA, or pursuant to the authority of the Department of Homeland Security and U. S. Citizenship and Immigration Services (USCIS) or their successors.

B. Contractor will not assign, delegate or subcontract any of its obligations or rights under the Agreement without the prior written consent of Company Representative. Any assignment, delegation or subcontract shall not relieve Contractor of 1) its responsibility to complete the Services in accordance with the terms of the Agreement, 2) its liability for any Services performed by Contractor Personnel, or 3) any other obligations that Contractor owes to Company.

C. Contractor shall incorporate the obligations of the Agreement (excluding the Licensed Software) into its respective subcontracts, agreements and purchase orders (a copy of which is to be submitted to Company upon request). Company is the intended third party beneficiary of all contracts for design, engineering or consulting services, all trade contracts, subcontracts, purchase orders and other agreements between Contractor and third parties. Contractor shall fully defend, indemnify and hold Company harmless from all acts or omissions of its Subcontractors.

5. WORK DOCUMENTS

Contractor shall deliver all Work Documents (whether or not completed) to Company upon request or termination of the Agreement. All Work Documents or Work Product furnished by Contractor in connection with the 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.

6. ELECTRONIC SUBMISSIONS

A. Contractor 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) Contractor 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) Contractor and Contractor's products comply with all applicable required cyber-security guidelines and standards. Upon Company's request, Contractor shall provide Company or Company's authorized representative with a written copy of its development security standards. Upon Company's

request, Contractor shall provide a third party assessment confirming Contractor'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 Contractor, Contractor shall reimburse Company for all labor and materials costs (whether internal or third party) incurred by Company to identify, contain and correct the effects of such virus.

7. CHANGES

A. During performance of the Services, changes to the Services may be made requiring a substitution for, an addition to, or deletion of any Service or a change in the method or manner of the Service, schedule or other requirement. Company may issue Change Orders without invalidating the Agreement, by notifying Contractor in writing and Contractor shall submit a written proposal for accomplishing the Change within ten days of notice of such request by Company, unless otherwise specified.

B. Contractor may request a change to the Services or to the Agreement by submitting a proposal of such change to Company within ten days of the occurrence of events giving rise to such change. Sufficient detail shall be given in the proposal to permit thorough analysis by Company. No amendment, alteration or modification of the Agreement or the Services shall be binding unless made pursuant to a written Change Order and, when required by Company, accepted in writing by Contractor. All Change Orders shall be supplementary to and incorporated as a part of the Agreement.

C. Contractor shall be solely responsible for any changes that are not made except to the extent such changes are made pursuant to a Change Order. No action, conduct, omission, prior failure or course of dealing by Company shall act to waive, modify, change or alter the requirement that a Change Order must be in writing executed by Company Representative.

D. If Company determines that an emergency has occurred or immediate action is required to avoid stopping or disrupting the Work in progress, the Company Representative may give Contractor an oral order, direction or instruction to proceed with a change. Contractor shall, within five days after commencement of the change, unless specified otherwise in the Agreement, provide Company with a written proposal on the effect of the change. The proposal shall be administered as provided in clause B of this Section. If no such Change Order is received by Contractor within 30 days of the event, Contractor shall have the right to suspend the services associated with the change or proceed at Contractor's own risk.

8. DISPUTE RESOLUTION

A. Contractor has the duty to promptly seek clarification and resolution of any error, omission, issue, discrepancy, misunderstanding, conflict or dispute arising from questions concerning contract interpretations or acceptable fulfillment of this Agreement on the part of Contractor and Company. Any request by Contractor for additional compensation, schedule adjustment, or other dispute resolution must be filed by Contractor and submitted to Company Representative no later than ten days after discovery of the discrepancy or no later than ten days after the occurrence of the event causing the dispute. Contractor's failure to provide such notice shall constitute a waiver by Contractor of any claim arising out of events occurring more than ten days prior to the date notice is provided to Company Representative.

B. Once Company receives notice of Contractor's formal request for dispute resolution, Company shall make every reasonable effort to arrive at a timely determination. This determination shall be provided to Contractor's authorized representative in writing. All determinations, instructions and clarifications of Company shall be final, and Contractor shall proceed with the Services in accordance with the determinations, instructions and clarifications of Company, unless Contractor protests the Company's resolutions within ten days of receipt thereof. Contractor's failure to timely protest Company's resolutions shall be considered a failure of a condition precedent to any other course of action and shall be deemed an express waiver by Contractor of all its rights to further protest, whether through arbitration, litigation or otherwise.

9. PAYMENT

A. Invoices, statement of charges or service receipts (as applicable) for Services performed shall be submitted on a timely basis, in the manner, frequency and form, and with such supporting documentation, including acknowledgment of receipt of work by Company, as required by the Agreement or as reasonably requested by Company. Company shall pay approved invoices in accordance with the payment terms specified in the Agreement or shall notify Contractor of its reasons for disapproval of such invoices. Company shall not be required to pay any portion of an invoice which is disputed in good faith until such dispute is resolved.

B. Contractor shall promptly pay its Subcontractors, Suppliers upon receipt of each payment, the respective amounts owed on account of the Services performed and to the extent of each interest therein.

C. Contractor 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 Contractor's failure to make any payments required by this Section. Nothing in the Agreement shall imply or infer an obligation of Company to make payment to any party other than Contractor.

10. GENERAL REPRESENTATIONS

Contractor represents and warrants that:

A. Contractor is qualified to perform Services in the State of Michigan or in any other state where any Services is to be performed. Execution, delivery and performance by Contractor of the Agreement have been authorized by all necessary action on behalf of Contractor.

B. The execution, delivery and performance by Contractor under the 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 Contractor is a party.

11. CONTRACTOR COVENANTS

Contractor will comply with all Laws, including but not limited to1) the applicable Laws set forth on the Schedules to these Terms and Conditions and attachments to the Agreement, 2) all applicable environmental and pollution control Laws, 3) Laws of bodies or tribunals having any jurisdiction or authority over the Services, 4) OSHA and MIOSHA, and 5) any rules or regulations of Company relating to health, safety or performance of the Services. If any discrepancy or inconsistency should be discovered between the Agreement and any such Laws, Contractor shall immediately report the same in writing to Company Representative. Contractor shall be responsible for Contractor Personnel's compliance with such Laws and shall be liable for all fines levied as a result of a violation of such Laws by Contractor or Contractor Personnel. Contractor shall immediately notify Company Representative if Contractor receives any notifications from governmental agencies alleging non-compliance with Laws or if Contractor becomes aware of any public hearings related to the Work.

12. CONFIDENTIALITY

A. Contractor recognizes and acknowledges that all information Company discloses to Contractor or which Contractor may have access during Contractor's performance of the Agreement is considered proprietary and confidential by Company, unless otherwise designated. Such information shall be used by Contractor only in connection with performing the Services and shall remain the property of Company. Contractor shall disclose such information to Contractor Personnel only to the extent necessary to perform the Services or other obligations under the Agreement. Contractor shall advise such persons of the existence of the Agreement, of the confidential nature of the information and of Contractor's obligations regarding same under the Agreement. Except as otherwise provided herein, Contractor and Contractor Personnel 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 Contractor or Contractor Personnel, 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. Contractor shall be responsible for any breach of these confidentiality obligations by Contractor Personnel.

B. Contractor 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 Contractor or Contractor Personnel, 2) is ordered to be disclosed by a court or administrative agency, or 3) is thereafter developed independently by Contractor.

C. In the event that Contractor is requested or required under compulsion of legal process to disclose such information, Contractor shall not, unless required by law, disclose the information until Company has first 1) received prompt written notice of such request or requirements to disclose, and 2) had an adequate opportunity to obtain a protective order or other reliable assurance that confidential treatment shall be accorded to the Confidential Information. Contractor shall not oppose actions by Company to assure such confidential treatment.

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

13. TAXES

A. Contractor accepts exclusive liability for all payroll taxes now or hereafter imposed by the United States or any state or local government, and any penalties and interest on such payroll taxes, resulting from amounts paid to Contractor Personnel. Such persons shall in no event be the employees of Company. Contractor agrees to indemnify Company for any such payroll taxes, penalties and interest levied against Company or which Company may be required to pay.

B. Contractor agrees to indemnify Company from any and all taxes under Section 4980B of the Internal Revenue Code of 1986, as amended, and any penalties and interest thereon, resulting from the failure of Contractor to satisfy the continuation coverage requirements provided in such section with respect to persons used by Contractor in performing under the Agreement. Contractor shall pay all income, property, sales and use, excise and any other taxes now or hereafter imposed by the United States or any state or local government, and any penalties and interest on such taxes, arising out of Contractor's performance of the Work, and shall indemnify Company for all such taxes, penalties and interest levied against Company or which Company may be required to pay.

C. Unless otherwise provided in the Agreement, Contractor shall pay all Michigan sales and use taxes on all materials used in performing the Work. If Contractor is purchasing materials pursuant to the Agreement, Contractor will provide an executed Sales and Use Tax Affidavit in the form attached hereto as Exhibit 1, confirming that the Company's payments under the Agreement includes all applicable sales and use tax and that such taxes have been remitted to the proper taxing authority. If Contractor (or its subcontractors) acquire materials that will be incorporated into the Work or that are for Company's use, then only for the purpose of the tax exemptions listed in this Section, Contractor (or its subcontractors) are acting as Company's agent in acquiring such materials.

D. Contractor shall break out all mixed-use services/materials on invoices as separate line items. If Contractor fails to do so, then such amount shall not be considered sales and use tax payable by Company. If Contractor receives any sales and use tax audit or related correspondence from the State of Michigan related to the Work, Contractor shall notify Company within three (3) business days.

E. Certain materials purchased pursuant to the Agreement may be exempt from sales tax by reason of industrial processing. Specifically, electrical generation materials and equipment qualify for a 100% industrial processing exemption from Michigan sales and use tax. Materials other than electrical generation materials and equipment may also be exempt from Michigan sales and use tax; however, such items will be exempt from Michigan sales and use tax only up to the corresponding exemption percentage listed in the applicable chart below:

ELECTRICAL MATERIALS AND EQUIPMENT:

Category	Exemption Percentage	Tax Rate
Transformers and Components	90	0.6%
Stations and Substations	90	0.6%
Poles and Pole Top Equipment	25	4.5%
Distribution Tools and Supplies	50	3.0%
Wires and Cabling	25	4.5%
Personal Safety and Equipment	50	3.0%
Customer Meters	25	4.5%

GAS MATERIALS AND EQUIPMENT USED WITHIN COMPANY'S NATURALGAS TRANSMISSION AND DISTRIBUTION SYSTEM (GAS SYSTEM EQUIPMENT):

Category	Exemption Percentage	Tax Rate
Equipment Pre-City Gate	100	0.0%
Equipment Post-City Gate	50	3.0%

14. INSURANCE

A. Prior to the start of the Services, Contractor shall provide Company with Certificate(s) of Insurance evidencing that insurance coverage of the types, amounts, and conditions specified in the Appendix entitled, “Insurance Provided by Contractor,” are in effect. Contractor affirms to Company that such insurance coverage shall remain in effect during the life of the Agreement.

B. Contractor 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, Contractor shall insure the activities of its Subcontractors.

15. INTELLECTUAL PROPERTY

A. Contractor represents and warrants that it has authority to grant, and hereby grants to 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 Services while performing Services (except for Licensed Software, the terms of which are governed exclusively by Exhibit A (Software Licensing Agreement).

B. Except for Licensed Software, 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(s) in electronic native-file format as well as Adobe Portable Document Format (PDF) upon request and upon expiration, termination or completion of the Agreement.

C. Company and Contractor agree that all Work Product is a Work-Made-For-Hire under the copyright laws of the United States. In addition, if any Work Product is not Work-Made-For-Hire, Contractor 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 Work Product. Contractor 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 the Agreement, Contractor agrees to assist Company in every reasonable way, at Company’s cost, to secure, maintain and defend for Company’s benefit all intellectual property rights it may have in any whole or part of the Work Product.

E. Notwithstanding the foregoing, Contractor shall retain ownership of all its Background Technology, provided that the Company shall have a transferable license to use such Background Technology to the fullest extent necessary to realize the benefits of the Services.

F. Contractor warrants that all materials, equipment and processes used or supplied, Work Product and the Services performed are free from infringement of any patent, trademark or other intellectual property right. Contractor shall pay all royalties and license fees necessary for the proper performance of the Services.

G. Contractor 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 or service performed pursuant to the Agreement constitutes an infringement or violation of any patent, trademark or other proprietary right. Company shall at Contractor’s expense give such information and assistance as it may deem appropriate for the defense of same, and Contractor 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, Contractor 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, or 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.

16. WARRANTY

Contractor represents and warrants that all Services 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. Contractor acknowledges and agrees that Company will be relying on the accuracy, competence and completeness of the Services to be performed and will use the results of such Services as input data for Company projects, including (in certain instances) construction projects. If at any time during the one year period after the product of Contractor’s Services are incorporated into a Company project (or such other period of time for this warranty as is expressly set forth in the Purchase Order or scope of work document expressly incorporated into the Purchase Order), it appears that the Services provided do not conform to the foregoing warranties, Company shall notify Contractor of such breach of warranty within a reasonable time after discovery and Contractor shall promptly provide services as necessary (including, if applicable, redesign and testing) to correct any nonconforming Services. The warranty for corrected Services shall be of equal duration and scope as the original warranty and commence upon Company’s acceptance of such corrected Services.

16. SUSPENSION

A. Company may at any time and for any reason, order Contractor to suspend, or interrupt all or any part of the Work for such period of time as appropriate for the convenience of Company.

B. If the performance of all or any part of the Work is suspended by Company, an adjustment shall be made for any increase in the cost and time of performance of this Agreement directly caused by such suspension. However, no adjustment shall be made under this Section for any suspension to the extent that performance would have been so suspended, delayed, or interrupted by any other provision of the Agreement, including due to the fault or negligence of Contractor.

C. Upon such suspension, Contractor waives all claims for damages, including, but not limited to, loss of profits, idle equipment, labor and facilities, and any claims of Contractor Personnel. Contractor's sole compensation for any suspension under this Section shall be either reasonable demobilization or standby costs, in each case, as agreed to by Company.

D. Upon receipt of notice to resume the suspended Work, Contractor shall resume performance to the extent required in the notice and, within ten days, submit to Company a revised schedule for review that reflects the effect of the suspension on the schedule. Contractor shall be reimbursed for its reasonable mobilization costs. These adjustments shall be limited to such matters as cost increases required under labor, Subcontractor or Supplier agreements in effect on the date of suspension.

17. TERMINATION FOR CONVENIENCE

Company may at any time, upon ten days written notice to Contractor, terminate the Agreement in whole or in part. Upon receipt of such notice, Contractor shall discontinue providing Services on the date and to the extent specified in the notice and shall thereafter do only such work as may be necessary to preserve and protect the Services already in progress. Upon such termination, Contractor waives all claims for damages as a result of such termination including, but not limited to, loss of anticipated profits, and any claims of Subcontractors or Suppliers as a result of such termination, and shall accept the value of all Services completed through the date of termination as sole and complete compensation. No termination fee(s) shall be payable by Company.

18. TERMINATION FOR CAUSE

A. Contractor shall be in default if at any time 1) Contractor refuses, neglects or fails in any respect to perform the Services hereunder or any portion thereof with promptness, diligence or in accordance with any of the provisions set forth herein, 2) Contractor refuses, neglects or fails to perform any other obligations under this Agreement or provide adequate assurances of performance, 3) Contractor makes an assignment for the benefit of creditors or bankruptcy or insolvency proceedings are instituted by or against Contractor, or 4) in Company's sole judgment, Contractor's financial or other condition or progress on the Agreement shall be such as to endanger timely performance.

B. If Contractor fails to remedy such default within 48 hours after receipt by it of such written notice (or, if such default is incapable of being remedied within 48 hours, Contractor fails to commence taking steps to remedy such default as quickly as possible, but, in any event within 30 days), Company may, in writing, and without notice to Contractor's sureties, if any, terminate the Agreement and/or pursue any other remedies available under the Agreement, by law, or in equity.

C. Upon receipt of notice of termination, Contractor shall return any Company property, deliver all Work Product in progress, and provide Company with all intellectual property rights in any Work Product.

D. Termination is not Company's exclusive remedy and is in addition to any other rights and remedies it may have under the Agreement or by law. Failure of Company to exercise any of its rights under this Section shall not excuse Contractor from compliance with the provisions of the Agreement nor prejudice rights of Company to recover damages for such default.

19. INDEMNIFICATION

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

B. In the event any suit or other proceedings for any claim, loss, damage, cost, charge or expense covered by Contractor's foregoing indemnity should be brought against any Company Indemnitee, then upon Company's request Contractor hereby covenants and agrees to assume the defense thereof and defend the same at Contractor'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, Contractor shall at once cause the same to be dissolved and discharged by giving bond or otherwise.

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 Contractor or any of Contractor's affiliated companies, to Company or to any of Company's affiliated companies, against sums payable by Company.

22. RECORDS AND AUDITS

Company or its authorized representative shall have access to Contractor's records to review, audit, and verify any information connected with the Agreement for a period of three years after the calendar year in which the work is completed. Contractor will provide Company or its authorized representative with access to all personnel, property, books, and records necessary to effectuate such audits. Contractor 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 the Agreement or any of its rights or obligations hereunder shall be made by Contractor without first obtaining the written consent of Company. The Agreement shall be binding upon and shall inure to the benefit of the respective successors and permitted assigns of the parties hereto.

24. FORCE MAJEURE

A. Except as otherwise provided herein, Contractor shall not be liable for a reasonable delay or default in performing Services 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 days of the commencement of any excusable delay described in clause A above, Contractor must notify Company Representative in writing of the nature, cause, date of commencement and expected impact of the event. Contractor must exercise due diligence in proceeding to meet its performance, obligations hereunder notwithstanding the delay. Upon Contractor 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 shall be sent to Company Representative and Contractor's representative identified 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 the 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 the Agreement which by their nature extend beyond 1) the termination or cancellation of this Agreement, or 2) the completion of the work shall survive and remain in full force and effect and apply to respective successors and assigns.

29. NON-EXCLUSIVITY

It is agreed that the Agreement is not exclusive, and that nothing herein shall be deemed to prevent Company from engaging others to perform any of the Services or to prevent Company from performing any of the Services through its own employees or agents.

30. CONSTRUCTION OF TERMS; SECTION HEADINGS

The terms of the 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 the 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.” All references to day(s) shall mean calendar day(s), unless otherwise expressly specified. The section headings contained in the Agreement are for convenience of reference only and shall not affect the meaning or interpretation hereof.

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 or the location of the Company Site where Services are performed, as applicable, without regard to its conflict of law principals. The parties agree that any action with respect to the 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 the Company and Contractor respecting the Services and no modification of the Agreement shall be effective unless 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 by the Agreement.

B. Any document submitted by Contractor (including any Contractor document referenced in the Agreement) is used solely for the purpose of describing the Services 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 counteroffer to Company and shall not be binding upon Company unless specifically accepted in writing by Buyer. In the absence of written acceptance of such counteroffer by Company, commencement of performance by Contractor shall be deemed to be an agreement by Contractor 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 Contractor to be physically present on any Company site, Contractor shall also comply with the provisions set forth in the attached On-Site Services Schedule.

34. NUCLEAR POWER PLANT ADDITIONAL TERMS

If Contractor performs any Work for or at a Company nuclear power plant, Contractor shall comply with the attached Nuclear Terms Schedule attached hereto, which may be modified by Company from time to time to conform to any change in law.

35. FEDERAL CONTRACTING REQUIREMENTS AND FOREIGN CORRUPT PRACTICES ACT

Contractor shall comply with the Federal Contracting Requirements and Foreign Corrupt Practices Act as set forth on the attached Federal Requirements Schedule, which may be modified by Company from time to time to conform to any change in law.

36. BACKGROUND INVESTIGATION REQUIREMENTS

Contractor 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. PROTECTION OF SENSITIVE PERSONAL CONFIDENTIAL INFORMATION
Contractor shall comply with the requirements set forth in the attached Protection of Sensitive Personal Confidential Information Schedule, which may be modified by Company from time to time to conform with any change in law, if Contractor will have access to "Sensitive Personal Confidential Information" as described in such schedule. To the extent any provisions of the Protection of Sensitive Personal Confidential Information Schedule conflict with the provisions set forth in Section 12 of these Terms and Conditions (Confidentiality), the provision of the Protection of Sensitive Personal Confidential Information Schedule will control.

38. 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.

39. NERC CIP COMPLIANCE
If Contractor requires physical or cyber access to areas containing BES Cyber Assets, Contractor shall comply with the attached Contractor NERC CIP Compliance Requirements Schedule, which may be modified by Company from time to time to conform with any change in Law.

40. 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.

EXHIBIT 1 – SALES & USE TAX AFFIDAVIT

SALES & USE TAX AFFIDAVIT

(STATE OF MICHIGAN)
) ss
COUNTY OF)

The Undersigned,_____ _____, hereby represents that on _____, 20__ it was awarded a contract by (the "Company"), to construct a project in accordance with the terms and conditions of Contract No.("Contract"); and Undersigned further represents that the subject work has now been accomplished and the Contract has now been completed. Undersigned hereby warrants and certifies that the payments made by Company to Undersigned under Contract were inclusive of all applicable sales and use taxes arising by reason of Contract and that Undersigned has fully paid and remitted to the proper taxing authority all said sales and use taxes. Undersigned further agrees that, if any claim should hereinafter arise, it shall assume responsibility for the same immediately upon request to do so by the Company. This affidavit is freely and voluntarily given with full knowledge of the facts, on this ___day of _____, 20___.

_____
_
(CONTRACTOR)

By:
_____

Its:
_____

Subscribed and sworn to before me, a

Notary Public in and for_____ County, State of _____,
on this _____ day of _____, 20___.

Notary Public:

My Commission Expires: _____

ON-SITE SERVICES SCHEDULE

CONTRACTOR'S EMPLOYEES, AGENTS, SUBCONTRACTORS

A. Contractor Personnel who are working on Company premises shall comply with all federal, state and local laws, ordinances, codes and regulations, and Company policies prohibiting unlawful discrimination and harassment.

B. At Company's request, Contractor shall remove any Contractor Personnel that Company deems incompetent, disorderly, insubordinate, careless or otherwise objectionable, at any time.

SAFETY AND SECURITY

A. Contractor shall take all necessary precautions for the protection of the health and safety of Contractor Personnel, 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 Services.

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 Contractor for loss and/or damages to persons or property.

REPORTING OF ACCIDENTS

(A) Contractor must verbally notify either (1) the Company employee (or his/her designee), who oversees the work day-to-day and is assigned as the contact for the activities of Contractor Personnel working at the Site ("DTE Representative") or (2) the Company employee (or his/her designee) who is assigned as being responsible for safety communications between Contractor and Company ("Designated Safety Person") whenever Contractor Personnel reports a work-related injury/illness.

(B) Injuries/Illnesses resulting in Medical Treatment will be reported to DTE Energy Legal Investigations at: 313.235.3604 during hours 8:00 am – 5:00 pm, Monday-Friday, or 24-hotline at 313.235.3600, during hours 5:00 pm - 8:00 am, Monday-Friday, weekends and holidays.

(C) Within 72 hours of the work-related injury/illness, Contractor must complete and submit a written report to either its DTE Representative or Designated Safety Person outlining:

(1) Description of event/incident which resulted in the injury/illness,

(2) Investigation report outlining Causal Analysis and Corrective Actions. Company does not mandate which Causal Analysis Tool will be employed, however have made available the National Safety Council – Guide for Causal Analysis and Corrective Actions. This tool can be found on the Quest Site, Corporate Safety – One Stop Shop for Safety Reporting and Recordkeeping). Corrective Actions are required to include a targeted Date of Completion.

(D) The Contractor is to make available at Company's request all reports, findings or other documents relating to the Contractor's investigation of the incident.

(E) Company reserves the right to conduct its own investigation on any incident/illness occurring on Company's property. Such an investigation may include, but not be limited to, inspection of the incident site, interviews of employees, the procurement of physical evidence, and employee statements deemed necessary by Company.

(F) Accidents involving death or serious injury shall be cause, upon Company's discretion, to have the Contractor made ineligible for further work pending review by the Company's Safety and Health Representative(s).

NUCLEAR TERMS SCHEDULE

PROTECTION AND INSPECTION OF MATERIALS

If Contractor is providing goods for delivery to or for use at a Company nuclear power plant, Contractor 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, Contractor 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, Contractor 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, Contractor shall assure that the materials supplied by Contractor meet all requirements of the latest version of the applicable manufacturer data sheet, description, and/or industry standard unless otherwise specified. If the Contractor is not the manufacturer of the materials, the Contractor shall make reasonable efforts to assure that the materials supplied under the Agreement are made by the original manufacturer and meet the applicable manufacturer data sheet or industry standard. Should Contractor desire to supply an alternate item that may not meet the requirements of this paragraph, Contractor 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 the 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 Purchaser for the removal, replacement and reinstallation of such materials in accordance with the warranty provisions applicable to the Agreement.

INSURANCE

Company shall, without cost to Contractor, procure and maintain liability and property damage insurance coverage for "nuclear incidents" prior to fuel delivery and during plant operation, as described below:

A. Nuclear Liability Insurance
(1) An agreement of indemnification as contemplated by Section 170 of Act (as defined below), as amended.
(2) Self-Insurance or nuclear liability insurance from American Nuclear Insurers (ANI) or other, in such form and in such amount as shall meet the financial protection requirements of Section 170 of Act, as amended.

In the event that the nuclear liability protection provisions established by Section 170 of the Act, as amended, is repealed or changed, Company shall maintain in effect during the period of Plant operation comparable protection or insurance in limits which Company deems reasonable in the light of existing conditions for plants of similar size and character and in accordance with the practice then prevalent for such similar plants.

B. Nuclear Property Damage Insurance - Nuclear property damage insurance available from Nuclear Mutual Limited (NML) and other excess insurance in such form and in such amount deemed reasonable by Company.

INDEMNIFICATION

Company agrees to indemnify and hold harmless Contractor and its subcontractors for losses, claims, damages, or liabilities arising out of or from a “nuclear incident” as defined in the Atomic Energy Act of 1954 (the “Act”), as amended, and to the extent recovery is available under the Nuclear Liability Insurance provisions required by the Agreement, the foregoing shall in no manner restrict or limit Contractor’s or its subcontractor’s obligations or liabilities under any other provision of the Agreement, except as such obligations or liabilities arise out of a “nuclear incident.”

ADDITIONAL PROVISIONS

Contractor is encouraged to utilize employees who have been previously trained and screened at a Company nuclear plant, if possible, to expedite in-processing and assure the passing of training. Failure to pass initial training on the first attempt will result in remedial training, increased costs, and possible delayed schedules. Company is not responsible for increased costs due to failed training. All personnel working in the radiological restricted area are required to have base level radiation worker training and have accurate annual dose records.

Contractor shall specify, as part of its quote if known at that time, but in no event later than 30 days prior to shipment to Company, whether each device or component Contractor is providing to Company either IS or IS NOT a “Digital Asset” under the following definition:

“Digital Asset”: A device that uses any combination of hardware, firmware, or software to execute internally stored programs and algorithms, including numerous arithmetic operations, without operator action (e.g., a microprocessor based component with configurable software (including firmware) and data). Solid state devices (e.g., electro-mechanical on/off devices, relays, hard-wired logic devices, circuit boards, etc.) that do not have firmware and/or software are not considered Digital Assets.

If the item is identified as a Digital Asset, then Contractor shall additionally provide the type of digital component and the revision of the software or firmware.

Contractor and its personnel shall at all times comply with the Nuclear Generation Supplemental Terms and Conditions, as modified by Company from time to time.

FEDERAL REQUIREMENTS SCHEDULE

A. Company, as a federal contractor, requires that Contractor 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 Contractor is exempt thereunder: Equal Opportunity, FAR 52.222-26 (applies to all orders) and 41 CFR 60.1.4; 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 Contractor'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, Contractor 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 contractors 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 "Contractor," "Company" and "Company Representative", respectively.

(2) Except to the extent that this Agreement is exempt from any of these requirements, Contractor agrees to be bound by and comply with the clauses set forth at 48 CFR 52.219-8 (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. Contractor does hereby represent, warrant and covenant that:

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

(4) Contractor 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 Contractor and its agents pursuant to the Agreement to ensure compliance with the FCPA. Contractor 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) Contractor 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.

BACKGROUND INVESTIGATION REQUIREMENTS SCHEDULE

A. Contractor 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, Contractor 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 contractor 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. Contractor must validate eligibility through E-Verify.
- Driving History (where permitted by law and if contractor is required to operate a Company motor vehicle).

D. Unless restricted by applicable law, all convictions for misdemeanors or felonies shall be reviewed by Contractor 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 Contractor 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, Contractor 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. Contractor provides Company an ongoing representation and warranty that it has conducted background checks consistent with the requirements set forth in this Schedule. Further, if Contractor 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. Contractor 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 Contractor, its Subcontractors and Suppliers, or property or both, arising directly or indirectly out of or in connection with Contractor'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 Contractor's foregoing indemnity shall be brought against any Company Indemnitee, Contractor hereby covenants and agrees to assume the defense thereof and defend the same at Contractor'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 Contractor 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 Contractor or Contractor 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 Contractor of any assignments requiring periodic updates or re-completion of background check activities. If any worker moves from one assignment to another, Contractor shall verify with Company whether a re-analysis is required.

PROTECTION OF SENSITIVE PERSONAL CONFIDENTIAL INFORMATION SCHEDULE

1. **Definitions**.

1.1. “Sensitive Personal Confidential Information” shall have the meaning set forth in Attachment A to this Protection of Sensitive Personal Confidential Information Schedule.

1.2. “Offshore” means any location which is not physically within the United States, Canada or their respective territorial possessions and subject to United States or Canadian Law.

1.3. “Offshore Outsourcing” means any work related with Company data not performed within Canada or the United States.

1.4. “Director, Compliance and Security” means the Company representative responsible for the DTE Energy information security program management. The mailing address and notification number for the Director, Compliance and Security is:

Director, Compliance and Security
One Energy Plaza
749 GO
Detroit, MI 48226
Ph: 313-235-5100

1.5. “One-way hash” means a cryptographic algorithm that generates a fixed string of numbers from a text message. As used herein, "one-way" means that it is extremely difficult to turn the fixed string back into the text message.

1.6. “Vulnerability” means a “flaw” or “weakness” in a system or application that could be triggered or intentionally exploited, resulting in a security incident or breach through which an intruder can easily gain control at the administrator level of any affected host or possibly access Sensitive Personal Confidential Information processed, transmitted or stored by the affected host.

1.7. “Vulnerability Management” means a security practice designed to identify, track, and mitigate vulnerabilities in order to minimize the risk of the exploitation of those vulnerabilities.

1.8. “Code Review” means the identification of potential areas of weakness or actual vulnerabilities. The areas that must be prioritized for investigation are (a) code that handles user input, especially file upload, (b) code that changes frequently, (c) code which calls system-level functions or executes with elevated permissions, (d) code that uses language-specific functions (e.g. file access) and (e) code that handles highly sensitive personal information.

1.9. "Secure Coding Practices" means software coding practices that adhere to industry best practices for system or application protection and that follow such industry-identified guidelines.

2. **General**. Contractor may only use Sensitive Personal Confidential Information in connection with completing the Work. Sensitive Personal Confidential Information is and shall, at all times, remain the property of Company. Contractor shall disclose such information to Contractor Personnel only to the extent necessary to perform the Work or other obligations under the Agreement. Contractor shall advise such persons of the existence of this Agreement, of the confidential nature of the information and of Contractor's obligations regarding same under this Agreement. Except as otherwise provided herein, Contractor and Contractor Personnel shall not disclose Sensitive Personal Confidential Information to any third party for any reason or purpose whatsoever. In the event of a breach or threatened breach of these confidentiality obligations by Contractor or Contractor Personnel, 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. Contractor shall be responsible for any breach of these confidentiality obligations by Contractor Personnel.

3. **Contractor Data Security Program**. Contractor shall maintain a data security program that meets

or exceeds the expectations defined in this Agreement.

4. **Audit and Examination.**

4.1. Annual General Audit. Contractor agrees to allow Company to perform at least one information security audit annually that consists of a review of information security policies, a review of Contractor's information security incident response plan, a review of vulnerability management procedures, a review of disaster recovery documentation, a review of signed nondisclosure agreements, network perimeter vulnerability scans, web application vulnerability scans and visits to any location(s) where Sensitive Personal Confidential Information is stored, transmitted, or processed.

4.2. Code Audit. In addition to the foregoing General Audit, Contractor agrees that Company or a Company-approved third party vendor may perform, at any time, in Company's sole discretion, code analysis on any code created by Contractor for Company ("Contractor-Developed Code") to ensure that the Contractor-Developed Code is not vulnerable and that Secure Coding Practices were adhered to in the creation of such Contractor-Developed Code. Such testing may include but is not limited to Code Review, penetration testing and scanning of the Contractor-Developed Code by a third-party software designed for such purposes.

5. **Information Handling, Protection, and Disposal.** Contractor represents and warrants that any medium and/or media that contain Sensitive Personal Confidential Information for the purposes of delivery or transfer between Company and Contractor is sufficiently secured and protected to prevent disclosure or examination by any unauthorized party.

5.1. Contractor shall immediately revoke access privileges to Sensitive Personal Confidential Information for Contractor Personnel following their separation (either involuntarily or voluntarily).

5.2. Before providing any media to a Subcontractor, Contractor must redact or obfuscate any Sensitive Personal Confidential Information contained in such media that Subcontractor does not need to perform its Work.

5.3. Prior to Contractor, or any Subcontractor, storing or accessing Company data offshore, pre-approval must be provided in writing by the Director, Compliance and Security. If Contractor desires to store or access Company data offshore, then Contractor must complete the form (see Attachment B) to the best of its ability and send it to the Company Representative. The Company Representative will then work with the respective DTE business unit reps to determine whether Contractor is granted permission to store or access Company data offshore.

5.4. Contractor shall ensure that any Sensitive Personal Confidential Information is encrypted in transit and at rest using a method or tool which encrypts the Sensitive Personal Confidential Information using a mutually agreed upon encryption algorithm of sufficient strength that it renders the Sensitive Personal Confidential Information unreadable and unintelligible by any means other than decryption. Contractor shall ensure that the encryption key or keys used to encrypt the information is not stored on the media or medium with the Sensitive Personal Confidential Information nor transmitted in the same session as the Sensitive Personal Confidential Information.

5.5. Contractor shall properly dispose of any Sensitive Personal Confidential Information, documents and media that contain any Sensitive Personal Confidential Information. Company defines "properly dispose of Sensitive Personal Confidential Information" as being in the state that is beyond recognition and beyond reconstruction. Specifically, data should be destroyed in one of the following methods:

5.5.1. Contractor will format and overwrite the media with meaningless data – either with some fixed pattern (e.g. binary zeroes) or random data. There are numerous software utilities that are designed to securely remove files from disks.

5.5.2. Contractor will degauss the media – Degaussing equipment is available for magnetic tapes, hard disks, and floppy disks.

3.5.3 Contractor will destroy the media – by crushing, incinerating, cross-cut shredding, or melting.

5.6. Upon destruction, the Contractor will notify the Company Representative that the Sensitive Personal Confidential Information has been destroyed within 72 hours of the completed action. Further, Company maintains the right to request proof of data destruction after notification from the Contractor that the Sensitive Personal Confidential Information has been destroyed. The Contractor will provide Company with proof of data destruction within 72 hours of request for the information. Formal notification and method of destruction must be submitted in writing to the Company Representative and the Director, Compliance and Security.

5.7. Contractor agrees to provide Company's Director, Compliance and Security at least 30 days prior written notice if Contractor is contemplating on moving its facility where the Sensitive Personal Confidential Information is stored. During that 30 day period, at Company's sole discretion, Company may initiate a review of the Vendor Security Review Questionnaire (VSRQ) and perform an information security audit.

5.8. Even after the termination or expiration of the Agreement, Contractor represents and warrants that it shall continue to protect any Sensitive Personal Confidential Information in accordance with these confidentiality obligations as long as Contractor possesses any Sensitive Personal Confidential Information.

6. **Password Security**

6.1. Contractor shall ensure that passwords are encrypted using a one-way hash of sufficient strength that it is rendered unreadable and unintelligible.

6.2. Passwords or Login IDs shall never be distributed to end users in clear text via email messages.

6.3. The following password standards must be programmatically enforced

6.3.1. All passwords shall change at least every 90 days.

6.3.2. Passwords can only change once every two days.

6.3.3. The previous five passwords shall not be repeated.

6.3.4. All passwords shall contain a minimum of 12 characters.

6.3.5. All passwords shall contain a minimum of one alpha and one numeric character.

7. **Security Incident and Response**. Contractor shall notify the Company Representative and the Company's Director, Compliance and Security at 313 235-5100 within twenty-four (24) hours of any breach of security which has, or which there is reasonable cause to believe has, exposed any Sensitive Personal Confidential Information to unauthorized parties.

8. **Security Awareness and Compliance**. Contractor shall provide annual information security awareness training for its personnel assigned to provide services to Company. Contractor shall maintain training attendance documentation for a minimum of twenty-four (24) months following the termination of the respective Company Contract or Purchase Order and, if requested by Company, make the documentation available for review by Company.

9. **Vulnerability Management**

9.1. Contractor shall develop, maintain and adhere to documented procedures for network vulnerability management, including quarterly scanning of systems transmitting, processing or storing any Sensitive Personal Confidential Information.

9.2. Vulnerability management procedures shall define timely remediation of detected vulnerabilities.

9.3. Contractor shall accurately log all activities of network vulnerability scanning and remediation and maintain appropriate documentation of sufficient detail that demonstrates reasonable good faith efforts to remediate vulnerabilities on systems which contain or have the potential to contain any Sensitive Personal Confidential Information. Contractor shall maintain this documentation for a period not less than 24 calendar months and provide same to Company upon request.

9.4. Contractor shall develop, maintain and adhere to documented procedures for vulnerability management. Those procedures shall include some automated inspection or scanning of any code transmitting, processing or storing any Sensitive Personal Confidential Information for OWASP Top 10 Most Dangerous Programming Errors.

9.5. Contractor shall accurately log all activities of any code vulnerability scanning and remediation and maintain appropriate documentation of sufficient detail that demonstrates reasonable good faith efforts to remediate vulnerabilities in any code which transmit, process or store any Sensitive Personal Confidential Information. Contractor shall maintain this documentation for a period not less than 24 calendar months and provide same to Company upon request.

10. **Disaster Recovery.** Contractor shall develop and maintain a disaster recovery plan ("DRP") which will provide for a back-up system and plan to maintain operations in the event of an emergency or catastrophe that would otherwise significantly impact the ability to perform services.

11. **Secure Coding.** Contractor shall develop, maintain, and disclose to Company the frameworks, Code Reviews, code analyzing tools, and methodologies that Contractor applies to identify and reduce common programming errors that may lead to any vulnerable code. Contractor shall adhere to Secure Coding Practices.

12. **Operating System**. Contractor must use and maintain an operating system, which is updated on an as-needed and required basis for security and operating system fixes. These security and operating system fixes must be maintained by the Contractor's suppliers and vendors as well as downstream distributors. Contractor shall immediately notify Company in writing if Contractor is unable to maintain the obligations in this section.

Attachment A
To Protection of Sensitive Personal Confidential Information Schedule

1.1. "**Sensitive Personal Confidential Information**" means:

1.1.1. The following customer related information, either alone or in combination with one or more of the following:

1.1.1.1. A name, number, or other information that is used for the purpose of identifying a specific person or providing access to a person's financial accounts, including, but not limited to, a person's name, address, telephone number, date of birth, driver's license or state personal identification card number, social security number (or any number derived from such number), place of employment, personal email address, personal phone number, energy consumption, payment history, employee identification number, employer or taxpayer identification number, government passport number, health insurance identification number, mother's maiden name, credit rating or credit history, demand deposit or other financial account number, or credit card or debit card number in combination with any required security code, access code, or password that would permit access to any of the resident's financial records, savings account number, financial transaction device account number or the person's account password, stock or other security certificate or account number, credit card number, vital record, or medical records or information.

1.1.2. The following Highly Sensitive Personal Information, either alone or in combination with one or more of the following:

1.1.2.1 Protected Health Information (PHI), medical prescription, medical screening, testing, results, and psychological records as defined by the Health Insurance Portability and Accountability Act (HIPAA) and/or covered under applicable Company policies, social security number, tax ID number, employee ID number, credit/debit card number(s), credit verification value (CVV), bank and investment account numbers, driver's license/state ID number, alien registration number, work permit number, account password, PINS, biometric data (e.g., fingerprint, voice, retina print, used for authentication), digitized signatures, date of birth or death, savings account number, financial transaction device account number or the person's account password, stock or other security certificate or account number.

1.1.3. Company employee records, including, but not limited to, an address including zip and other geocodes (when combined with other information in this subcategory), personal email address, personal phone number, salary, performance ratings, social security number or federal ID number, work permit number, bank account numbers.

1.1.4. Company shareholder information, including, but not limited to, an address including zip and other geocodes (when combined with other information in this subcategory), personal email address, personal phone number, number of shares, social security number or national ID number.

1.2 "Sensitive Personal Confidential Information" shall not include any such information which (1) becomes known to the public through no act or omission of Contractor or Contractor Personnel; (2) is ordered to be disclosed by a court or administrative agency; or (3) is thereafter developed independently by Contractor.

Attachment B
To Protection of Sensitive Personal Confidential Information Schedule

Instructions for completing this form: Contractor is to fill in as much information as possible and then forward that form to Company Representative.
Contractor does not have Company's permission to store or access Company's data offshore until Company and Contractor further discuss this matter and until both parties sign this form below. Company retains the right, in its sole discretion, to not approve this request.

Request Date: _____

Company's Contract Number: _____

Company's Purchase Order Number: _____

Information regarding Contractor's representative submitting this request:

1. Name: _____
2. Phone number: _____
3. Email address: _____

Is Contractor requesting permission to store Company data offshore, access Company data offshore, or both (enter which one): _____

Which Country and City will Company's data be stored or accessed from: _____

Company's approval as of {enter date}
_____

Company
By:
Name: _____
Title: Security Relationship Manager

Company's approval as of {enter date}
_____

Company
By:
Name: _____
Title: Director, Compliance and Security

Company's approval is granted subject to the following conditions:
_____

Contractor's Acceptance {enter date}
_____

By:
Name: _____
Title: _____

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. ".

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

f. "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.

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

h. "

i. "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.

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

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

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

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

n. "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”)

PLEASE PROVIDE THE FOLLOWING INFORMATION FOR ALL USERS THAT REQUIRE ACCESS:

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.