Purchase Order

Mail Invoice To:

Follow Invoice Instructions
As Shown Below

Purchase Order	:	**03209687**
Revision	:	
Printed	:	**11/20/2025**
Issue Date	:	**11/20/2025**

Invoice Instructions:

All original invoices and supporting documentation shall be issued via the Ariba Network either directly through your Ariba Network Account or through the interactive email you received from Ariba. Nuclear Purchase Order invoices must reference the Purchase Order, applicable Release, and the correct Line Number; Nuclear Contract invoices must reference the Contract and its associated Release Number. Failure to do so will impact invoice processing.
When submitting through the Ariba Network, it is required that the Suppliers original invoice be added as an attachment to the submission.

For the rare instances of a Supplier who either cannot submit through the Ariba Network or has not yet signed up for their Ariba account, the following method is appropriate on a temporary basis:
Electronically as a single invoice portable document file (PDF or TIF) no larger than 25mb to DukeNuclearInvoices@duke-energy.com.

Suppliers that have not yet signed up for their Ariba account, please reach out to AribaSupplierEnable@duke-energy.com to start the process.
All invoice related questions should be sent to APQuestions@duke-energy.com.
Payment term is calculated based on the date an acceptable invoice is received.

Duke Energy EIN Number 56-0205520
Duke Energy Florida, Inc. FL Tax (Form DR 16P) Permit Number TPP-1047
Duke Energy Carolinas, LLC – NC Permit # NC00026, SC Tax Certificate # 1317293-037
Duke Energy Progress, LLC – EIN 56-0165465, NC Permit #NC00007, SC Tax Certificate # 1289532-000

Please Direct Inquiries to:

JOHN F EMERSON

Title: NSC PROCUREMENT SPEC

Phone: 864-873-4071

Fax:

Email: John.Emerson@duke-energy.com

Vendor:

CANOIL CANADA LTD
Solongo Lewis
62 TODD ROAD
GEORGETOWN ON L7G 4R7

Phone: 905/820-2022

Fax: .

Quality Approved Manufacturer:	ANY SUPPLIER	**Manufacturer**	QAV #A036
Quality Oversight Requirements:	No Oversight Requirements		
Commercial Grade Quality Program:	None Listed		
Manufacturer Address:	ANY ADDRESS ANY CITY 99999		

Purchase Order

Mail Invoice To:

Follow Invoice Instructions
As Shown Below

Purchase Order	:	**03209687**
Revision	:	
Printed	:	**11/20/2025**
Issue Date	:	**11/20/2025**

Payment Terms		**%**	**Days**	**Net**	45 **Days**
ERS	N	**Reference Contract**			

Primary Ship To: OCONEE NUCLEAR STATION
155 East Pickens Highway
Seneca SC 29672

Attention: Receiving Ph 864-873-3731

Instructions Please confirm receipt of PO REF RFQ 34032

Purchase Order

Mail Invoice To:

Follow Invoice Instructions
As Shown Below

Purchase Order	:	**03209687**
Revision	:	
Printed	:	**11/20/2025**
Issue Date	:	**11/20/2025**

Fac	Standard Name	Rev	Header Terms & Conditions - Applies to All Lines
	05	001	Info to be Shown on Packing list, Invoices,etc
	1P	002	Invoice Requirement
	59	001	Shelf Life Requirement
	64	000	MSDS REQUIREMENT
	7D	020	Routing Instructions
	7E	021	INSTRUCTIONS TO SELLER
	81	001	No Substitution without approval
	45025	036	DUKE ENERGY CORP. TERMS AND CONDITIONS OF PURCHASE

Line	Quantity	UP	Item Description			Unit Price	Extension
0001	240	BL	**Catalog ID:**	0000864146	**PQL:** 2	$17.92	$4,300.00

Schedule: **Quantity:** 240 **Delivery Date:** 12/18/2025

Transit Type:

COMMERCIAL GRADE

Description LUBRICANT, GREASE, PASTE, 120 LB KEG, MOV LONG LIFE, NLGI GRADE 1

TYPE:
FORM: PASTE
CONTAINER: 120 LB KEG
DE NUMBER:
DUKE CLASS:
TRADE NAME: MOV LONG LIFE, NLGI GRADE 1

MFR SPECIFIC INFO: MOV LONG LIFE, NLGI 1
APPLICATION: LIMITORQUE ACTUATORS
PROCUREMENT: SHALL BE FROM A SINGLE
BATCH/LOT NUMBER
PACKAGING: LABEL CONTAINER WITH
MANUFACTURER NAME AND PRODUCT NAME (MOV
LONG LIFE GRADE 1)

Quality Approved Manufacturer: ANY SUPPLIER QAV #A036

Purchase Order

Mail Invoice To:

Follow Invoice Instructions
As Shown Below

Purchase Order	:	**03209687**
Revision	:	
Printed	:	**11/20/2025**
Issue Date	:	**11/20/2025**

Manufacturer: CHEMTURA

Model:

Part: BY DESCRIPTION

FAC	Standard Name	Rev	Applies to Line	Lines Terms and Conditions
	PE004-002	001	0001	ITEMS, PARTS AND/OR PACKAGING IDENTIFICATION
	PE004-005	000	0001	CONTAINER(S) IDENTIFIED TO A BATCH/LOT NUMBER.
	PE007-001	002	0001	NO SUBSTITUTIONS ALLOWED
	PE007-002	000	0001	ONLY NEW MATERIALS SHALL BE SUPPLIED

Purchase Order Total Amount

TOTAL THIS PO: $4,300.00

Fac	Standard Name	Rev	Applies to Line	Terms and Conditions
	05	001	ALL	Info to be Shown on Packing list, Invoices,etc

PURCHASE ORDER NUMBER, CATALOG ID NUMBER, PO LINE ITEM NUMBER AND PART(S) NUMBER (AS APPLICABLE) MUST BE SHOWN ON ALL PACKING LISTS, BOXES, CARTONS, REELS, PART(S) TAGS, AND INVOICES. (05)

	1P	002	ALL	Invoice Requirement

To ensure timely payment, the invoice price, quantity, and unit of measure must exactly match the purchase order. To do otherwise, may cause the invoice to be returned to you or payment to be delayed.

Any special charges authorized on your PO such as Certificate of Compliance (C of C), Expediting, and Rental Charges, (etc.) need to be listed on the same invoice as the material.

	59	001	ALL	Shelf Life Requirement

Purchase Order

Mail Invoice To:

Follow Invoice Instructions
As Shown Below

Purchase Order	:	**03209687**
Revision	:	
Printed	:	**11/20/2025**
Issue Date	:	**11/20/2025**

IF APPLICABLE, ITEMS ON THIS ORDER REQUIRE SPECIAL SHELF LIFE CONSIDERATION. THE SELLER SHALL PROVIDE SHELF LIFE DOCUMENTATION TO THE BUYER PRIOR TO OR AT TIME OF SHIPMENT. IN LIEU OF DOCUMENTATION BOTH THE MANUFACTURED DATE AND EXPIRATION DATE MAY BE IDENTIFIED ON THE ITEM OR ITS PACKAGING.
THE ITEMS ON THIS ORDER MUST BE FURNISHED WITH A MINIMUM OF 80% SHELF LIFE REMAINING FROM THE MANUFACTURED DATE

64 000 ALL MSDS REQUIREMENT

MATERIAL SAFETY DATA SHEETS USED TO COMPLY WITH OSHA'S HAZARD COMMUNICATION STANDARD, 29CFR1910.1200, MUST BE FORWARDED WITH THE SHIPMENT OF THIS MATERIAL. THE PRODUCT TRADENAME ON THE MATERIAL SAFETY DATA SHEET MUST MATCH THE NAME THAT APPEARS ON THE PRODUCT LABEL.
(64)

7D 020 ALL Routing Instructions

Routing Instructions

Routing instructions are an integral part of this Purchase Order. Failure to comply with these instructions in any manner without prior approval of Duke Energy Logistics Group will be construed as a direct violation of this contract. In the event routing instructions cannot or should not be executed as instructed in this Purchase Order, Vendor is instructed to contact the buyer or Duke Energy Logistics Group at (800) 279-8729 or SCLogistics@Duke-Energy.com for revised routing instruction. Failure to comply with these instructions will result in freight charges being for the Vendor's account.

In the event this Purchase Order is generated from an existing contract between Duke Energy, or a subsidiary thereof, and the Vendor, all shipping terms and conditions established by the contract will apply.

In the event the material is to be shipped as Freight Origin Collect (OC), the Vendor must ship per the following guidelines:

Parcel: Shipments routed Parcel are not to exceed 150 lbs. and parcel allowable measurements for the total shipment. Weights and measurements exceeding these limits are to be referred to the Duke Energy Logistics Group for revised shipping instructions. Use of multiple bills/shipments to circumvent these weight limits are not acceptable, and if so used, all freight charges will be for the Vendor's account. Vendor must utilize Duke Energy's online freight route guide at DukeEnergyFreight.com to enter a shipping request. The online freight route guide will generate a pre-paid UPS label.

Vendor acknowledges and agrees that it will indemnify Duke Energy for costs to the extent directly caused by the negligent or willful misuse by Vendor, any of its employees, subcontractors, or agents, of Duke Energy's freight account number (s)/information.

Less-Than-Truckload (LTL): Shipments routed LTL are to be between 150 lbs. - 10,000 lbs., not to exceed 10 linear feet, and material not to be greater than $75,000 in total value. Vendor must utilize Duke Energy's online freight route guide at DukeEnergyFreight.com to enter a shipping request.

* Pipe that is not crated or palletized cannot be shipped LTL, regardless of dimensions. Please contact the Duke Energy

Purchase Order

Mail Invoice To:

Follow Invoice Instructions
As Shown Below

Purchase Order	:	**03209687**
Revision	:	
Printed	:	**11/20/2025**
Issue Date	:	**11/20/2025**

Logistics Group at (800) 279-8729 or SCLogistics@Duke-Energy.com for logistics service.

Truckload, Expedited, and Other: For all orders greater than 10,000 lbs., exceeding 10 linear feet, exceeding $100,000 in total value, or requiring expedited shipping, air freight, truckload, or special transportation equipment, vendor must contact the Duke Energy Logistics Group at (800) 279-8729 or SCLogistics@Duke-Energy.com. Vendor must call 24 hours prior to shipment date or immediately upon notification of expedited or air shipments.

For non-emergent shipments, Vender must notify Duke Energy twenty-four (24) hours prior to pick-up request date.

If Vendor requests a Duke Energy shipment and the material is not ready upon the arrival of the truck causing a Truck Ordered and Not Used (TONU) charge, these charges will be passed to the Vendor through a credit memo to the associated Purchase Order. If the Vendor cancels a scheduled shipment more than twelve (12) hours prior to the scheduled pick-up request, the TONU charge will not apply.

If Vendor causes detention charges due to Vendor negligence, the detention charges will be passed to the Vendor through a credit memo to the associated Purchase Order.
In the event routing instructions cannot be executed, contact the Duke Energy Logistics Group at (800) 279-8729 or SCLogistics@Duke-Energy.com.

Guidelines for Wood Packing Materials. U.S., Canada and Mexico are strictly enforcing "International Standards for Phyto-sanitary Measures Publication No. 15(ISPM 15)". Wood packing for all shipments that require customs clearance, including skids, crates and pipe dunnage must be treated to the ISPM 15 standard and is required to bear the unique certification stamp. Seller wi ll be responsible to insure all goods shipped meet ISPM standards.

Vendor Managed Freight. In the event the material is being shipped under Vendor’s management (i.e. Master Contract, or freight terms sanctioning vendor to manage), the Vendor should defer to the Terms and Conditions and/or buyer for the appropriate routing guidance. If a shipment is 10 feet in length or greater, the item must be transported on open truck/flat bed. Palletized items shipped in covered trucks shall not exceed the width of the truck rendering offloading from rear entry implausible/unsafe. Pallet orientation shall be such that horizontal entry from back of truck is utilized.

7E	021	ALL	INSTRUCTIONS TO SELLER

Purchase Order

Mail Invoice To:

Follow Invoice Instructions
As Shown Below

Purchase Order	:	**03209687**
Revision	:	
Printed	:	**11/20/2025**
Issue Date	:	**11/20/2025**

INSTRUCTIONS TO SELLER

1. DUKE ENERGY ("BUYER")AGREES TO PURCHASE ,AND SELLER AGREES TO SELL, SOLELY ON THE TERMS AND CONDITIONS OF THIS PURCHASE ORDER, THE GOODS (COLLECTIVELY, "GOODS") AND THE SERVICES (COLLECTIVELY, "SERVICES") DESCRIBED IN THIS PURCHASE ORDER. NO TERM OF ANY ORDER CONFIRMATION OR ANY OTHER DOCUMENT ISSUED BY SELLER AND NOT EXECUTED AND DELIVERED BY AN AUTHORIZED EMPLOYEE OF BUYER SHALL BIND BUYER. BUYER'S PURCHASE OF THE GOODS AND SERVICES IS EXPRESSLY CONDITIONED ON SELLERS ACCEPTANCE OF THE TERMS AND CONDITIONS OF THIS PURCHASE ORDER. BUYER OBJECTS TO ALL DIFFERENT AND ADDITIONAL TERMS IN SELLER'S ORDER CONFIRMATION AND OTHER DOCUMENTS.

2. UNLESS OTHERWISE STATED BELOW,BUYER'S FORM 45025 (Latest Rev) IS INCORPORATED BY REFERENCE AND WILL GOVERN THIS PURCHASE ORDER.

3. IF FREIGHT IS PREPAID AND ADDED TO INVOICE, ATTACH FREIGHT BILL OR OTHER APPROPRIATE SHIPPING PAPERS. PURCHASE ORDER NUMBER AND ID NUMBERS MUST BE SHOWN ON ALL INVOICES, PACKING LISTS, CORRESPONDANCE, AND BOXES.

4. IF SELLER DOES NOT RECEIVE A COPY OF THE TERMS AND CONDITIONS APPLICABLE TO THIS PURCHASE ORDER, CONTACT BUYER.

(7E)

81	001	ALL	No Substitution without approval

NOTIFY THE BUYER IMMEDIATELY IF ANY OF THE PART NUMBERS SHOWN ON THIS PURCHASE ORDER HAVE BEEN REVISED,SUPERSEDED OR OTHERWISE CHANGED.
SUPPLIER SHALL NOT SUBSTITUTE OTHER ITEMS FOR ITEMS REQUESTED WITHOUT WRITTEN APPROVAL OF THE BUYER PRIOR TO SHIPMENT. MATERIALS/ PARTS FURNISHED ON THIS ORDER SHALL BE NEW. USED OR RE-MANUFACTURED ITEMS ARE NOT ACCEPTABLE.

(81)2

45025	036	ALL	DUKE ENERGY CORP. TERMS AND CONDITIONS OF PURCHASE
PE004-002	001	ALL	ITEMS, PARTS AND/OR PACKAGING IDENTIFICATION

ITEMS, PARTS AND/OR PACKAGING MUST BE IDENTIFIABLE BY ORIGINAL MANUFACTURER PART NUMBER AND NAME AND/OR TRADEMARK.

PE004-005	000	ALL	CONTAINER(S) IDENTIFIED TO A BATCH/LOT NUMBER.

CONTAINER(S) SHALL BE CLEARLY IDENTIFIED TO A BATCH/LOT NUMBER.

PE007-001	002	ALL	NO SUBSTITUTIONS ALLOWED

Purchase Order

Mail Invoice To:

Follow Invoice Instructions
As Shown Below

Purchase Order	:	**03209687**
Revision	:	
Printed	:	**11/20/2025**
Issue Date	:	**11/20/2025**

NO SUBSTITUTIONS ARE ALLOWED WITHOUT WRITTEN APPROVAL OF THE BUYER PRIOR TO SHIPMENT.

THE SUPPLIER IS TO NOTIFY THE BUYER OF ANY PARTS OR PART NUMBERS SHOWN ON THIS PURCHASE ORDER THAT HAVE BEEN REVISED, SUPERSEDED, OR OTHERWISE CHANGED AND ANY KNOWN MANUFACTURING CHANGES, UPGRADES, PROBLEMS, OR PERFORMANCE ISSUES.

PE007-002	000	ALL	ONLY NEW MATERIALS SHALL BE SUPPLIED

ONLY NEW MATERIALS SHALL BE SUPPLIED. REFURBISHED OR USED ITEM
S, COMPONENTS AND/OR ACCESSORIES ARE NOT ACCEPTABLE.

End of Purchase Order

DUKE ENERGY STANDARD TERMS AND CONDITIONS
FOR PURCHASES OF GOODS AND SERVICES

SECTION 1: DEFINITIONS

1.1 Parties. Under these Duke Energy Standard Terms and Conditions for Purchases of Goods and Services ("**Standard Terms and Conditions**"), the term "**Duke Energy**" shall mean the Duke Energy legal entity listed on the face of the Purchase Order (as defined below) to or within which these Standard Terms and Conditions are attached or included, or one of Duke Energy's authorized affiliates or assigns, and the term "**Seller**" shall mean the legal entity or individual person listed on the face of said Purchase Order as the party from which Duke Energy is purchasing Goods or Services under the Agreement. Duke Energy and Seller are each referred to in these Standard Terms and Conditions as a "**Party**" and collectively as the "**Parties**."

1.2 General.

"**Agreement**" shall mean (and shall be interpreted in the following order of priority in the event of a conflict among them): (a) any Amendment or Change Order signed by both Parties; (b) the Purchase Order issued to Seller or agreed to in writing by Duke Energy to which these Standard Terms and Conditions are attached or included; (c) these Standard Terms and Conditions, including the Attachments and Supplements incorporated herein by reference; and (d) any exhibit(s) in addition to these Standard Terms and Conditions, or schedule(s), or descriptions and specifications attached to the applicable Purchase Order and incorporated into the Agreement by reference therein.

"**Goods**" shall mean the goods or products set forth in the applicable Purchase Order or to be delivered by the Seller or its subcontractors to Duke Energy under the Agreement.

"**Purchase Order**" shall mean purchase orders, statements of work, contract orders and contracts (including those to or within which these Standard Terms and Conditions are attached).

"**Services**" shall mean all work, services and actions (including pursuant to any warranty obligations) and related and reasonably inferable obligations to be performed by Seller or its subcontractors under the Agreement, including any such activities in connection with, or relating to, the Goods.

SECTION 2: SCOPE

Seller and its subcontractors, if any, shall provide any and all Goods and perform any and all Services in accordance with all terms of the Agreement, including any specific requirements contained in the applicable Purchase Order.

SECTION 3: COMPLIANCE WITH LAWS AND PROCEDURES

3.1 Legal Requirements. Seller and its subcontractors, if any, shall observe and abide by all applicable federal, state, foreign and local laws, statutes, rules, regulations or orders, any and all rules, orders, and regulations promulgated thereunder, and the rules and regulations of any lawful regulatory body acting under such laws in connection with the Services or Goods ("**Legal Requirements**"), including but not limited to such requirements related to: (i) labor, employment, and immigration, including laws relating to the verification of Seller's workers' eligibility to work in the United States, including the Immigration Reform and Control Act of 1986 and Form I-9 requirements, and laws and regulations prohibiting discriminatory practices with respect to employment and occupation; (ii) export and import control laws and regulations; (iii) the Foreign Corrupt Practices Act (15 U.S.C. Section 78dd-1, et. seq.); (iv) Executive Order 13706, and Executive Order 13496 (29 CFR Part 471, Appendix A to Subpart A); (v) the Equal Employment Opportunity provisions contained in 41 C.F.R. 60-300.5(a), and 41 C.F.R. 60-741.5(a), and the reporting clause set forth in 41 C.F.R. 61-300.10; (vi) the Federal Acquisition Regulation ("FAR") clauses listed in FAR 52.244-6(c)(1); (vii) the Federal Aviation Regulations (Title 14 CFR); (viii) the Occupational Safety and Health Act of 1970 and the regulations and standards issued thereunder; and (ix) if applicable to Seller's performance of the Services, the ACA requirements set forth in Attachment A, and all amendments of any of the foregoing that may be made from time to time.

(a) This contractor (Duke Energy) and subcontractor (Seller) shall abide by the requirements of 41 CFR 60-300.5(a) and 60-741.5(a). 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.

(b) For any Services that are to be performed in South Carolina, Seller certifies that it will comply with the applicable requirements of Title 41, Chapter 8 of the South Carolina Code of Laws and agrees to provide, upon request any documentation required to establish that Seller and its subcontractors are in compliance with Title 41, Chapter 8 of the South Carolina Code of Laws. Seller shall provide to Duke Energy written evidence of Seller's compliance with this requirement at least five days prior to beginning any Services subject to this requirement.

(c) Seller will obtain, at its expense, all permits and licenses required to perform any Services, unless otherwise specified in the Purchase Order.

3.2 Duke Energy Rules, Programs and Procedures. Seller and its subcontractors, if any, shall observe and abide by all Duke Energy rules, programs, policies, and procedures, including but not limited to the following:

(a) Compliance with Regulatory Code of Conduct. Seller acknowledges that Seller may be given access to or otherwise become aware of certain operational information of Duke Energy, the disclosure of which to departments or affiliates of Duke Energy is prohibited by federal law. Such operational information includes, but is not limited to, (i) planned outage schedules, (ii) events of forced outages and generating derating, (iii) construction schedules, (iv) operational practices at Duke Energy's generating stations, and (v) transmission system planning and operational data. Seller shall, and shall require its subcontractors to (A) maintain the strict confidentiality of such operational information, and (B) not share such operational and planning information with any third parties, including any other departments or affiliated entities of Duke Energy, without prior written consent, which shall be granted in Duke Energy's sole discretion.

(b) Fraud and Ethics. At all times during performance of the Services, Seller shall be familiar with and adhere to the principles of Duke Energy's Supplier Code of Conduct located at http://www.duke-energy.com/pdfs/Supplier_Code_of_Conduct.PDF; provided, however, that if Seller provides notice to Duke Energy that it is required to adhere only to its own code of conduct, and not Duke Energy's, during performance of the Services, Seller hereby (i) acknowledges that it is aware of Duke Energy's Supplier Code of Conduct, (ii) agrees to implement, administer, and comply with Seller's own code of conduct and ethics and compliance guidelines (collectively, "**Seller's Code of Conduct**") during performance of the Services and to promptly provide a copy thereof to Duke Energy upon its request, and (iii) certifies that Seller's Code of Conduct is substantially similar to, and no less stringent than, Duke Energy's Supplier Code of Conduct. Seller shall promptly report any alleged or confirmed fraud, illegal activity, fiscal waste or abuse, or other violations of Duke Energy's Supplier Code of Conduct or Seller's Code of Conduct, as applicable, by any party, including Seller's suppliers and service providers, and any other events or media coverage that could reasonably be expected to impact or cause harm to the parties' relationship, Duke Energy's business or the Duke Energy brand. Such activity may be reported by contacting: (A) Duke Energy's contract administrator or assigned project manager; (B) Duke Energy's EthicsLine managed by an independent third party at 866.8ETHICS (866.838.4427), which may be called anonymously, or by web submittal at https://ethicsline.duke-energy.com/; or (C) by sending an e-mail to Duke Energy's Ethics and Compliance Office at EthicsOfficer@duke-energy.com.

(c) No Conflict of Interest. Seller warrants that it has given no commissions, payments, gifts, kickbacks, lavish or extensive entertainment or other things of value to any employee or agent of Duke Energy or anyone else in connection with the Agreement in violation of Duke Energy's Supplier Code of Conduct located at http://www.duke-energy.com/pdfs/Supplier_Code_of_Conduct.PDF, and acknowledges that the giving of any such payments, gifts, entertainment, or other things of value is strictly in violation of Duke Energy's policy and may result in the cancellation of the Agreement and any other agreements between the Parties. Seller shall notify Duke Energy 's Ethics and Compliance Office of any such solicitation by any of Duke Energy's employees or agents.

(d) Nuclear Station Services. If any of the Services will be performed by Seller inside the Owner Controlled Area of a Duke Energy nuclear station (other than Services performed at fossil units within the

Owner Protected Area), the terms and conditions of Duke Energy Nuclear Supplement NS0001 shall apply to the Agreement, and such terms are hereby incorporated by reference as if set forth herein in full.

3.3 Regulator Examinations. Seller agrees that any regulator or other governmental entity with jurisdiction over Duke Energy and Duke Energy's affiliates may examine Seller's activities relating to the performance of Seller's obligations under the Agreement to the extent such authority is granted to such entities under the law. Seller 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. Seller agrees to comply with all reasonable recommendations that result from such regulatory examinations within reasonable timeframes at Seller's sole cost and expense.

3.4 Electronic Communications. If, in Duke Energy's sole discretion, Duke Energy desires to i) more effectively communicate electronically with Seller; and ii) automate various operations between Duke Energy and Seller, then the parties shall utilize Duke Energy's third party e-commerce service provider, currently Ariba Network, or as otherwise identified by Duke Energy to Seller from time to time ("E-Commerce Provider"). Upon prior written notice to Seller, Duke Energy, in its sole discretion, may change to another E-Commerce Provider. The parties acknowledge and agree that use of an E-Commerce Provider will allow the parties to transmit to one another various documents and communications, including but not limited to, purchase orders, work orders, change requests, advance ship notices, delivery schedules and receipt confirmations, requests for proposals, invoices, acknowledgements, catalogs, catalog punch-outs, portal usage, fees, discount rates, acceptances of discounts, reports provided by Seller to Duke Energy, product literature and information, parts lists, notices as required or allowed hereunder, clarifications and confirmations (collectively, "E-Documents").

SECTION 4: DUKE ENERGY'S REVIEW, APPROVAL AND COMMENT

Seller shall be responsible for any discrepancies, errors or omissions in any documents, reports or other such materials prepared by Seller or Seller's subcontractors, without regard to whether such documents, reports or other such materials have been reviewed or approved by Duke Energy. No such Duke Energy approval, review or lack of review shall be deemed an approval or acceptance by Duke Energy of any portion of the Goods or Services, nor shall any such Duke Energy approval, review or lack of review create any liability on the part of Duke Energy. Duke Energy's approval, either with or without comments or modification(s) of any documents, reports or other such materials furnished by Seller or Seller's subcontractors shall not relieve Seller of any responsibility or liability imposed upon Seller by any provisions of the Agreement.

SECTION 5: SUBCONTRACTING

5.1 General. Seller shall not delegate, subcontract or otherwise outsource all or any portion of its obligations, duties or other responsibilities under the Agreement without the prior written consent of Duke Energy. Upon prior written notice and with the written consent of Duke Energy (such consent not to be unreasonably withheld), Seller may have any portion of the Services or delivery of Goods performed by subcontractors. Seller and any proposed subcontractors must meet the specific safety criteria as defined in the Duke Energy EHS Supplemental Requirements included in Duke Energy's EHS Orientation and Training located at https://www.duke-energy.com/partner-with-us/suppliers/ehs-orientation-training. If subcontracting is authorized by Duke Energy, Seller shall continue to be responsible for the delivery of the Goods or completion of the Services. Seller shall be fully responsible for all acts, omissions, failures, and faults of all of its subcontractors as fully as if they were the acts, omissions, failures and faults of Seller. If requested by Duke Energy, Seller shall provide Duke Energy with copies of any contracts with third parties regarding the delegation, subcontracting or other outsourcing of any of Seller's duties under the Agreement. All subcontracts by Seller shall be in writing and Seller shall obtain terms and conditions in its contracts with subcontractors and suppliers which are consistent with the rights of Duke Energy and the duties of Seller in the Agreement, which Seller shall not waive, release, modify or impair. Any attempted delegation, subcontracting or other outsourcing by Seller, its subcontractors or its suppliers without Duke Energy's prior written consent shall be ineffective and void. No contractual relationship shall exist between Duke Energy and any of Seller's subcontractors, if any, with respect to the Goods or Services.

5.2 Prohibited Subcontractors and Equipment. Notwithstanding anything contained herein to the contrary, in no event shall Seller or any of its subcontractors subcontract with, outsource to, or use any equipment or services, including in any Goods or Services provided hereunder, from any party identified in the Covered List set forth in 47 U.S. Code Sections 1601-1609.

5.3 Diverse and Local Suppliers. If the total compensation to Seller under the Agreement will equal or exceed $750,000.00, Seller shall adopt and utilize a subcontracting plan (a) to use subcontractors who meet the description of at least one of the categories of diverse suppliers set forth at http://www.duke-energy.com/suppliers/supplier-diversity-definitions.asp ("**Diverse Suppliers**") and (b) to use Local Suppliers, as defined below. Seller shall: (x) use commercially reasonable efforts to utilize Diverse Suppliers and Local Suppliers; and (y) provide Duke Energy a quarterly status report in Duke Energy's Power Advocate reporting tool and in a format reasonably acceptable to Duke Energy containing Seller's Diverse Supplier and Local Supplier spend. Duke Energy's designated auditors shall have the right of access during normal business hours to inspect Seller's records related to compliance with this Section 5.3. For the purposes of this Section 5.3, "**Local Supplier**" shall mean a subcontractor of Seller who has a headquarters or branch within at least one of the states in which the applicable Goods or Services are provided under the Agreement.

SECTION 6: SCHEDULE; DELAY LIQUIDATED DAMAGES

6.1 Time of the Essence. Time is of the essence with respect to the Goods and Services to be delivered and performed under the Agreement.

6.2 Schedule. Seller shall perform and complete its obligations under the Agreement, including complete the Services and deliver the Goods, within and in accordance with the schedule provided in the applicable Purchase Order, as modified from time to time in accordance with the Agreement ("**Schedule**"). The Schedule includes, as applicable, the agreed final completion date for the Services and/or the agreed final delivery date for the Goods.

6.3 Delay Liquidated Damages. The Parties may agree in a Purchase Order that Seller shall deliver the Goods and/or complete the Services on or before a guaranteed delivery date ("**Guaranteed Delivery Date**"). The Parties agree that it would be extremely difficult and impracticable under the presently known and anticipated facts and circumstances to ascertain and fix the actual damages Duke Energy would incur if Seller does not deliver the Goods or Services by the Guaranteed Delivery Date. Accordingly, the Parties agree that if Seller does not meet the Guaranteed Delivery Date, Duke Energy's remedy for that delay shall be to recover from Seller as liquidated damages, and not as a penalty, the amount of liquidated damages, if any, set forth in the applicable Purchase Order, for each day or portion of a day completion or delivery, as applicable, is delayed beyond the Guaranteed Delivery Date ("**Delay Liquidated Damages**"). The Delay Liquidated Damages shall not limit Duke Energy's remedies for other breaches, actions or omissions of Seller. The Delay Liquidated Damages shall be due and payable by Seller to Duke Energy within ten (10) days after written demand by Duke Energy. In addition to its other rights and remedies, Duke Energy shall have the right to offset the amount of any unpaid Delay Liquidated Damages plus interest against any amounts due or that may become due Seller under the Agreement.

SECTION 7: CONTRACT PRICE; INVOICES AND PAYMENT

7.1 Contract Price. Duke Energy shall pay Seller the contract price set forth on the face of the applicable Purchase Order (the "**Contract Price**") in the manner described therein. Except as set forth in Section 22 (Taxes), the Contract Price includes all amounts necessary to compensate Seller for the Goods and Services. Subject to Section 10 (Force Majeure), Seller shall not be entitled to an increase in the Contract Price or any other compensation, reimbursement of expenses or additional payment of any kind without prior written authorization of Duke Energy or as otherwise specifically set forth in the Agreement.

7.2 Invoices and Payment

(a) Invoices. All of Seller's invoices shall refer to the Agreement and contain the applicable Duke Energy Purchase Order number. If Services are being performed on a time-and-materials basis, the invoice shall include a statement or be accompanied by time sheets showing each employee's name, classification, hours worked, and the applicable rate of compensation to Seller. If any equipment has been used for which a charge applies, the invoice must also specify the equipment used, hours of usage and rate of reimbursement for use. Any tax paid on material or equipment must be shown separately from the sale or rental price of those items. Any prompt payment discount Seller offers Duke Energy shall be

determined using the date Duke Energy receives a correct invoice. Seller shall submit a final invoice for payment to Duke Energy no more than sixty (60) days after the later of Final Acceptance (defined below) of the Services or of the Goods, as applicable.

(b) Payments; Withholding. Upon submission of proper invoices and supporting documentation, Duke Energy shall pay Seller the price due and owing for Services performed or Goods received on a net ninety (90) day basis. Duke Energy may withhold from any payment amounts incorrectly invoiced, amounts in dispute, or an amount sufficient to reasonably protect Duke Energy from loss, damage or expense arising out of assertions by other parties of any claim or lien against Duke Energy arising in connection with the Agreement.

7.3 No Additional Charges; Packaging. The prices specified in the applicable Purchase Order are the total prices of the Goods and Services to Duke Energy, and Duke Energy shall not be responsible for any other charges, fees, taxes or expenses, including sales taxes unless otherwise expressly agreed in said Purchase Order. No separate charge shall be made for cartons, wrapping, packaging, boxing, crating, drayage or other packaging or loading costs unless authorized on the face of the applicable Purchase Order. All Goods shall be suitably packed or otherwise prepared for shipment, so as to secure the lowest transportation and insurance rates and to meet the carrier's requirements. All shipments shall be declared at full valuation to insure full coverage. Packing lists must accompany each shipment.

SECTION 8: PERFORMANCE STATUS REVIEWS AND IMPROVEMENT PLANS

8.1 Management Review Meetings. At any time and from time to time, Duke Energy may request to have a Management Review Meeting ("**MRM**") with Seller. Seller shall send qualified management representatives to the MRM and, at Duke Energy's request, Seller shall provide the following minimum information for the MRM discussion: (a) environmental, health, security, or safety events, which includes OSHA Recordable injuries and illnesses, fatalities and significant injuries (with respect to Seller's work for Duke Energy or Seller's work for other parties), OSHA Total Incident Case Rate ("**TICR**") at Seller's corporate level, preventable vehicle incidents, and environmental events (with respect to Seller's work for Duke Energy), (b) reliability and quality, which includes rework events, and unplanned system disruptions and outages, (c) schedule performance, and/or (d) cost performance.

8.2 Performance Improvement Plans. Seller may have the opportunity to, or may be required by Duke Energy to, improve or to remediate its performance at Seller's own cost to the satisfaction of Duke Energy under a performance improvement plan approved by Duke Energy, developed at Duke Energy's request without delay by the Seller at Seller's own cost, and reviewed and accepted in a reasonably timely manner by Duke Energy. Seller shall submit a performance improvement plan to Duke Energy for review and approval at Seller's own cost within five (5) days of any such order from Duke Energy. Seller's failure to improve or to remediate its performance to the satisfaction of Duke Energy may negatively affect Duke Energy's allocation of future work to Seller.

8.3 Reservation of Rights. Notwithstanding any provision in this Section 8, any MRMs, or any performance improvement plans, Duke Energy shall retain all rights and remedies with respect to Seller's performance under the Agreement, including but not limited to suspension and termination.

SECTION 9: CHANGE ORDERS; CHANGES IN SERVICES AND GOODS

Duke Energy may order changes in the Services or Goods from time to time consisting of additions, deletions, or other revisions (a "**Change**"). Seller may not order Changes, but if Seller believes that due to changed circumstances which do not arise as a result of an act or omission of Seller a Change is required, it may request that Duke Energy issue a Change. A "**Change Order**" is a written instrument issued by Duke Energy reflecting the Parties' mutual agreement upon all of the following: (a) a change in the Services or Goods, if any; (b) the amount of the adjustment in the Contract Price, if any; and/or (c) the extent of the adjustment, if any, to the Schedule, including to any Guaranteed Delivery Dates. If Seller's Contract Price or Schedule will be affected by a Change, Seller must submit a request for a Change Order, and Duke Energy must approve such Change in writing through the issuance of a Change Order prior to Seller starting the changed Services or Goods. Additionally, in the event the Parties are unable to agree to the terms of the Change Order, or in the event of an emergency, Duke Energy may, at any time, provide Seller with a written change directive (a "**Directive Change Order**") to make changes in, additions to and omissions from the Services or the Schedule, and Seller shall promptly proceed with the performance of Services so changed. Claims for additional compensation or time for performance must be itemized and supported with adequate documentation. Services performed outside the scope or Schedule set forth in the Agreement which are not requested by a Change Order or Directive Change Order may not form the basis of a claim for additional compensation or time. If an omission or a reduction in scope is made from the Services or Goods, any decrease in the Contract Price shall be agreed to by both Parties.

SECTION 10: FORCE MAJEURE

10.1 Definition. "**Force Majeure**" shall mean: (a) war, riots, insurrection, rebellion, floods, hurricanes, tornadoes, earthquakes, extreme and unanticipated weather conditions, pandemic, epidemic and other natural calamities; (b) acts or inaction of any government authority which directly impact the critical path of the Services; (c) explosions or fires arising from lightning or other natural causes unrelated to acts or omissions of the Party; or (d) delays in obtaining goods or services from any subcontractor caused solely by the occurrence of any of the events described in the immediately preceding subparts (a) through (c). Such acts, events or conditions listed in (a) through (d) above shall only be deemed a Force Majeure event to the extent they: (i) directly impact the critical path of the Services and are beyond the reasonable control of the Party claiming a delay, (ii) are not the result of the willful misconduct or negligent act or omission of such Party claiming a delay (or any person over whom that Party has control), (iii) are not an act, event or condition, the risk or consequence of which such Party has expressly assumed under the Agreement, and (iv) cannot be cured, remedied, avoided, offset, or otherwise overcome by the prompt exercise of reasonable diligence by such Party (or any person over whom such Party has control).

10.2 Effect of Force Majeure Event. Any delays in performance by Duke Energy or Seller shall not constitute a default under the Agreement if and to the extent such delays of performance are caused by a Force Majeure event. The scheduled final completion or final delivery date shall be adjusted by Change Order to account for any delay caused by a Force Majeure event. The affected Party shall exercise all reasonable efforts to overcome and mitigate the effects of any Force Majeure event at its own cost. If a Party believes it will experience a delay in performance of its obligations hereunder due to a Force Majeure event, it shall notify the other party in writing within five (5) days after becoming aware of such delay.

SECTION 11: SELLER'S WARRANTIES

11.1 Warranty Applicable to the Purchase of Goods. To the extent Seller provides any Goods to Duke Energy, the provisions of this Section 11.1 apply to the Agreement. Seller represents and warrants that: (a) Seller shall deliver good, exclusive and marketable title to the Goods free and clear of all liens, security interests, claims, and encumbrances; (b) the Goods shall be new, fit for their intended purpose and operate as intended, merchantable, free from defects in design, materials and workmanship and shall comply with all final written descriptions, specifications, drawings and representations, including those specified in the Agreement and shall not infringe or misappropriate any third party's intellectual property rights; (c) except as authorized by Duke Energy in writing, all Goods and materials furnished, delivered or installed by Seller shall contain no asbestos, and (d) no Legal Requirements will be violated in manufacturing, selling or delivering of the Goods. Seller shall promptly repair or replace, at Duke Energy's election, all Goods that do not comply with the warranty set forth in this Section 11.1. If Duke Energy gives Seller notice of noncompliance with this Section 11.1, Seller shall, at its own cost and expense, within thirty (30) days of such notice, replace or repair the defective or nonconforming Goods and pay for all related expenses, including, but not limited to, removal costs, restocking fees, transportation charges for the return of the defective or nonconforming Goods to Seller and the delivery of repaired or replacement Goods to Duke Energy. If Seller fails to comply with its obligations in the immediately preceding sentence, or in the event of an emergency, Duke Energy shall have the right to have the defective or nonconforming Goods repaired by third parties and Seller shall, on demand, reimburse Duke Energy for all costs incurred by Duke Energy in connection with such repair.

11.2 Warranty Applicable to the Purchase of Services. To the extent Seller provides Services to Duke Energy, the provisions of this Section 11.2 apply to the Agreement. Seller represents and warrants to Duke Energy that (a) Seller shall perform the Services consistent with the Agreement, in a professional, good and workmanlike manner, and in accordance with the standards of care, thoroughness and competence normally practiced by

recognized firms in the industry performing Services of a similar nature, and in full compliance with all final written descriptions, specifications, drawings and representations, including those specified in the Agreement; (b) the Services shall be free from defects in design and fit for their intended purpose; (c) Seller shall employ only competent, experienced and qualified personnel to perform the Services; (d) Seller shall perform and complete the Services within the timeframes set forth in the Schedule; (e) Seller is not a party to nor subject to any agreement or order which would limit, prevent or restrict its performance of any services; and (f) no Legal Requirements will be violated in the performance of the Services. If Duke Energy gives Seller notice of noncompliance with this Section 11.2, Seller shall, at its own cost and expense, within thirty (30) days of such notice, re-perform or correct all Services that were performed incorrectly or otherwise do not comply fully with the warranty set forth in this Section 11.2, or, at Duke Energy's election and in its sole discretion, in the event Duke Energy determines that re-performance or correction is not practical, refund to Duke Energy the portion of the Contract Price paid for such Services. If Seller fails to commence and pursue corrective action as provided in this Section 11.2, or in the event of an emergency, Duke Energy may at its option correct the defective Services itself or hire others to do so and all costs to make such correction shall be paid by or back-charged to Seller.

11.3 Warranty Applicable to Software. To the extent Seller provides Software to Duke Energy in connection with the Agreement, including through the provision of Goods that contain Software, then the provisions of this Section 11.3 apply to the Agreement. Seller represents and warrants to Duke Energy that the Software shall not contain any viruses, Trojan horses, disabling code, timer, clock, counter or other limiting design or routine which causes the Software to be erased, inoperable or otherwise incapable of being used in the full manner for which it was designed and licensed pursuant to the Agreement after being used or copied a certain number of times, or after the lapse of a certain period of time, or after the occurrence or lapse of any similar triggering factor. Seller warrants that the Software shall conform to and perform in accordance with all applicable Software descriptions and specifications and if Duke Energy gives Seller notice of noncompliance with this Section 11.3, Seller shall deliver to Duke Energy within thirty (30) days of such notice, at no cost all fixes, corrections, and patches for errors and bugs to the Software, including without limitation those relating to program code and documentation. If Seller is unable to correct any errors or bugs, Seller shall promptly replace such Software without charge. All replacement Software must comply with the requirements of this warranty provision.

SECTION 12: ACCEPTANCE AND INSPECTION

12.1 Duke Energy Right to Inspection. Duke Energy shall have the right to inspect the Goods or Services before accepting them, shall have free access to the Services and Goods for inspection purposes, and shall have a reasonable period of time after discovering a defect or nonconformity to reject or revoke acceptance of the Goods or Services. Duke Energy shall have the right to place one or more inspectors in Seller's facilities at any time to inspect the Goods or Services and the manufacturing and assembling process for the Goods and to inspect and copy all quality assurance and other records relating to the Goods at no cost to Duke Energy. All Goods or Services are also subject to inspection after receipt at Duke Energy's location before Final Acceptance.

12.2 Rejection by Duke Energy. Duke Energy's inspection or acceptance of the Services or Goods shall not relieve Seller of its obligation to comply with the terms of the Agreement. Duke Energy may reject non-conforming Services or Goods, and Seller shall correct such non-conformity at Seller's expense. If Duke Energy rejects the Goods or Services or revokes its acceptance of the Goods or Services, and Seller does not deliver conforming Goods or Services on or before the final delivery date or final completion date, as applicable, specified in the applicable Purchase Order, Duke Energy shall have the right, at Duke Energy's election and without waiving any of its remedies at law it is otherwise entitled to, to terminate all or a portion of said Purchase Order in accordance with Section 20.3(a) and obtain a prompt refund from Seller of all payments Duke Energy has made with respect to that portion of the Purchase Order which Duke Energy has terminated. Seller shall pay all costs Duke Energy incurs in returning the rejected Goods or correcting defective Services.

12.3 Final Acceptance. Duke Energy will provide its final acceptance of all Services or/and Goods outlined in each applicable Purchase Order when Duke Energy determines in its reasonable discretion that such Services have achieved final completion and/or that the final delivery of such Goods has been completed in accordance with the Agreement, including with the specifications outlined in the Purchase Order and including that any and all defects or nonconformities have been fully corrected or otherwise remedied by Seller to Duke Energy's satisfaction ("**Final Acceptance**").

SECTION 13: INDEMNIFICATION

To the maximum extent permitted by law, Seller shall indemnify, defend (with counsel acceptable to Duke Energy) and hold harmless Duke Energy (including its parent, subsidiary and affiliate companies), Duke Energy's other contractors and suppliers, their respective officers, employees, agents, consultants, partners, members and directors, and any third party with an ownership interest in the premises (the "**Duke Energy Indemnitees**") from and against all liability, loss, costs, including reasonable attorneys' fees, claims, damages, expenses, judgments, and awards, whether or not covered by insurance, arising or claimed to have arisen in whole or in part:

(a) as a result of negligence by Seller, its subcontractors, materialmen, or assignees and their agents or employees, which resulted in: (i) injury (including mental or emotional) to or death of any person, including employees of Duke Energy (including its parent, subsidiary and affiliate companies) or (ii) damage to or destruction of any property, real or personal, including without limitation property of the Duke Energy Indemnitees;

(b) from demands, actions or disputes asserted by any subcontractors, employees or suppliers of Seller;

(c) from any claim that the Goods or Services or Duke Energy's use of the Goods or Services infringes any patent, copyright, trademark, trade name, service mark or other property right;

(d) from any failure of Seller or its subcontractors to comply with all applicable Legal Requirements;

(e) from all third party claims due to Seller's breach of the Purchase Order; and

(f) from any breach of, act or omission related to, or failure of Seller to comply with, the terms and obligations set forth under Section 16 (Confidential Information; Trademarks; Publicity) or the Network Security Supplement attached hereto as Attachment C.

In the case of a claim that the Goods or Services are infringing, Seller shall have the right, at its sole expense, to obtain for Duke Energy the right to continue using the Goods or Services without interference or to modify or replace the Goods or Services in a manner acceptable to Duke Energy in its sole discretion. Duke Energy shall give Seller reasonable notice of any claim Duke Energy contends falls within the indemnification obligations of this Section 13. Seller waives all rights of recovery, including for contribution, against the Duke Energy Indemnitees for any matters to which this Section 13 may apply.

SECTION 14: INSURANCE

14.1 Coverage and Limits. Commencing with Seller's performance under the Agreement, and continuing until the termination or later expiration of the Agreement, including during the performance of any warranty services, Seller (and any tier subcontractors) shall maintain or cause to be maintained occurrence form insurance policies as follows:

(a) Workers' Compensation specific to the applicable statutory requirements for the Services to be performed; provided that Seller (or its subcontractor(s)) must notify Duke Energy if it is exempt from the statutory Workers' Compensation requirements;

(b) Employer's Liability Insurance of not less than $1,000,000.00 each accident/employee/disease;

(c) Commercial or Comprehensive General Liability Insurance having an available limit of at least $1,000,000.00 per occurrence/$2,000,000.00 in the annual aggregate for contractual liability, personal injury, bodily injury to or death of persons, and/or loss of use or damage to property, including but not limited to products and completed operations liability (which shall continue for at least three (3) years after completion), premises and operations liability, explosion, collapse, and underground hazard, and, if the Services will be performed within fifty feet of a railroad, contractual liability - railroads coverage;

(d) Commercial/Business Automobile Liability Insurance (including owned (if any), non-owned or hired autos) having an available

limit of at least $1,000,000.00 each accident for bodily injury, death, property damage and contractual liability and no fellow employee exclusion;

(e) Umbrella/Excess Liability Insurance with available limits of at least $4,000,000.00 per occurrence and follow form of the underlying Employer's Commercial General and Auto Liability insurance, and providing at least the same scope of coverages thereunder;

(f) E&O. If engineering, consulting, design, or other professional services are to be performed under the Agreement, Professional Liability/Errors & Omissions ("**E&O**") Insurance (claims-made form acceptable with reporting requirements of at least three (3) years after completion) with no resulting bodily injury or property damage exclusion with available limits of at least $1,000,000.00 each claim. Such policy shall not contain a cyber incident exclusion for any vendor that has access to Duke Energy's IT network;

(g) Inland Marine Transit and/or Ocean Cargo and/or Installation Floater. If providing equipment to be transferred to Duke Energy's ownership under the Agreement, inland marine transit and/or ocean cargo and/or installation floater for the replacement cost value of such items for physical loss or damage during transit, loading/unloading, conducting services and/or installation;

(h) Cyber Risk/Privacy Data Protection Liability Insurance. If accessing Duke Energy Confidential Information, Duke Energy PII, Critical Cyber Systems or having Remote Access, Cyber Risk/Privacy Data protection liability insurance covering claims arising from breaches of security; violation or infringement of any right privacy, breach of federal, state, or foreign security and/or privacy laws or regulations; data theft, damage, destruction, or corruption, including without limitation, unauthorized access, unauthorized use, identity theft, theft, or inadvertent disclosure of Duke Energy Confidential Information, Duke Energy PII, transmission of a computer virus or other type of malicious code information security or data breaches, or misappropriation of data; with available limits of at least $1,000,000.00 each occurrence and in the aggregate; and

(i) Aviation Liability Insurance / UAS-Specific Insurance. If the Services to be provided by Seller include the operation of an aircraft of any type, including without limitation an unmanned aircraft system, (x) Aviation Liability Insurance with a minimum limit of $10,000,000.00 each accident for bodily injury, death, property damage, and contractual liability (or, in the case of the operation of an unmanned aircraft system ("**UAS**"), such UAS-specific insurance as is comparable to the Aviation Liability Insurance coverage described herein, in form and substance acceptable to Duke Energy in its sole and absolute discretion) and (y) if such operation is being undertaken for the purpose of chemical application, $1,000,000 in Chemical Liability. In such instance, Seller must confirm with Duke Energy that chemicals being sprayed are covered under Seller's Chemical Liability Policy and provide a certificate of insurance evidencing this coverage acceptable to both Insurance and Aviation Services. The certificate must confirm the type of chemical coverage (Comprehensive Chemical or Restricted Chemical) Seller has before Seller may commence performance of any Services under the Agreement.

14.2 Insurance Requirements. In addition to meeting the requirements established in Section 14.1, all insurance policies provided and maintained by Seller and each subcontractor shall: (i) be underwritten by insurers acceptable to Duke Energy which are rated A.M. Best "A- VII" or higher; (ii) specifically include Duke Energy and its directors, officers, employees, affiliates, subcontractors, and joint owners of any facilities as additional insureds, including for ongoing and completed operations, with respect to Seller's or its subcontractors' acts, omissions, services, products or operations, whether in whole or in part, excluding, however, for Worker's Compensation/Employer's Liability and if applicable, those coverages set forth in Sections (f) through (i) above; (iii) be endorsed to provide, where permitted by law, waiver of any rights of subrogation against Duke Energy and its directors, officers, employees, affiliates and subcontractors, and joint owners of any facilities; (iv) provide that such policies and additional insured provisions are primary with respect to the acts, omissions, services, products or operations of Seller or its subcontractors, whether in whole or in part, and without right of contribution from any other insurance, self-insurance or coverage available to Duke Energy and its affiliates; and (v) contain a standard cross liability clause and separation of insured and severability of interest provisions except with respect to the limits of the insurer's liability. Any deductibles or retentions shall be the sole responsibility of Seller and its subcontractors. The limits of insurance required under the Agreement are minimums. All insurance policies shall provide that the insurer will provide at least thirty (30) days' written notice to Seller, and Seller, in turn, shall provide at least thirty (30) days' written notice to Duke Energy prior to cancellation or non-renewal of any policy (or ten (10) days' prior notice in the case of non-payment of premium).

14.3 Evidence of Insurance; Compliance

(a) Evidence of the insurance coverage required under the Agreement shall be provided via Seller's certificate of insurance furnished to Duke Energy prior to the start of Services, upon any policy replacement or renewal and upon Duke Energy's request. If there is a Dispute or an insurance claim related to the Services or Goods under the Agreement, Seller or its applicable subcontractors shall, upon Duke Energy's request, provide a copy of any or all of Seller's required insurance policies, including endorsements in which Duke Energy is included as an additional insured.

(b) Seller's compliance with these provisions and the limits of insurance specified herein shall not constitute a limitation of Seller's liability or otherwise affect Seller's indemnification obligations pursuant to the Agreement. Any failure by Seller to comply with any of the provisions of this Section 14 shall permit Duke Energy to suspend all Services until compliance is achieved to Duke Energy's reasonable satisfaction. The failure by Seller to provide any or accurate certificates of insurance, or by Duke Energy to insist upon any or accurate certificates of insurance, shall not be deemed a waiver of any rights of Duke Energy under the Agreement or with respect to any insurance coverage required under the Agreement.

SECTION 15: SAFETY, HEALTH, AND ENVIRONMENTAL PROTECTION

15.1 Site Safety and Security

(a) All Services performed by Seller or its subcontractors on Duke Energy's premises, and the design of all equipment and systems brought onto Duke Energy's premises, shall comply fully with Duke Energy's environmental, safety and security procedures, policies and regulations, inclusive of: (i) Duke Energy's Environmental, Health and Safety (EHS) Handbook located at https://www.duke-energy.com/partner-with-us/suppliers/ehs-orientation-training, which includes Duke Energy Business Unit EHS Supplemental Requirements; and (ii) Duke Energy's Safety and Security procedures - all when such documents are provided or made available by Duke Energy and all as amended, restated, or supplemented from time to time. At any time and from time to time, Duke Energy reserves the right to conduct an audit of OSHA compliance, including but not limited to the verification of training to OSHA vertical standards and the qualification of oversight personnel provided by the Seller. Duke Energy reserves the right to require the Seller to provide safety oversight of its work if Duke Energy deems the Seller's safety oversight to be insufficient. In addition, Seller must follow detailed technical safety specifications when they are provided.

(b) Seller shall not, and shall not permit any worker, employee, or other third party to bring any firearm of any type or other weapon of any type upon any property owned or controlled by Duke Energy. Further, Seller shall not permit or tolerate the introduction or use of intoxicating liquor, narcotic drugs, gambling, drug paraphernalia, or gambling paraphernalia at any Duke Energy site or during the performance of any Services. Any employee, independent contractor, or agent of Seller found engaging in such activities shall be removed and permanently barred from Duke Energy property, including any and all Duke Energy sites.

(c) If Seller employs non-English speaking persons, Seller shall ensure that a bilingual person fluent in speaking, reading and writing both English and the applicable non-English language is available at the jobsite where the non-English speaking person(s) are working for purposes of safety and hazard related communications, communicating technical information, emergency response, and similar issues. Seller shall further ensure that all written and verbal safety training, hazard communications, and work rules are provided in the appropriate language for such non-English speaking employees or persons.

15.2 Qualifications; Minimum Screening Guidelines; Drug Policy

(a) For any Services performed at a Duke Energy site or Duke Energy customer site and/or requiring access to Duke Energy assets, Seller and its subcontractors shall participate in E-Verify, perform all required employment eligibility and verification checks, and cooperate with the scope, timing, documentation, etc., of audits requested by Duke Energy, which shall be performed by a third-party immigration attorney selected by Duke Energy. Seller shall maintain all required employment records for at least three years following an employee's date of hire or one year following an employee's termination.

(b) By providing an employee or subcontractor under the Agreement to perform Services at a Duke Energy site, a Duke Energy customer site and/or requiring access to Duke Energy assets, Seller warrants and represents that the Minimum Screening Guidelines (as set forth at https://www.duke-energy.com// /media/pdfs/external/minimum-screening-guidelines-nov2020.pdf) have been completed with respect to such employee or subcontractor and that they did not reveal any information that could adversely affect such employee's or subcontractor's suitability for employment by Seller or competence or ability to perform duties under the Agreement following an individualized assessment of the specific facts and circumstances and consideration of Duke Energy's Potential Disqualification Criteria, which are set forth at https://www.duke-energy.com// /media/pdfs/external/potential-disqualification-criteria-nov2020.pdf. Generally, Duke Energy will rely on Seller to make a determination as to whether to disqualify a candidate based on the Potential Disqualification Criteria. However, if there is a question as to a candidate's qualifications, Seller may seek additional input from Duke Energy. Seller may also perform other screening measures as a reasonably prudent employer would deem appropriate; provided, however, that nothing in this Section shall be interpreted as authorizing or requiring Seller to perform any screening measures or disqualify any worker in a manner that violates the federal Fair Credit Reporting Act, Title VII of the Civil Rights Act of 1964 or any other applicable law. Seller agrees to use additional screening measures that may be required by Duke Energy based upon audit results to ensure Seller's compliance with this Section. Except where prohibited by law, should Seller learn after assigning an individual to provide Services at a Duke Energy site or requiring access to the Duke Energy assets that Seller, acting reasonably, considers would adversely affect such personnel's suitability for performance of the Services, Seller will promptly advise Duke Energy and remove the individual immediately from performing Services at a Duke Energy site or on the Duke Energy assets. Duke Energy, in its sole discretion, shall have the option of barring from the Site any person whom Duke Energy determines does not meet the qualification requirements set forth above.

(c) Seller acknowledges that it is aware of Duke Energy's Alcohol and Drug Policy ("Policy") located under Contractor Training Materials at http://www.duke-energy.com/suppliers/contractor-training.asp as revised or updated by Duke Energy from time to time. Seller and its subcontractors shall implement and administer an alcohol/drug abuse policy acceptable to Duke Energy and at least as stringent as that of Duke Energy and further acknowledges that any employee, contractor or subcontractor of Seller performing Services under the Agreement shall be subject to referral for "for cause" testing on the basis of reasonable suspicion observed by Duke Energy. Duke Energy does not perform or adjudicate alcohol/drug tests for contract workers. Duke Energy may, at its sole discretion, upon notice to Seller, audit Seller's substance abuse testing records relating to the Services. Duke Energy encourages Seller to offer employee assistance to all employees who test positive and to have employees visit a Substance Abuse Program (SAP).

(d) For any Services to be performed by Seller at Duke Energy Fossil/Hydroelectric generation properties for Regulated & Renewable Energy, participating Renewable Regulated Generation sites, Coal Combustion Products department sites, and Project Management & Construction department sites within Duke Energy Indiana, Duke Energy Ohio, Duke Energy Kentucky, Duke Energy Carolinas, Duke Energy Progress, Duke Energy Florida, and Piedmont Natural Gas Company, Inc. Seller's drug and alcohol policies and procedures shall meet the requirements set forth in Attachment B.

15.3 Hazardous Materials Management and Environmental Requirements

(a) At least two (2) weeks before any Services are performed on Duke Energy's premises or at any Duke Energy project site, Seller shall deliver to Duke Energy's designated point of contact and the project site: (i) a copy of Seller's hazard communication program; (ii) a list of all hazardous chemicals and other substances Seller proposes to bring onto Duke Energy's premises or onto the Duke Energy project site, if any, and the quantities of each; and (iii) safety data sheets for each chemical and substance on the list. Seller shall not use, apply, store, construct, or otherwise introduce on a Duke Energy site any materials that contain methylene chloride, asbestos, or hexavalent chromium. For primers or coatings suspected of containing lead, Seller shall ensure the lead content of such products or materials is no more than the current Consumer Product Safety Commission threshold. Seller will collect and maintain safety and health data for the performance of the Services, which will include but not be limited to total hours worked, incidents, near misses, lost work days, restricted duty, recordable injuries, workers' compensation experience modifier, and any OSHA or state plan citation history. Upon request, Seller will provide this data to Duke Energy or Duke Energy's third party vendor.

(b) Any performance by Seller involving the generation, storage, handling, packaging, marking, labeling, transportation, or disposal of materials, substances, or wastes that may be hazardous, and any work in an area defined as a confined space shall be in accordance with any and all Legal Requirements.

15.4 Cleanliness Control and Foreign Material Exclusion (Power Generation Facilities). If Seller is supplying materials, parts, equipment, or components to be installed in power generation facilities or if Seller is providing equipment repair/refurbishment services relating to a power generation facility, then the provisions of this Section 15.4 apply to the Agreement.

(a) Cleanliness Control/Foreign Material Exclusion Practices. Seller acknowledges and agrees that the Goods or Services to be supplied by Seller under the Agreement that are subject to this Section 15.4 are important to the operation of a power plant facility. The Seller shall establish "**Cleanliness Control/Foreign Material Exclusion Practices**" including but not limited to those described in this Section 15.4 to ensure that new, repaired or refurbished parts and equipment delivered under the Agreement are free from dirt, soil, mill scale, weldsplatter, oil, grease, stains, broken or lose parts, contaminants, or other foreign material that may be detrimental to the operation of the equipment or interfacing equipment and systems of Duke Energy. Other examples of foreign material include loose fasteners, debris resulting from machining or other manufacturing processes, and tags or labels used in the manufacturing process that are not permanently affixed to internals.

(b) Inspection and Precaution. Prior to shipment, Seller shall inspect the parts and equipment to ensure that no foreign materials or detrimental contaminants are present, including internal surfaces and cavities of the equipment. Additional measures shall be taken by the Seller to prevent foreign material from entering the equipment, including protective caps, plugs, or covers in or over such openings. Precautions shall also be taken to ensure foreign material is not introduced during packaging and shipping. If the equipment is shipped with other parts (such as seals, gaskets, lubricants, mounting hardware), precautions shall be taken to ensure smaller items cannot be introduced into openings or cavities of larger parts and equipment. The packing list shall clearly identify every item included with the shipment. If desiccants or other preservatives are used to protect the item(s), the affected part or 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.

SECTION 16: CONFIDENTIAL INFORMATION; TRADEMARKS; PUBLICITY

(a) Definition. Each Party agrees that any (A) Personally Identifiable Information (as defined below), (B) non-public or proprietary information relating to the other Party's business, including but not limited to, technical, financial, administrative and internal activities or any business plans and methods, operating and technical data, drawings, and reports, (C) data specific to each Party's customer or group of customers, including, with respect to Duke Energy, any information that is or has been obtained or compiled by Duke Energy in connection with supplying electric services or gas services to such customers, and (D) any and all other data or information written, oral, or other media form that is: (i) disclosed at any time to either Party in connection with or incidental to the Services contemplated by the Agreement; (ii) processed at any time by either Party in connection with or incidental to the Services contemplated by the Agreement; (iii) derived by either Party from the information described in (i) or (ii) above; or (iv) marked "Restricted", "Confidential", "Proprietary" or contains a similar marking is considered confidential and proprietary information (categories (i) – (iv) in this Section 16(a) are collectively referred to as **"Confidential Information"**). **"Personally Identifiable Information" ("PII")** means that portion of Confidential Information relating to an identified or identifiable individual, and the collection, use, or disclosure of which is governed by applicable law or regulation. PII includes, but is not limited to, name; likeness; physical location; postal or service address; email address or other online contact information (such as an online user ID); telephone number; date of birth; Social Security number (or its equivalent); driver's license number (or other government or regulator-issued identification numbers or information); account information (including but not limited to utility account information and identifiers that would permit access to an individual's financial, insurance policy, stock, or other security account information); payment card data (including, but not limited to, primary account information such as card number, expiration date, security

code, full magnetic stripe data or equivalent on a chip, or PIN); access code, password, security questions and answers; medical information; health insurance information; biometric data; fingerprints; digital signatures; Internet Protocol (IP) address; or any other unique identifier.

(b) Definition Exclusions. Except with respect to PII, "Confidential Information" shall not include any information that: (i) was already known to the receiving Party at the time it was disclosed by the disclosing Party; (ii) was available to the public at the time it was disclosed by the disclosing Party; (iii) becomes available to the public after being disclosed by the disclosing Party through no wrongful act of, or breach of the Agreement by the receiving Party; (iv) is received by the receiving Party without restriction as to use or disclosure from a third party; or (v) is independently developed by the receiving Party without benefit of any disclosure of information by the disclosing Party. For the avoidance of doubt, PII is considered Confidential Information and the terms of the Agreement (including those in this Section 16) apply to such information regardless of (i) – (v) above.

(c) Disclosure and Use Restrictions. Each Party agrees that it shall not use (except for the purpose described herein), share, transfer, disclose, publish, or otherwise provide the Confidential Information of the other Party to any third party (including affiliates and subcontractors) for any reason unless approved in writing by the disclosing Party. Duke Energy shall not disclose, nor approve the disclosure of, any proprietary customer information without the prior consent of the applicable customer and Seller shall not disclose or transmit any PII to Duke Energy without prior written consent of Duke Energy. Each Party agrees to use Confidential Information solely for the purpose of the Agreement and shall disclose the other Party's Confidential Information only to its directors, officers, employees, advisors, contractors, consultants, suppliers, or other representatives (a "**Representative**") with a need to know such information for the performance of the Agreement and only after any such Representative understands and agrees to be bound by terms at least as restrictive as those contained in this Section. Each Party shall (i) provide its Representatives training, as appropriate, regarding the privacy, confidentiality, and information security requirements set forth in this Section 16 and as otherwise set forth in the Agreement; and (ii) exercise the necessary and appropriate supervision over its Representatives to maintain the appropriate privacy, confidentiality, and security of Confidential Information. Seller shall be responsible for, shall and remain liable to Duke Energy for, Seller's Representatives' compliance with this Section 16.

(d) Degree of Care. Each Party agrees to protect the Confidential Information of the other Party with at least the same degree of care used to protect its own confidential information.

(e) Court Order. To the extent the Parties have an existing non-disclosure or other confidentiality agreement which covers the same subject matter as the Agreement in effect as of the effective date of the Agreement, this Section shall supersede such agreement unless otherwise agreed by the Parties. If the receiving Party is requested or ordered by a court or governmental entity to disclose any or all of the Confidential Information, to the extent legally permissible, the receiving Party shall (i) promptly notify the disclosing Party of the existence, terms, and circumstances surrounding the request or order; (ii) consult with the disclosing Party on the advisability of taking steps to resist or narrow the request or order; (iii) cooperate with the disclosing Party in any lawful effort the disclosing Party undertakes to obtain any such relief and with any efforts to obtain reliable assurance that confidential treatment will be given to that portion of Confidential Information that is disclosed; and (iv) furnish only the minimal portions of Confidential Information as the receiving Party is advised by counsel is legally required to be disclosed, unless the disclosing Party expressly authorizes broader disclosure in writing.

(f) Storage and Encryption of Duke Energy Confidential Information and Duke Energy PII. Seller shall store all Duke Energy Confidential Information and PII in accordance with the Network Security Supplement.

(g) Return of Confidential Information. Promptly upon the expiration or earlier termination of the Agreement, or such earlier time as Duke Energy requests in writing, Seller will return to Duke Energy or its designee, or render unreadable or undecipherable if return is not reasonably feasible or desirable to Duke Energy (which decision will be at Duke Energy's sole discretion), each and every original and copy in every media of all Duke Energy Confidential Information in Seller's possession, custody, or control including all information and materials that contain or are derived from Duke Energy Confidential Information ("Data Return Requirements"), unless Seller is required to keep copies of such Duke Energy Confidential Information by law, and then only to the extent necessary for compliance. For electronically stored information to render such media unreadable or undecipherable, Seller shall use Cryptographic Erasure of the device or Crypto shredding of all encryption keys. To the extent Seller is required to keep copies of Duke Energy Confidential Information by law, Seller shall provide Duke Energy with a written, detailed inventory of such information and a citation to the applicable law for each such item, in advance of keeping such copies. Promptly following any return or alternate action taken to comply with the Data Return Requirements, Seller will provide to Duke Energy a written certification from one of Seller's officers certifying that such return or alternate action occurred.

(h) Compliance with Privacy Laws. Seller shall comply, and shall require its subcontractors to comply, with (i) all applicable international, federal, state, provincial, and local laws, rules, regulations, directives and governmental requirements currently in effect and as they become effective relating in any way to the privacy, confidentiality, or security of Confidential Information ("Privacy Laws"); (ii) all applicable industry standards concerning privacy, confidentiality, or information security including, without limitation, the ISO/IEC 27001 and ISO/IEC 27002 Standards, the National Institute of Standards and Technology ("NIST") Framework for Improving Critical Infrastructure Cybersecurity and the Payment Card Industry Data Security Standard ("PCI DSS"); and (iii) applicable provisions of Duke Energy's written requirements currently in effect and as they become effective relating in any way to the privacy, confidentiality, or security of Confidential Information, or applicable privacy policies, statements, or notices that are provided to Seller by Duke Energy in writing.

(i) Injunctive Relief. Seller agrees that any use, disclosure, or handling of Confidential Information in violation of this Section 16 (including a Security Event as defined in Attachment C hereto) may cause immediate and irreparable harm to Duke Energy and Duke Energy shall be entitled to equitable relief, including an injunction and specific performance, in addition to all other remedies available at law or equity. Therefore, Seller agrees that Duke Energy may obtain specific performance and injunctive or other equitable relief for any such violation, in addition to its remedies at law, without proof of actual damages and without the necessity of securing or posting any bond in connection with such remedy.

(j) Duke Energy Name and Logo; No Publication; Web Content Accessibility. Seller shall not use Duke Energy's (including Duke Energy's parent, affiliates and/or subsidiaries) name or the fact that Seller is performing Services for Duke Energy in any press releases, media statements, or public communications or otherwise publicize the Agreement without Duke Energy's prior written consent, which shall be at Duke Energy's sole discretion. Seller shall not use Duke Energy's (including Duke Energy's parent, affiliates and/or subsidiaries) name, logos, copyrights, trademarks, service marks, trade names, or trade secrets in any way without Duke Energy's prior written consent, which shall be at Duke Energy's sole discretion; and Duke Energy shall not be deemed to have granted Seller a license of, or granted Seller any rights in, any of the foregoing by entering into the Agreement. Additionally, Seller agrees to cooperate with Duke Energy in maintaining good community relations. Duke Energy will issue all public statements, press releases, and similar publicity concerning any Services, its progress, completion, and characteristics. Seller shall not make or assist anyone to make any such statements, releases, photographs, or publicity without prior written approval of Duke Energy. If applicable to Seller's performance of Services under the Agreement, Seller represents and warrants that all Services have been completed in adherence to Duke Energy's web accessibility guidelines which are set forth at https://www.duke-energy.com/customer-service/accessibility.

SECTION 17: NETWORK SECURITY

To the extent that:

(a) Duke Energy provides Seller access to (i) an external network to access the internet while Seller works on-premises at a Duke Energy facility or (ii) Duke Energy's internal network, whether remotely or while Seller works on-premises at a Duke Energy facility;

(b) Seller provides Goods that contain Software that (i) has access to, processes, or stores Duke Energy Confidential Information or (ii) is executed or installed on any device connected to a Duke Energy computer, information system, or network;

(c) Seller provides Services that (i) support or maintain such Software referenced above or (ii) connect to a Duke Energy information system or network; or

(d) Seller requires or is be permitted cyber access or unescorted physical access to Duke Energy's assets,

then Seller shall comply with the Network Security Supplement.

SECTION 18: SOFTWARE LICENSE TERMS

For any of Seller's Goods that contain software, firmware, opensource, or source code ("**Software**"), Seller hereby grants to Duke Energy an irrevocable, non-exclusive, perpetual, worldwide right and license to use and reproduce the Software, data and other documentation provided by Seller to Duke Energy. Seller represents and warrants that it owns all ownership rights, title, and interest (including without limitation all copyright, patent, trade secret, and other intellectual property rights) to the Software sufficient to provide the preceding grant. Seller shall retain all ownership rights, title, and interest (including without limitation all copyright, patent, trade secret, and other intellectual property rights) to the Software, except to the extent that the Software may incorporate any proprietary or Confidential Information (as defined in Section 16) of Duke Energy or its customers.

SECTION 19: TITLE; LIENS; RISK OF LOSS

19.1 Transfer of Title to Goods. Title to the Goods shall pass to Duke Energy upon delivery to and acceptance of the Goods at the Duke Energy site. The passage of title to Duke Energy shall not be deemed an acceptance or approval of such Goods (or the Services to be performed in connection therewith) or affect the allocation of risk of loss thereof.

19.2 Mechanics Liens. To the fullest extent permitted by law, Seller agrees that it will not assert any lien with respect to the Goods, Services, or amounts owed under the Agreement and expressly waives any right to file or cause to be filed any such lien. Seller, in its subcontracts, shall require all subcontractors, to the extent permitted by law, to expressly waive the right to assert any liens against Duke Energy's property or funds and, if requested, provide Duke Energy with copies of such waivers. Seller shall immediately bond off any lien against Duke Energy and shall indemnify Duke Energy for any costs or expenses resulting from a breach of this Section 19.2. In the event that rights to a mechanic's lien are claimed upon Duke Energy's property by a subcontractor of Seller, Seller shall expeditiously obtain a bond or release of said mechanic's lien. Upon Seller's failure to expeditiously obtain said bond or release, Duke Energy may withhold payment to Seller and proceed to obtain the bond or release of the mechanic's lien and Seller shall be liable to Duke Energy for any costs and expenses, including attorneys' fees, which are incurred by Duke Energy in obtaining said bond or release.

(a) Notices; Lien Agent. Each Party shall designate a representative for the receipt of notices, which may be changed from time to time. All notices required to be given under the Agreement shall be in writing and delivered by personal delivery, email, or U.S. mail. Notices shall be effective upon receipt or such later date specified in the notice.

With respect to Qualified Projects (defined below) in the State of North Carolina, the contact information for the lien agent designated by Duke Energy is as follows:

Name:	Chicago Title Company, LLC
Physical Address:	223 S. West Street, Suite 900, Raleigh, NC 27603
Mailing Address:	223 S. West Street, Suite 900, Raleigh, NC 27603
Facsimile Number:	(913) 489-5231
E-mail Address:	support@liensnc.com

In order to facilitate the provision of prompt and accurate information regarding lien agents for projects in North Carolina, any and all requests to Duke Energy for lien agent contact information made pursuant to N.C.G.S. §44A-7, *et. seq.*, or otherwise shall be sent via e-mail to lienagentinfo@duke-energy.com. Seller covenants and agrees that it shall contractually require and cause all subcontractors, suppliers, or other persons performing any portion of the Services or providing any portion of the Goods to make all requests for lien information in accordance with this provision. For the purpose of the Agreement, a "**Qualified Project**" is a project involving the provision of Services, the Contract Price of which is in excess of $30,000, in connection with the improvement of real property.

19.3 Risk of Loss.

(a) Seller shall bear all risk of loss with respect to the Goods until Duke Energy actually receives and accepts the Goods.

(b) Whenever any property of Duke Energy is sent to Seller's premises for repair, refurbishment, or any other purpose related to Seller's provision of warranty services, title to such property shall at all times remain with Duke Energy and such property shall not be subject to any lien, security interest or other claim asserted by any creditor of Seller. Seller shall clearly mark such property to show that it is owned by Duke Energy. Seller shall bear the risk of loss or damage to such property while it is on Seller's premises and in transit between Duke Energy's premises and Seller's premises.

(c) Risk of loss or damage to the tools, materials, or equipment of Seller, all Seller's subcontractors, and their respective employees and agents shall at all times remain with those parties, and Duke Energy shall have no responsibility for any such tools, materials, or equipment.

SECTION 20: TERMINATION AND CANCELLATION; SUSPENSION

20.1 Termination and Cancellation by Duke Energy for Convenience

(a) Duke Energy may terminate the Agreement for Duke Energy's convenience for any reason or no reason and in its entirety upon thirty (30) days' written notice to Seller, in which event Duke Energy shall pay the cancellation charges set forth in Section 20.1(b).

(b) To the extent more than one Purchase Order is issued under the Agreement, Duke Energy shall have the right at any time to cancel all or a portion of such a Purchase Order by giving Seller written notice. If Duke Energy cancels all or a portion of such a Purchase Order, Duke Energy shall pay Seller reasonable cancellation charges on which the Parties agree which shall consist solely of direct costs for labor and materials for the Purchase Order expended by Seller before the cancellation. Seller shall take all reasonable actions to minimize any cancellation charges and shall provide an accurate accounting of all charges to Duke Energy at the time Seller makes a request for payment of those charges. Cancellation charges shall not include any incidental or indirect charges or expenses or any lost or anticipated profits. If the sum of Duke Energy's prior payments and deposits under a cancelled Purchase Order exceed the cancellation charges and other amounts due under such Purchase Order, Seller shall promptly refund the balance to Duke Energy.

20.2 Suspension by Duke Energy for Convenience. Duke Energy shall have the right at any time to delay the delivery date of some or all of the Goods or to suspend the performance of some or all of the Services by giving Seller written notice. If Duke Energy delays the delivery date of some or all of the Goods or suspends the performance of some or all of the Services under this Section 20.2, Duke Energy shall pay Seller reasonable delay or suspension, as applicable, charges on which the Parties agree shall consist solely of necessary increases in the direct costs of labor or materials for the Purchase Order for which Seller has not been compensated by reason of escalation. Seller shall take all reasonable actions to minimize any delay or suspension charges and shall provide an accurate accounting of all charges to Duke Energy at the time Seller makes a request for payment of those charges. Delay and suspension charges shall not include any incidental or indirect charges or expenses or any lost or anticipated profits. If the sum of Duke Energy's prior payments and deposits under the applicable Purchase Order exceed the delay or suspension charges and other amounts due under such Purchase Order, Seller shall promptly refund the balance to Duke Energy.

20.3 Default

(a) Seller Events of Default; Duke Energy Termination for Cause. If Seller defaults under any term of the Agreement and does not cure that default within fifteen (15) days after Duke Energy gives Seller written notice of default, Duke Energy shall be entitled: (i) to suspend its performance under the Agreement (or, if more than one Purchase Order is issued under the Agreement, then, at Duke Energy's option, suspend its performance under the applicable Purchase Order); (ii) to terminate the Agreement (or, if more than one Purchase Order is issued under the Agreement, then, at Duke Energy's option, cancel the applicable Purchase Order and have no further obligation to Seller thereunder) and have no further obligation to Seller; (iii) to declare all or part of Seller's obligations to Duke Energy under the Agreement (or, if more than one Purchase Order is issued under the Agreement, then, at Duke Energy's option, under the

applicable Purchase Order) immediately due and payable; and (iv) to pursue any other right or remedy Duke Energy may have. Duke Energy shall be entitled to set off all of its losses, costs and damages against all amounts Duke Energy owes Seller.

(b) Duke Energy Events of Default; Seller Termination for Cause. Duke Energy shall be in default of its obligations pursuant to the Agreement if within thirty (30) days after Duke Energy's receipt of written notice from Seller that the following amount is past due Duke Energy fails to pay or cause to be paid any verifiable amount that (i) is not subject to a good faith dispute and (ii) has become due and payable by it to Seller under the Agreement (a "**Duke Energy Default**"). In the event of a Duke Energy Default, if Duke Energy has not cured that Duke Energy Default within the thirty (30) day notice period, Seller shall be entitled, subject to the limitations on Duke Energy's liability set forth in Section 23.7: (a) to terminate the Agreement or suspend performance under the Agreement (or, if more than one Purchase Order is issued under the Agreement, then terminate or suspend its performance under the applicable Purchase Order) immediately by delivery of written notice thereof to Duke Energy, and such termination or suspension shall be deemed as if done for convenience of Duke Energy under Section 20.1 or 20.2 (as applicable); (b) to seek equitable relief, including specific performance and injunctive relief, to cause Duke Energy to take action, or to refrain from taking action, pursuant to the Agreement, or to make restitution of amounts improperly retained or received under the Agreement; and (c) to pursue any other right or remedy Seller may have.

20.4 Remedies. The remedies in the Agreement are cumulative and in addition to all rights and remedies at law and in equity.

SECTION 21: RECORDS; AUDIT

21.1 Seller's Records. Seller shall maintain accurate and reasonably detailed books, records, and accounts, including all correspondence, of all fees and expenses billed to Duke Energy under the Agreement consistent with Generally Accepted Accounting Principles ("**GAAP**"). Seller shall retain for a period of three (3) years following final payment of the Contract Price all information and records relating to the Services performed or Goods delivered under the Agreement.

21.2 Duke Energy Audit Rights. Duke Energy and its designated third-party auditors shall have the right to audit Seller's records at any time during performance of the Agreement, after completion of the Services or delivery of the Goods, or, in the event more than one Purchase Order is issued under the Agreement, after any termination or cancelation of a Purchase Order, to the extent necessary to permit evaluation and verification of invoices, notices, payroll records; or claims submitted with respect to and Seller's compliance with the Agreement and Seller's dealings with Duke Energy, including without limitation the following (all as provided or made available to Seller upon commencement of performance under the Agreement and all as amended, restated, or supplemented from time to time): (a) Duke Energy's Supplier Code of Conduct; (b) Duke Energy's Alcohol and Drug Policy located under Contractor Training Materials at http://www.duke-energy.com/suppliers/contractor-training.asp; (c) Duke Energy's environmental, safety and security procedures, policies and regulations, inclusive of Duke Energy's Environmental, Health and Safety (EHS) Handbook located at https://www.duke-energy.com/partner-with-us/suppliers/ehs-orientation-training, which includes Duke Energy Business Unit EHS Supplemental Requirements; and (d) Duke Energy's Safety and Security procedures.

Duke Energy or its third-party auditors may examine and copy Seller's information and records maintained or retained in accordance with the Agreement at Seller's premises during regular business hours. Seller shall make any materials to be audited available within seven (7) to fourteen (14) calendar days from the date of the request. If any audit shows an overcharge to Duke Energy, then Seller shall immediately refund such overcharged amount.

SECTION 22: TAXES

22.1 Seller shall be responsible for, and shall pay directly, any and all corporate and individual taxes that are measured by net income, profit or gross receipts imposed by any governmental authority on Seller, its employees or subcontractors due to the execution of any agreement or the performance of or payment for Goods or Services in accordance with the Agreement. The price for the Services or Goods shall include all applicable foreign, federal, state and local taxes payable with respect to the Agreement. Seller assumes exclusive liability for all sales, use or privilege taxes applicable to any materials, supplies, equipment or tools purchased, rented, leased, used or otherwise consumed by Seller in conjunction with the performance of the Services. Seller shall invoice the sale of tangible personal property separately from the provision of labor or services. Tangible personal property includes materials, parts or other property that Seller installs, incorporates, furnishes or otherwise supplies for Duke Energy's use or consumption that becomes the property of Duke Energy. Invoices for tangible personal property sold or leased to Duke Energy shall contain a note stating, "Property Transferred to Duke Energy". Taxes shall be billed as a separate line item on the original invoice for taxable purchases. When sales tax is not billed on the original invoice for taxable purchases, Duke Energy is not responsible for reimbursement for the sales tax and such tax is the sole obligation of the Seller. If Duke Energy is exempt from the payment of any applicable sales, use or other taxes or has a direct payment permit with respect to such taxes, Seller may access such certificate or permit, duly executed and issued by the appropriate governmental authority in the following link: https://www.duke-energy.com/partner-with-us/suppliers/direct-pay-permits. Request for clarity or guidance around the appropriate certificate or permit to be used may be made to the dukesalestax@ey.com mailbox. If Seller fails to avail itself of such certificate or permit, Seller shall be responsible for and shall pay any sales, use or privilege tax resulting from such failure. The language in the following link shall apply to Goods or Services to be delivered or performed for the applicable Duke Energy utility entity or entities: https://www.duke-energy.com/_/media/pdfs/partner-with-us/state-specific-tax-language-01-2020.pdf?la=en.

22.2 Seller assumes exclusive liability for all contributions, taxes or payments required to be made under the applicable federal and state Unemployment Compensation Acts, Social Security Acts and all amendments, and all other current or future acts, federal or state, requiring payment by the Seller on account of the person hired, employed or paid by Seller for Services performed under the Agreement. When Services are to be performed in South Carolina, Seller shall submit prior to commencement of Services, a properly completed State of South Carolina, Department of Revenue, Nonresident Taxpayer Registration Affidavit Income Tax Withholding form, Form I-312.

22.3 Duke Energy shall be solely responsible for any ad valorem, property, license, privilege, excise, or similar taxes lawfully imposed on property owned by Duke Energy. Seller and its subcontractors shall be solely responsible for any ad valorem, property, license, privilege, excise or similar taxes lawfully imposed on property owned by Seller and its subcontractors, respectively that is used for but not incorporated into the Services.

SECTION 23: DISPUTES; WAIVER OF CONSEQUENTIAL DAMAGES

23.1 Notice of Dispute. Notice of any Dispute (as defined below) by Seller shall be made in writing to Duke Energy within five (5) calendar days after the first day of the event giving rise to such claim or Seller shall be deemed to have waived the claim. Written documentation and supporting data shall be promptly submitted by Seller to Duke Energy.

23.2 Dispute Resolution Procedure. The Parties shall attempt to resolve any claims, disputes and other controversies arising out of or relating to the Agreement (each a "**Dispute**" and, collectively, "**Disputes**") promptly by negotiation between individuals who have authority to settle the Dispute and who are at a higher level of management than the persons with direct responsibility for administration of the Agreement. All negotiations pursuant to this Section 23.2 are to be deemed confidential and shall be treated as compromise and settlement negotiations for purposes of applicable rules of evidence. If the Dispute has not been resolved by negotiation within sixty (60) days of the disputing Party's notice under Section 23.1, then either Party may initiate litigation.

23.3 Joinder. Either Party shall have the right, in its discretion, to include by joinder persons or entities substantially involved in a common question of law or fact whose presence is required if complete relief is to be accorded in any litigation.

23.4 Jurisdiction; Venue. Venue for any litigation of any Dispute shall lie exclusively in the appropriate state or federal courts in and for the State of North Carolina.

23.5 Continuing Performance. Seller shall proceed diligently with the performance of the delivery of the Goods and Services, as directed by Duke Energy, regardless of any pending Dispute.

23.6 Waiver of Jury Trial. To the extent permitted under applicable law, Seller and Duke Energy agree to relinquish and waive their rights to a trial by jury in any action brought hereunder.

23.7 Waiver of Consequential Damages. Excluding Seller's indemnity obligations set forth herein and excluding any liability under Section 16 and Section 17, neither Party shall be liable to the other Party for any incidental, indirect, special, punitive or consequential damages (including without limitation any damages relating to lost profits) ("**Consequential Damages**") arising in connection with the Agreement. The foregoing waiver shall not apply to (a) damages or losses covered by any insurance required by the Agreement; or (b) claims, losses, costs, or damages arising out of or relating to a Party's fraud, gross negligence, willful misconduct or intentional acts.

SECTION 24: MISCELLANEOUS PROVISIONS

24.1 Independent Contractor. Seller is an independent contractor and not an agent or employee of Duke Energy and nothing contained in the Agreement shall be so construed as to justify a finding of the existence of any relationship between Duke Energy and Seller inconsistent with that status. Seller shall have exclusive control of and responsibility for its labor relations.

24.2 Governing Law. The Agreement shall be governed and construed in accordance with the laws of the State of North Carolina, except that the North Carolina conflict of law provisions shall not be invoked in order to apply the laws of any other state or jurisdiction.

24.3 Entire Agreement. The Agreement contains the entire agreement of the Parties relating to the subject matter and supersedes all prior and contemporaneous agreements, understandings, usages of trade and courses of dealing, whether written or oral.

24.4 Successors and Assigns. Seller shall not assign all or any portion of the Agreement without the prior written consent of Duke Energy. If requested by Duke Energy, Seller shall provide Duke Energy with copies of any contracts with third parties regarding the assignment of rights hereunder. Any attempted assignment without Duke Energy's prior written consent shall be ineffective and void. The terms and conditions of the Agreement shall be binding upon and inure to the benefit of any and all successors and/or assigns of Duke Energy and Seller.

24.5 No Third-Party Beneficiaries. Notwithstanding any provision herein, the Agreement shall not confer or be construed in any manner to confer, directly or indirectly, any rights, privileges, benefits, and/or remedies, upon any parties other than the parties hereto and their respective successors and/or permitted assigns.

24.6 No Waiver. No delay in exercising or failure to exercise a right or remedy shall impair that or any other right or remedy or be construed as a waiver of any default. The failure of either Party in any one or more instances to insist upon performance of any of the terms or conditions of the Agreement, or to exercise any right or privilege contained in the Agreement, or the waiver of any breach of the terms or conditions of the Agreement, shall not be construed as thereafter waiving any such terms, conditions, rights or privileges, and the same shall continue and remain in full force and effect as if no waiver had occurred.

24.7 Survival. The provisions of Section 3.2(a) (Compliance with Regulatory Code of Conduct), Section 12.1 (Warranty Applicable to the Purchase of Goods), Section 12.2 (Warranty Applicable to the Purchase of Services), Section 12.3 (Warranty Applicable to Purchase of Software), Section 13 (Indemnification), Section 14 (Insurance), Section 16 (Confidential Information; Trademarks; Publicity), Section 19.2 (Mechanics Liens), Section 20 (Termination and Cancellation; Suspension), Section 23 (Disputes; Waiver of Consequential Damages), of these Standard Terms and
Conditions and all other provisions of the Agreement providing for indemnification or limitation of or protection against liability shall survive the termination, cancellation, or expiration of the Agreement.

24.8 Severability. If any term or provision of the Agreement shall to any extent be held invalid or unenforceable by a court of competent jurisdiction, the Agreement shall remain in full force and effect and the invalid or unenforceable term or provision shall be deemed stricken, and a suitable and equitable provision shall be substituted for such invalid or unenforceable provision in order to carry out, so far as may be valid and enforceable, the intent and purpose of such invalid or unenforceable provision.

24.9 Headings. Headings are provided for the convenience of the Parties and shall not affect the interpretation of any provision.

24.10 Modification. Changes to the Agreement and to the Services or Goods shall only be permitted and valid if accomplished pursuant to a written agreement signed by both Parties expressly modifying the Agreement (an "**Amendment**"), a Change Order or a Directive Change Order.

24.11 Differing Terms. DUKE ENERGY HEREBY GIVES NOTICE THAT IT OBJECTS TO THE INCLUSION OF ANY DIFFERENT OR ADDITIONAL TERMS PROPOSED BY SELLER. Any and all additional or different terms and conditions contained in any of Seller's acceptance, invoices, bills or other commercial documents are hereby rejected and shall not become part of the Agreement between the Parties, and any reference to Seller's proposal in the Agreement is solely for the purpose of incorporating said proposal's description and specifications of the Goods and Services to the extent that such description and specifications do not conflict with the description and specifications on the face of the Purchase Order to which these Standard Terms and Conditions are attached or included.

ATTACHMENT A

ACA AND MEDICAL COVERAGE

For purposes of this Attachment A ("Attachment"), Consultant, Contractor, and Seller shall mean "Labor Service Provider", this Attachment memorializes the agreement between Duke Energy and Labor Service Provider regarding the implementation of certain provisions of the Patient Protection and Affordable Care Act, as amended, and the rules, regulations and other guidance issued thereunder (the "ACA").

i. Consistent with the Agreement and for purposes of clarity, Labor Service Provider acknowledges that the individuals who perform services under the Agreement are employees of Labor Service Provider or Labor Service Provider's subcontractors ("Labor Service Provider Employees") and shall be treated accordingly and not as employees of Duke Energy.

ii. Labor Service Provider shall ensure that the Labor Service Provider Employees who are *full-time employees* ("Full-Time Labor Service Provider Employees") and their *dependent child(ren)* receive an offer of *minimum essential coverage* under Labor Service Provider's or Labor Service Provider's subcontractor's health care plan at least once each year that is *affordable* and provides *minimum value* ("ACA Coverage"), and shall satisfy all applicable reporting requirements under the ACA with respect to the Full-Time Labor Service Provider Employees.

iii. In accordance with the Agreement negotiated between the parties, Duke Energy shall pay Labor Service Provider a higher fee for each Full-Time Labor Service Provider Employee who enrolls in ACA Coverage than Duke Energy pays for Full-Time Labor Service Provider Employees who do not enroll in ACA Coverage, with the differential in such fee determined in accordance with the Agreement and applicable requirements of the ACA and the tax code, such that Labor Service Provider's and/or Labor Service Provider's subcontractor's offer of coverage shall be treated as an offer of coverage by Duke Energy, in accordance with the ACA and Section 4980H of the tax code.

iv. Labor Service Provider shall indemnify, defend and hold Duke Energy (including its parent, subsidiary and affiliate companies), its officers, employees, agents and employee benefits plans (collectively, the "Indemnified Parties") harmless from all claims, actions, fines, penalties, taxes, excise taxes, and liabilities (collectively, the "Claims") including, but not limited to, Claims imposed on the Indemnified Parties with respect to:

(a) Full-Time Labor Service Provider Employees and

(b) Duke Energy's (including its parent, subsidiary and affiliate companies') *full-time employees* arising out of Labor Service Provider's failure to comply with this Attachment.

This Attachment shall remain in full force and effect for the duration of the parties' Agreement unless and until agreed otherwise in writing by both parties.

Attachment B
Requirements for Seller Drug and Alcohol Policies and Procedures

(i) For any Services to be performed by Seller at Duke Energy Fossil/Hydroelectric generation properties for Regulated & Renewable Energy, participating Renewable Regulated Generation sites, Coal Combustion Products department sites, and Project Management & Construction department sites within Duke Energy Indiana, Duke Energy Ohio, Duke Energy Kentucky, Duke Energy Carolinas, Duke Energy Progress, Duke Energy Florida, and Piedmont Natural Gas Company, Inc., Seller's drug and alcohol policy shall be consistent with either the Coalition for Construction Safety ("CCS") (formerly MICCS) and/or the Construction Owners Association of the Tri-State ("COATS") COATS/Bethesda substance abuse testing programs and Seller and its subcontractor(s) will use their program, which may be the CCS/COATS program, and includes initial testing, for cause testing, and random testing (5% to 15% quarterly). A valid drug screen chain-of-custody form, documenting a pending result of a drug test performed within the past five days, may be accepted to access a Duke Energy site while testing is in process. Seller must confer with their designated Duke Energy Seller interface for applicability. The following are the minimum substance abuse testing parameters:

(A) Use of a Substance Abuse and Mental Health Services Administration ("SAMHSA") approved laboratory.
(B) Use of a Medical Review Officer ("MRO") for confirmation of positive test results.
(C) Use of a SAMHSA 5 Panel Drug Screen with the following ng/ml cutoff and confirmation levels:

Drug	Ng/ml Cutoff	Ng/ml Confirmation
Marijuana (THCA)	50	15
Amphetamines/ Methamphetamines	500	250
MDMA – Ecstasy/MDA	500	250
Cocaine	150	100
Phencyclidine (PCP)	25	25
Codeine/Morphine	2000	2000
Hydrocodone/Hydromorphone	300	100
Oxycodone/Oxymorphone	100	100
6-AM - Heroin	10	10

(D) Use of an evidential breath-testing device to detect the consumption of alcohol based on the following PHMSA/DOT Regulations:

BAC	Result	Required Action
0.00 - 0.019	Negative	No action required
0.02 - 0.039		Removed from covered functions until tested <0.02 or until >eight (8) hours (next shift)
0.04 and above	Positive	No work until: a) Referred, evaluated, and released by SAP, and b) Negative Return-To-Duty test result

(E) Unless otherwise prohibited by applicable law, Seller and its subcontractors shall conduct post-accident testing, as well as testing when there is an objective reasonable basis to do so as determined by Seller or by Duke Energy.

(F) Any Seller's worker, including contractors, subcontractors, and Seller's employees, under the influence of alcohol, or in possession of alcohol, any illegal drug, or any controlled substance will be removed, except that the lawful use of a controlled substance during work time shall be permitted if such use does not create a safety hazard to property or person, does not adversely affect the worker's ability to perform job duties and is disclosed to, and approved in writing by Seller management prior to its use. In all cases, the Seller's workers, including contractors, subcontractors, and Seller's employees must be fit for duty and pose no health or safety concern to themselves and others.

(ii) In addition to the Seller's drug testing program, while performing Services for Duke Energy, Seller and its subcontractors shall be subject to referral for random drug and alcohol testing by Duke Energy's vendor using the SAMHSA 5 limits as shown above for drug testing and the PHMSA/DOT criteria as shown above for alcohol testing, which results will be provided by the testing vendor solely to Seller for appropriate action. The random selection method used shall be truly random and credible. Random substance abuse testing may be on any day or night and generally encompasses up to approximately 15% of Seller's employees on site at a given time. At Duke Energy's discretion, random testing percentages may be adjusted higher or lower where Duke Energy deems appropriate.

(iii) Immediately upon receipt of test results, Seller shall remove from the job site any Seller or subcontractor employee who tests positive or in any way does not comply with the requirements herein and under applicable law, except as per (F) above in this section. Seller shall not allow an employee who tests positive to return to the Services for the duration of the project, unless, at a minimum, the following steps are completed by the employee: (a) the employee completes an evaluation with an SAP; (b) the SAP must, at a minimum, recommend the following: (1) some type of treatment or education beyond the initial assessment; (2) at least 3 follow-up tests in the 12 months following the return-to-duty test; (c) a minimum of 14 days must pass from the date of the positive test (date of that collection) before a test can be administered; and (d) the employee presents Seller with written documentation from a qualified SAP that states the employee is fit for duty (ready to return to work), has completed an evaluation, and has at least started some form of education or treatment beyond the initial evaluation; Seller or the employee must submit the written documentation to Duke Energy's random drug testing vendor when the positive test resulted from Duke Energy's referral to the random drug testing vendor. The written documentation should be on the SAP's letterhead and be personally signed by the SAP.

(iv) Operating nuclear stations are covered by a separate set of supplemental terms and conditions.

Attachment C

Network Security Supplement

1. **Storage and Encryption of Duke Energy Confidential Information and Duke Energy PII:**

   a. Seller shall not store, access, or maintain any Duke Energy Confidential Information outside the United States (including its territories and protectorates), or in any cloud service or facility, without the express prior written consent of Duke Energy.
   b. Seller shall encrypt all electronically stored Duke Energy Confidential Information in its possession both at rest and in transit.
   c. Seller shall encrypt all electronically stored Duke Energy PII data elements using the following design elements:

      i. The Duke Energy PII shall be encrypted in all applications where the Duke Energy PII is initially acquired.
      ii. Decryption of data elements of the Duke Energy PII shall only occur in a consuming application, or in output, with a Legitimate Business Requirement for native data elements of the PII . (A "Legitimate Business Requirement" is a need that supports or fulfills the provision of a Service under the Agreement.)
      iii. Access to a fully decrypted data element of the Duke Energy PII is provided only to individuals/entities with a Legitimate Business Requirement for such access, where such access is authenticated using identity management techniques.
      iv. Masking output is utilized to provide access to, or display, a portion of decrypted data in the absence of a Legitimate Business Requirement for decrypted access (i.e. mask all but last 4 digits of Social Security number on reports).
      v. Custom application(s) will be developed to accommodate ad hoc database queries returning decrypted results appropriate for the individual's Legitimate Business Requirement.

   d. Seller shall use encryption algorithms used for the Duke Energy Confidential Information and the Duke Energy PII that are currently endorsed by NIST (www.nist.gov), and such algorithms shall be updated as such NIST endorsements are updated from time-to-time. Seller may not use proprietary encryption algorithms.
   e. Seller shall employ encryption / decryption key management such that the keys are managed confidentially.

2. **Security.**

(a) **Vendor Network**: Upon request, Duke Energy may provide Seller access to an external network to access the Internet ("Vendor Network") while Seller works on-premises at a Duke Energy facility. Seller agrees that any use of the Internet and electronic mail through the Vendor Network will be solely for necessary business purposes.

(b) **Internal Network**: Duke Energy's internal network ("Internal Network") is independent of the Vendor Network. Seller agrees that it may access the Internal Network solely for the purpose of performing the Services. The Internal Network contains Duke Energy Confidential Information, which Seller may be required to access to perform the Services. Seller agrees that access to the Internal Network for other purposes, or the use of the Internal Network to access other non-Services-related networks, is strictly forbidden; and Seller shall be responsible and liable for all damages arising or resulting from such unauthorized access. Seller further agrees that such activity may result in the discontinuation of any and all Duke Energy network access.

(c) **Internet Access**: In accordance with Duke Energy's existing Internet usage policies, Seller and its employees shall not access any gambling, pornography or hate or violence sites from either the Vendor Network or the Internal Network; introduce any viruses, worms, Trojan horses, malware, bugs or errors in any Duke Energy network; or forward any chain letters, executable "ready to run" files, or other files which may cause damage to Duke Energy's computer or network systems. Duke Energy reserves the right to monitor Seller's use of the Vendor Network, the Internal Network, the Internet through the Vendor and Internal Networks, and Duke Energy's information systems for these or other unauthorized or unlawful activities and Seller agrees and consents to such monitoring.

(d) **Access Termination**: Duke Energy reserves the right, in its sole discretion, to terminate Seller's access to and use of the Vendor Network or Internal Network at any time, for any reason, and without notice to Seller.

(e) **Seller's Security Procedures**; **Seller's Security Program Requirements; Seller's Response Plan.**

(1) In addition to any other privacy, confidentiality, or security requirements set forth herein, Seller will maintain a comprehensive data and systems security program ("Security Program"), which encompasses (but is not limited to) any of Seller's goods that contain Software that processes Duke Energy Confidential Information, is executed or installed on any device connected to a Duke Energy information system or network, and any of Seller's Services that support or maintain such Software or connect to a Duke Energy information system or network and shall include, but may not be limited to, reasonable and appropriate technical, organizational, administrative and physical security measures to (i) ensure the security and confidentiality of and (ii) protect against the destruction, loss, and unauthorized access, acquisition, use, disclosure, or alteration of: (x) Duke Energy Confidential Information, (y) Duke Energy's information systems, and (z) Duke Energy's networks.

(2) Without limiting the generality of the foregoing, Seller's Security Program shall, (unless otherwise agreed in advance, in writing) at a minimum: (i) use industry standard software and hardware data and system security tools generally available on the market and shall not use Seller's proprietary technology without express written consent of Duke Energy; (ii) include secure user authentication protocols; secure access control measures; reasonable monitoring of systems on which Confidential Information is maintained; appropriate segregation of, and appropriate limited access to, Confidential Information from information of Seller or its other customers; effective systems for identifying and responding to threats; effective systems for identifying and addressing information security vulnerabilities; and appropriate personnel security and integrity procedures and practices; and (iii) use best practice cyber security and coding practices that address issues identified in the then current Open Web Application Security Project Top 10, and the SysAdmin, Audit, Networking, and Security ("SANS") Top 25 Programming Errors, and SANS top 20 critical controls.

(3) Seller shall promptly upon Duke Energy's request: (y) disclose to Duke Energy IT Security all backdoors, embedded credentials, and interactive remote management/support capabilities, and (z) verify that unused features not required for the operation and/or maintenance of the Goods have been removed or disabled. If Software that is not required cannot be removed or disabled, the Seller shall document a specific explanation and provide risk mitigating recommendations and/or specific technical justification. Software to be removed and/or disabled may include, but not be limited to: (a) games, (b) device drivers components not procured/delivered, (c) messaging services (e.g., email, instant messenger, peer-to-peer file sharing), (d)

source code and compilers, (e) unused networking and communications ports and protocols, and (f) all unused data and configuration files. The content and implementation of Seller's Security Program shall be fully documented in writing by Seller. Upon Duke Energy's request, Seller shall permit Duke Energy to review such documentation and/or inspect Seller's compliance with the Security Program.

(4) Seller's Security Program shall also include Multi-Factor Authentication (MFA) for access to Seller's electronic mail systems, and all Seller's systems which store, access or maintain Duke Energy Confidential Information. Seller shall have internal policies that prohibit employees and subcontractors from using email accounts or other methods outside of Seller's controlled systems for conducting email correspondence with Duke Energy or for the storage, access, use, maintenance, or destruction of Duke Energy Confidential Information.

(5) Seller's Security Program shall include a "Response Plan" which shall consist of implemented policies and procedures to address a Security Event (defined below) by mitigating the harmful effects of Security Events and addressing and remedying the occurrence to prevent the recurrence of similar Security Events in the future. 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. 2[6], NIST Special Publication 800-53 Rev. 4, CP-1 through CP-13 and the incident response requirements of NIST Special Publication 800-53 Rev. 4, IR-1 through IR-10 as those standards may be amended. All steps taken in responding to a Security Event shall be properly documented and chain of custody shall be maintained for all such documentation, including but not limited to any images captured.

If Seller does not have the in-house capability to perform the actions required by this Section in a professional and competent manner, Seller shall retain an outside forensic expert to do so at Seller's own expense. All loss of information or knowledge, or of the reliability thereof, caused by Seller's failure to retain an independent qualified forensics expert shall be presumed to be the fault of Seller.

A "Security Event" means any circumstance when (i) Seller knows or reasonably believes that Duke Energy Confidential Information has been subject to any circumstance where the security, integrity, or confidentiality of any Duke Energy Confidential Information has been compromised, including but not limited to incidents where Duke Energy Confidential Information has been damaged, lost, corrupted, destroyed, or accessed, acquired, modified, used, disclosed, or rendered inaccessible, by any unauthorized person, by any person in an unauthorized manner, or for an unauthorized purpose, (ii) Seller knows or reasonably believes that an act or omission has compromised or may reasonably compromise the cybersecurity of the goods or services provided to Duke Energy by Seller or the physical, technical, administrative, or organizational safeguards protecting Seller's systems or Duke Energy computer network, informational systems, or operational systems; or (iii) Seller receives any complaint, notice, or communication which relates directly or indirectly to a Security Event involving (A) Seller's handling of Duke Energy Confidential Information or Seller's compliance with the data safeguards in the Agreement or applicable law in connection with Duke Energy Confidential Information or (B) the cybersecurity of the products or services provided to Duke Energy by Seller.

(6) Seller, and any of Seller's subcontractors, agrees to notify Duke Energy Cyber Command Center by phone at 1-980-373-4916 or email to CyberCommandCenter@Duke-Energy.com with copy to the Duke Energy representative (in accordance with Section 37 hereof), as soon as reasonably possible (but in no case later than twenty-four (24) hours) after it becomes aware of any Security Event. Notwithstanding the twenty-four (24) hour requirement set forth above, Seller agrees to provide such notification within thirty (30) minutes after it becomes aware of any such Security Event that is reasonably likely to have a material adverse effect on the integrity or operation of a Critical Cyber System (as defined below). All notices of the Security Event shall summarize in reasonable detail, including but not limited to, (i) the effect on Duke Energy, if known, and (ii) the date and time identified. Seller shall cooperate fully with Duke Energy and remediate the effects of such Security Event, develop and execute a plan that reduces the likelihood of the same or similar Security Event from occurring in the future and consistent with the requirements of Seller's Response Plan, provide Duke Energy guidance, recommendations and other necessary information for recovery efforts and long-term remediation and/or mitigation, and provide Duke Energy with such assurances as Duke Energy shall request that such Security Event is not likely to recur. The content of any filing, communication, notice, press release or report related to any Security Event with inference to or identification of Duke Energy must be approved by Duke Energy prior to any publication or communication. "Critical Cyber System: means any computer or information network, system, facility, equipment, hardware device, or Software which, if misused, degraded, destroyed, or rendered unavailable, would adversely affect the reliable operation of Duke Energy's bulk electric systems, natural gas transmission or distribution systems, nuclear facilities or electric distribution system."

(7) Upon the occurrence of a Security Event involving (i) Confidential Information in the possession, custody or control of Seller or for which Seller is otherwise responsible, or (ii) Critical Cyber Systems accessed by or accessible to Seller in connection with Seller's performance of the Services for or on behalf of Duke Energy, Seller shall reimburse Duke Energy on demand for; (x) all Notification Related Costs (as defined below) incurred by Duke Energy arising out of or in connection with any such Security Event; (y) all Security Event Damages (as defined below) incurred by Duke Energy arising out of or in connection with any such Security Event. "Notification Related Costs" shall include Duke Energy's internal and external costs associated with investigating, addressing and responding to the Security Event, including but not limited to: (i) preparation and mailing or other transmission of notifications or other communications to consumers, employees or others as Duke Energy deems reasonably appropriate; and (ii) costs for commercially reasonable credit monitoring or identity protection service. "Security Event Damages" shall include Duke Energy's internal and external costs associated with investigating, addressing and responding to the Security Event, including but not limited to: (i) establishment of a call center or other communications procedures in response to such Security Event (e.g., customer service FAQs, talking points and training); (ii) public relations and other similar crisis management services; (iii) legal, consulting, forensic expert and accounting fees and expenses associated with Duke Energy's investigation of and response to such event; (iv) damages incurred by Duke Energy related to third party claims for unauthorized access, exposure or disclosure of such third party's data possessed or licensed by Duke Energy; and (v) damages related to unauthorized access, exposure or disclosure of Duke Energy Confidential Information.

(8) Upon determining that a Security Event has been resolved or for which Seller's actions otherwise cease in accordance with its Response Plan or otherwise upon request by Duke Energy after a reasonable time has elapsed since the Security Event was reported, Seller shall within ten (10) business days provide to Duke Energy a written executive summary or other similar document detailing the (i) suspected or confirmed cause of the Security Event; (ii) Duke Energy data, including Confidential Information and a list of Critical Cyber Systems, affected; (iii) steps taken to address the Security Event and steps to be implemented by Seller's management to prevent reoccurrences of Security Events of a similar nature; (iv) list of communications made to third parties, including data subjects and law enforcement agencies, as a result of the Security Event; (v) a list of services provided by the Seller to affected data subjects, including, but not limited to, credit monitoring services, reimbursement of related costs, etc.; and (vi) a statement certifying that the underlying cause of the Security Event has been mitigated.

(f) **Data Security and Compliance Audits**: If Seller: (i) provides any Software that is installed on a Duke Energy computer or network; or (ii) has access to, or stores or processes any Duke Energy Confidential Information; or (iii) connects its computer systems, Software, and/or applications to any Duke Energy network, including but not limited to, the Vendor Network or Internal Network, then Duke Energy shall have the right to monitor Seller's

compliance with the terms of this Section and perform data security and system integrity audits ("Audits") on any of Seller's applicable systems and/or applications used to provide the Software or Services. Seller hereby grants permission to Duke Energy to perform such Audits.

a. On an annual basis, Seller, at Seller's expense, shall require auditors to conduct an examination of the controls placed in operation and a test of operating effectiveness either: (1), as defined by current Statement on Standards for Attestation Engagements ("SSAE") reporting on Service Organization Controls ("SOC"), of the services performed by Seller for or on behalf of Duke Energy and issue SOC 2 (Type 2) and SOC 3 reports thereon (collectively "SOC Reports") for the applicable calendar year, or (2) as evidenced through providing current ISO 27001 or IEC 62443 certification. Seller shall deliver to Duke Energy a copy of the SOC Reports, ISO 27001 certification, or IEC 62443 certification within six (6) weeks after conducting the assessment for the calendar year. Seller shall correct any audit control issues, deficiencies or weaknesses identified in any assessment reports, at no additional cost to Duke Energy. If specific audit recommendations are not implemented by Seller, then Seller should implement such alternative steps as are reasonably satisfactory to Duke Energy for the purposes of minimizing or eliminating the risks identified in any such assessment report.
b. If Seller does not cause an SSAE examination or obtain ISO 27001 or IEC 62443 certification of the controls placed in operation and a test of operating effectiveness to be conducted as described in paragraph a. above and deliver the SOC Reports, ISO certification, or IEC 62443 certification to Duke Energy, Duke Energy shall, at its discretion, conduct an audit, or have an audit conducted by a designated representative, at Duke Energy's expense at a date and time mutually agreed to by Duke Energy and Seller. Such Audits may include, but shall not be limited to, physical inspection of facilities and equipment, external scan, penetration testing, process reviews, and reviews of system configurations, including firewall rule sets, and any information or materials in Seller's possession, custody or control, relating in any way to Seller's obligations under this Section. Duke Energy has the right to review summary results of internal scans that have been performed on Seller's internal servers connected to the Internal Network.
c. To the fullest extent permitted by law, Seller hereby waives the benefit of any state or federal law which may provide a cause of action against Duke Energy based on actions permitted under this Section.
d. Should the Audits result in the discovery of material data security or system integrity risks to Duke Energy, Duke Energy shall notify Seller of such risks and Seller shall respond to Duke Energy in writing with Seller's plan to take reasonable measures to promptly correct, repair or modify its network or application to effectively eliminate the risk, at no cost to Duke Energy, and Seller shall have 10 (ten) business days to cure such data security or system integrity risks, unless Duke Energy agrees to a longer period of time for such cure. If a data security or system integrity risk is, in good faith, found by Duke Energy and such risk cannot be alleviated in the timeframe contemplated by this Section, based on the nature of the risk, Duke Energy may terminate its network connection to Seller immediately with or without notice to Seller without cost or liability to Duke Energy. Upon Duke Energy's written request, Seller shall complete and submit to Duke Energy an information security due diligence questionnaire provided by Duke Energy within the time-frame requested by Duke Energy.

(g) **Remote Access:** Duke Energy may require Services from Seller that require or involve Seller accessing Duke Energy's information systems ("Systems") via "Remote Access", which is any method used to access a Duke Energy network or information technology or communications asset from an offsite location, including but not limited to: direct or static connections, virtual private network ("VPN"), or virtual desktop image connectivity. These Systems include, but are not limited to, those systems, networks, applications, equipment, Software or hardware of Duke Energy to which seller has Remote Access. Seller recognizes and acknowledges that the Systems are valuable and sensitive assets of Duke Energy and may be damaged by misuse. Seller recognizes that it has no legal or contractual right to continue receiving Remote Access but Duke Energy is willing to permit the continued Remote Access subject to Seller's compliance with the Agreement.

i. Access to Systems. In connection with (and as part of) the Services, Duke Energy may in its sole discretion permit Seller to have Remote Access to the Systems using a Duke Energy-authorized communications protocol and subject to compliance with the Agreement. Seller acknowledges and agrees that such Remote Access may be subject to monitoring by Duke Energy.

ii. Regulatory Framework. Without limiting any other provision of the Agreement, Seller acknowledges that Duke Energy Affiliates (as owners and operators of energy generation, transmission and distribution assets and systems) are subject to regulation and oversight by a number of agencies and bodies, including, but not limited to, the NRC, the Federal Energy Regulatory Commission ("FERC"), and NERC. As such, Duke Energy, and its Affiliates, are required to comply with various security and reliability regulations, rules and standards promulgated from time to time by FERC, NERC, the NRC and potentially other bodies. In addition, Duke Energy Affiliates may also receive regulatory guidance from time to time from such bodies or through executive orders. Such regulations, rules, standards and guidance include, but are not limited to, 10 CFR §73.54; 18 CFR Parts 39 – 40; the NERC Critical Infrastructure Reliability ("CIP") standards (currently located at http://www.nerc.com/pa/stand/Pages/ReliabilityStandardsUnitedStates.aspx?jurisdiction=United); the Framework for Improving Critical Infrastructure Cybersecurity issued by the National Institute of Standards and Technology pursuant to Executive Order 13636; modifications, updates or replacements of the foregoing regulations, rules, standards and guidelines; and new rules, regulations, standards and guidelines that may hereafter be issued by any of such agencies or bodies (collectively the "Security Regulations & Standards"). In addition, Seller acknowledges that it may receive access to Systems that host PII relating to customers, employees, contractors, Seller and/or other representatives of Duke Energy, and that such data may be protected by Privacy Laws.

iii. Seller Controls for Remote Access: Seller shall ensure Seller personnel do not use any virtual private network or other device to simultaneously connect machines on any Duke Energy system or network to any machines on any Seller or third party systems, without (i) prior written consent of Duke Energy, (ii) providing Duke Energy with the unique identifier and full name of each individual who uses any such remote access method and the phone number and email address at which the individual may be reached while using the remote access method, and (iii) ensuring that any computer used by Seller personnel to remotely access any Company system or network will not simultaneously access the Internet or any other third party system or network while logged on to Duke Energy systems or networks. For Seller's IT assets connecting to a Duke Energy network, the Seller shall provide virus protection and apply appropriate hardware, software, and firmware updates to remediate newly discovered vulnerabilities or weaknesses within 30 days. Updates to remediate critical vulnerabilities shall be provided within a shorter period than other updates, within 10 days.

iv. Exceptions. If Seller believes it cannot implement one or more updates within the time required without adversely affecting its own network(s) or business, it may so inform Duke Energy by notice to Duke Energy, and Duke Energy will reasonably attempt to resolve Seller's concerns while still protecting the Systems. Duke Energy may, in its sole discretion, allow Seller to adopt measures equivalent in effectiveness to those to which exception has been taken. Duke Energy is not obligated to extend the deadline for denying access or to address or resolve Seller's concerns in a manner acceptable to Seller or at all prior to denying access, although Duke Energy will use reasonable efforts to do so. The final decision on any exception requested by Seller shall be made by Duke Energy's Cybersecurity & IT Compliance organization or its successor organization.

v. Suspension of Access. Seller acknowledges and agrees that Duke Energy may suspend access to the Systems at any time without further notice for any reason, including, but not limited to, Seller's failure to implement and certify its implementation of the security procedures and standards set forth in the Agreement. Any such suspension shall be without prejudice to any other rights or remedies that Duke Energy may have. Unless otherwise directed by Duke Energy, following any suspension of Remote Access Seller shall: (a) use good faith efforts to find a reasonable, mutually acceptable alternative method for performing any of the Services which were performed through Remote Access; and (b) use that method to perform such Services. If despite its good faith efforts, Seller is unable to perform all or any portion of the Services as a result of the Remote Access suspension, and provided such suspension was not attributable to Seller's breach of the Agreement, Seller shall be temporarily relieved of any requirement to perform only those Services that cannot be performed as a result of the Remote Access suspension (the "Suspended Services") and Duke Energy shall be relieved of paying for such Suspended Services that are not performed. Upon resumption of the Remote Access, Seller shall promptly recommence performance of the Suspended Services.

vi. Nuclear Station Remote Services. If any of the Remote Services will be performed by Seller inside the Owner Controlled Area of a Duke Energy nuclear station, the terms and conditions of Duke Energy Nuclear Supplemental Terms shall apply to the Agreement. "Owner Controlled Area" shall have the meaning set forth in the Duke Energy Nuclear Supplemental Terms.

vii. System Information. Seller agrees any information contained within, relating to, or obtained by Seller from, the Systems shall be deemed "System Information". Such System Information shall be treated as Confidential Information in accordance with the Agreement, and Seller shall hold such System Information in confidence in accordance with the provisions of the Agreement. Seller shall: (i) not remove or delete the System Information (or any other data within the Systems) from the Systems, nor shall it copy (or permit to be copied) any of the System Information (or any other data within the Systems) to any computer, media or storage device or file under the control of Seller or any other person or entity acting by or through Seller; and (ii) only permit access to System Information to a Seller employees and subcontractors with a need to know such information for Remote Access as necessary to render the Services. Seller shall not permit access to, or otherwise provide, any System Information to any person or entity except as expressly permitted in the Agreement or as authorized in writing by Duke Energy. As a condition of any such Remote Access, all permitted subcontractors hereunder shall agree to be bound by the terms of the Agreement.

viii. Access Records Retention and Audit. If Seller's access and use of the Systems is established using a direct or static connection that may limit Duke Energy's capability to authenticate the individual, Seller shall ensure Seller personnel accessing Duke Energy's networks are uniquely identified and that accounts are not shared between personnel, maintain complete and accurate books, user logs, access credential data, records, equipment/application inventories and system diagrams relating to any Seller's access to the Systems, and any hardware, equipment, devices, communication systems or software used by Seller to access any of the Systems during the periods of Remote Access (the "Access Records"). During the period that Seller has been provided Remote Access, and for a period of one year thereafter, Duke Energy shall have the right to inspect, copy and audit at all reasonable times at Seller's offices the Access Records, including compliance by Seller with each of its obligations under the Agreement.

(h) **Duke Asset Access.** Should Seller or any of its employees, subcontractors, representatives, or any other similarly authorized third parties under the control of Seller who will be providing Services hereunder on behalf of such Seller require or be permitted cyber access or unescorted physical access to Duke Energy's assets, shall be required to meet certain pre-requisites prior to access to any such assets. Therefore, when any secured electronic or physical access is needed or permitted, all persons identified above in this provision shall: (a) take the Duke Energy administered role-based Cybersecurity trainings and, if needed, the IT courses located under Contractor Training Materials at http://www.duke-energy.com/suppliers/Contractor-training.asp; and (b) be given a company identification number in the Duke Energy Human Resources Management System (HRMS) for tracking purposes. If any persons identified above require or be permitted cyber access or unescorted physical access to Duke Energy's BES Cyber Systems (BCS) or BES Cyber System Information (BCSI) as such terms are defined by the regulatory requirements of the North American Electric Reliability Corporation (NERC), all such persons shall be required to meet additional pre-requisites prior to access to any BCS or BCSI. Therefore, when any secured electronic or physical access is needed or permitted to BCS or BCSI, all persons identified above in this provision shall additionally: (a) successfully complete the Duke Energy-administered background screening requirement; (b) take the Duke Energy-administered Cybersecurity trainings applicable to the type of access provided on a frequency as prescribed by Duke Energy. In the event that Seller (i) determines that any of the persons permitted access pursuant to this Section no longer require access or (ii) suspends or terminates the employment of any of the persons permitted access pursuant to the Section or (iii) reasonably believes any persons permitted access pursuant to this Section poses a threat to the safe working environment at or to any Duke Energy property, including to employees, customers, buildings, assets, systems, networks, and/or Confidential Information or (iv) there are any material adverse changes to any persons permitted access pursuant to this Section background history, including, without limitation, any information not previously known or reported in person's background report or record or (v) any persons permitted access pursuant to this Section no longer meet pre-requisites required to obtain such access or (vi) any persons permitted access pursuant to this Section loses their U.S. work authorization or (vii) Seller's provisions of goods and services to Duke Energy under the Agreement is either completed or terminated, so that Duke Energy can discontinue permitted access, Seller will take all steps reasonably necessary to immediately deny such Seller persons electronic and physical access to Duke Energy Confidential Information as well as Duke Energy property, systems, or networks, including, but not limited to, removing and securing individual credentials and access badges, multifactor security tokens, and laptops, as applicable, and will return to Duke Energy any Duke Energy-issued property including, but not limited to, Duke Energy photo ID badge, keys, documents, or electronic equipment in the possession of such Seller person. Seller shall notify Duke Energy promptly to allow for the removal of the ability for access within 24 hours of such determination access is no longer required or suppension or termination of persons permitted access. Seller shall review and verify Seller's person's continued need for access and the level of cyber access or unescorted physical access on a quarterly basis and retain evidence of such reviews for two years.

(i) **Return of Hardware and Removable Media**. Promptly upon the expiration or earlier termination of the Agreement, or such earlier time as Duke Energy requests in writing, Seller will return to Duke Energy or its designee, all hardware and removable media provided by Duke Energy containing Duke Energy Confidential Information. Confidential Information in such returned hardware and removable media shall not be removed or altered in any way. The hardware and removable media should be physically sealed and returned via a bonded courier or as otherwise directed by Duke Energy. If the return of hardware or removable is not reasonably feasible or desirable to Duke Energy (which decision will be at Duke Energy's sole discretion), Seller shall dispose of hardware following disposal procedures that are compliant with current NIST Special Publication 800-88 and provide Duke Energy written certification from one of Seller's officers within fifteen (15) calendar days after destruction with information detailing the destruction method used, the date of destruction, and the entity or individual who performed the destruction.

(j) **Patch Management and Updates**. For Seller's Goods or IT assets connecting to a Duke Energy network, the Seller shall provide appropriate

hardware, software, and firmware updates to remediate newly discovered malware, vulnerabilities or weaknesses within 30 days. Updates to remediate critical vulnerabilities shall be provided within a shorter period than other updates, within 10 days. All updates as provided in this section shall be individually referred to as a "Patch Update" and collectively referred to as "Patch Updates". If Seller believes it cannot provide or implement one or more Patch Updates within the time required, it may so inform Duke Energy by notice to Duke Energy, and Duke Energy will reasonably attempt to resolve Seller's concerns. Duke Energy may, in its sole discretion, allow Seller to adopt measures equivalent in effectiveness to those to which exception has been taken. The final decision on any exception requested by Seller shall be made by Duke Energy's Cybersecurity & IT Compliance organization or its successor organization.

(k) **Software Supplement**. If Seller provides Software to Duke Energy, Seller hereby agrees to the Software Security Supplement attached hereto as Supplement A and incorporated herein by reference.

(l) **Hardware Supplement**. If Seller provides any Goods that are information system, operational system, communications system or, other cyber asset computer, device, equipment that may be connected to Duke Energy network, Seller hereby agrees to the Hardware Security Supplement attached hereto as Supplement B and incorporated herein by reference.

(m) **Hosting Service Supplement**. If Seller provides or use any managed hosting services, which is inclusive use of any cloud services, in the performance of Services, Seller hereby agrees to the Hosting Services Security Supplement attached hereto as Supplement C and incorporated herein by reference.

(n) **Personnel Services**. If Seller's personnel shall (a) have access to Duke Energy Confidential Information, Vendor Network, Internal Network, Systems; or (b) provide Services in the development, maintenance, or support of Duke Energy Software, Seller hereby agrees to the Services Security Supplement attached hereto as Supplement D and incorporated herein by reference.

Attachment C - Supplement A
SOFTWARE SECURITY SUPPLEMENT

This Software Security Supplement applies to any Supplier, which may be referenced in the Agreement as Consultant, Contractor, or Seller, that provides Software to Duke Energy. Software shall include any software, firmware, opensource, or source code (collectively "Software") provided with Supplier's Goods, products, or Services.

1. Software and Services.

1.1 The Supplier shall provide the application inventory of all Software that supports the procured product, including open source code, scripts and/or macros, run time configuration files and interpreters, databases and tables, and all other included software (identifying versions, revisions, and/or patch levels, as delivered). The documentation shall include all ports and authorized services required for normal operation, emergency operation, or troubleshooting.

1.2 The Supplier shall provide access to summary documentation of the Software's security features and security-focused instructions on product maintenance, support, and reconfiguration of default settings.

2. Access Control.

2.1 The Supplier shall configure each component of the Software to operate using the principle of least privilege. This includes operating system permissions, file access, user accounts, application-to-application communications, and information system services. The Supplier shall configure the Software, or provide Duke Energy documentation, detailing how to configure Software, such that when a session is initiated from a less privileged application, access shall be limited and enforced at the more critical side.

2.2 The Supplier shall provide access to documentation of available options for defining access and security permissions, user accounts, and applications with associated roles. If the Supplier performs the configuration, the Supplier shall configure these options as specified by Duke Energy. User accounts shall allow configurable access and permissions associated with one or more organizationally defined user role(s), where roles are used. If roles are used, the Supplier shall provide a system administration mechanism for changing user(s') role (e.g., group) associations.

2.3 The Supplier shall verify and, upon Duke Energy's request, provide documentation for the Software, attesting that unauthorized logging devices are not installed (e.g., key loggers, cameras, and microphones).

2.4 The Supplier shall deliver a product that has no restrictions with components being placed in separate network zones. In addition, all products and components will have no restrictions on placement of stateful or next generation firewalls.

3. Account Management.

3.1 The Supplier shall provide access to documentation for all accounts (including, but not limited to, generic and/or default) that need to be active for proper operation of the Software. Where technically feasible, Supplier default accounts not needed for normal or maintenance operations shall be removed or deactivated. When Supplier default accounts cannot be removed or deactivated, then Supplier shall ensure (a) where technically feasible, the account is renamed (b) passwords are changed to meet Duke Energy password requirements, (c) usage is limited to only Duke Energy authorized personnel, and (d) accounts are not used for individual access. The Supplier shall change default account settings to Duke Energy-specific requirements or support Duke Energy in these changes. The Supplier shall not publish changed account information. When supplier modifies default account settings, the Supplier shall provide new account information to Duke Energy via a protected mechanism.

3.2 Account password controls must be provided for all accounts unless otherwise agreed to in writing by both parties. Password controls shall include (a) passwords must be complex and have a minimum of 15 characters, (b) passwords must not be easily associated with Duke Energy or any individual person, including but not limited to account name, user name, social security number, employee number, (c) force users to change passwords at least every sixty days, (d) users must not use cyclical or patterned passwords, such as when changing passwords, users must not add a number at the end of the password in sequence, (e) password history controls to disallow the user from reusing one of their passwords previously used in the last 10 password changes, and (f) password changes will have a minimum lifetime of 24 hours. Complex password requirements shall include at least three of the following four characteristics: (1) Uppercase letters (A-Z), (2) Lowercase letters (a-z), (3) Numbers (0-9), and (4) Special characters (i.e. "!, @, #, $, %, ^, &, *, and +).

4. Session Management.

4.1 The Supplier shall not permit user credentials to be transmitted or shared in clear text. The Supplier shall not store user credentials in clear text unless the Supplier and Duke Energy agree that this is an acceptable practice given the protection offered by other security controls. The Supplier shall only allow access protocols that encrypt or securely transmit login credentials (e.g., tunneling through Secure Shell Terminal Emulation ("SSH"), Transport Layer Security ("TLS")).

4.2 Unless specifically requested by Duke Energy, the Supplier shall not allow multiple concurrent logins using the same authentication credentials, allow applications to retain login information between sessions, provide any auto-fill functionality during login, or allow anonymous logins.

4.3 The Supplier shall provide configurable session logout and timeout settings (e.g., alarms and human-machine interfaces).

5. Authentication / Password Policy and Management.

5.1 The Supplier shall provide access to documentation of the levels, methods, and capabilities for authentication and authorization.

5.2 The Supplier shall provide integration with Active Directory for authentication and authorization or provide a centralized and local account management capability with a configurable account password management system that allows for, but is not limited to, the following: (a) Changes to passwords (including default passwords), (b) Selection of password length, (c) Frequency of change, (d) Setting of required password complexity, (e) Number of login attempts prior to lockout, (f) Inactive session logout, (g) Comparison to a library of forbidden strings, (h) Derivative use of the user name / user ID, and (i) Denial of repeated or recycled use of the same password. The Supplier shall ensure passwords are not stored in clear text and not hardcoded into Software or scripts.

5.3 If single-sign on is provided, the Supplier shall (a) ensure that account access for single sign-on is equivalent to that enforced as a result of direct login, (b) use a secure method of authentication (e.g., strong two-factor authentication) to allow single sign-on to a suite of applications, (c) protect key files and access control lists used by the single-sign-on system from non-administrative user read, write, and delete access, (d) I provide access to documentation on configuring a single-sign-on system, as well as documentation showing equivalent results in running validation tests against the direct login and the single sign-on.

6. Logging and Auditing.

6.1 The Supplier shall provide access to a list of all log management capabilities that the Software is capable of generating, the format of those logs, recommended log management and Security Information and Event Management ("SIEM") integration methods (e.g., syslog) with Duke Energy's existing logging system, and identification of which of those logs are enabled by default. Logging capabilities provided by the Supplier shall cover the following events, at a minimum (as appropriate to their function): (a) Information requests and server responses, (b) Successful and unsuccessful authentication and access attempts, (c) Account changes, (d) Privileged use, (e) Application start-up and shutdown, (f) Application failures, and (g) Major application configuration changes

6.2 The Supplier shall provide standard time synchronization in the procured product (e.g., Global Positioning System ("GPS"), Network Time Protocol ("NTP"), and IEEE 1508-2008). If the Supplier is not providing standard time synchronization and is providing an authoritative time source, the procured product shall be configured to synchronize to the authoritative time source.

6.4 The Supplier shall provide for the confidentiality, integrity, and availability of log files. All audit trails and log files shall include time stamp of each event.

6.5 The Supplier shall provide access to documentation regarding recommended or implemented approach for collecting and retaining logs for a period of time that will provide a complete audit trail should events require a forensics investigation.

7. Communication Restrictions.

7.1 The Supplier shall recommend guidance on the design and configuration of network security zones within the procured product.

7.2 The Supplier shall provide access to information on all communications (e.g., protocols) required between network security zones, whether inbound or outbound, and identify each network component of the procured product initiating communication.

7.3 For IP addressable products, the Supplier shall verify that the procured product allows use of unique routable network address spaces (i.e., address spaces other than 192.168.0.0/16, 172.16.0.0/12, and 10.0.0.0/8 must be supported) that work within Duke Energy's network. Where this is not available, the Supplier shall offer an alternative approach, with mitigating security measures, that is acceptable to Duke Energy.

8. Malware Detection and Protection.

8.1 The Supplier shall ensure that the Software is compatible and supported with Duke Energy current malware detection capabilities. In the event Supplier Software is not capable of operating with Duke Energy malware detection capabilities, the supplier share obtain Duke Energy approval and implement at least one of the following: (a) Provide a host-based malware detection capability, quarantine (instead of automatically deleting) suspected infected files, provide an updating scheme for malware signatures, and test and confirm compatibility of malware detection application patches and upgrades, (b) if the Supplier is not providing the host-based malware detection capability, the Supplier shall suggest malware detection products to be used and provide guidance on malware detection and configuration settings that will work with Supplier products, or (c) if the Supplier is not providing a host-based malware detection capability, nor suggesting malware detection products, and if specified by Duke Energy, the Supplier shall provide an application whitelisting solution that is tested, validated, and documented that shall only permit approved applications to run.

8.2 The Supplier shall validate that cybersecurity services running on the Software (e.g., virus checking and malware detection) do not conflict with other such services running on the Software.

9. Reliability and Adherence to Standards.

9.1 The Supplier shall verify that the addition of security features does not adversely affect the solution's ability to meet Supplier benchmarks for performance or service level agreements. Upon request, Supplier shall provide documentation on the test criteria, platforms and results.

10. Secure Development Practices.

10.1 The Supplier shall provide access to summary documentation of its secure product development life cycle including the standards, practices (including continuous improvement), and development environment (including the use of secure coding practices) used to create or modify Supplier-provided information system Software.

10.2 The Supplier shall identify the country (or countries) of origin of the Software and its components. The Supplier shall identify the countries where the development, maintenance, and service for the Software are provided. The Supplier shall notify Duke Energy of changes in the list of countries where Software maintenance or other services are provided in support of the Software or services. This notification shall occur within 30 days prior to initiating a change in the list of countries.

10.3 Supplier shall implement a Quality Assurance program and validate that the Software procured has undergone Quality Control testing to identify and correct potential cybersecurity weaknesses and vulnerabilities. Supplier shall use positive and appropriate negative tests to verify that the Software operates in accordance with requirements and without extra functionality, as well as monitor for unexpected or undesirable behavior during these tests. For all web-based applications, interfaces and other modules, the Supplier shall provide access to documentation of all input validation testing including, but not limited to, measures for prevention of command injection, Structured Query Language ("SQL") injection, directory traversal, Remote File Include, Cross-Site Scripting ("XSS"), and buffer overflow. Supplier shall provide access to summary documentation of the results of the testing that includes unresolved vulnerabilities and recommended mitigation measures.

10.4 The Supplier shall provide a contingency plan for sustaining the security of the Software in the event the Supplier leaves the business (e.g., security-related procedures and products placed in escrow).

11. Vulnerabilities and Material Defects.

Supplier shall develop and implement policies and procedures to address the disclosure and remediation by Supplier of vulnerabilities and material defects related to the Software and services provided to Duke Energy under the Agreement including the following:

11.1 Prior to the delivery of the Software or service, Supplier shall provide or direct Duke Energy to an available source of summary documentation of publicly disclosed vulnerabilities and material defects related in the Software or services, the potential impact of such vulnerabilities and material defects, the status of Supplier's efforts to mitigate those publicly disclosed vulnerabilities and material defects, and Supplier's recommended corrective actions, compensating security controls, mitigations, and/or procedural workarounds.

11.2 Supplier shall provide or direct Duke Energy to an available source of summary documentation of vulnerabilities and material defects in the Software or services within seven (7) calendar days after such vulnerabilities and material defects become known to Supplier. This includes summary documentation on vulnerabilities that have not been publicly disclosed or have only been identified after the delivery of the Software. 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.

11.3 Whether or not publicly disclosed by Supplier, and notwithstanding any other limitation in the Agreement, Duke Energy may disclose any vulnerabilities or material defects in the Software provided by Supplier to (a) the Electricity Information Sharing and Analysis Center (E-ISAC), the United States Cyber Emergency Response Team (CERT), Department of Homeland Security, or Federal Bureau of Investigation, or any equivalent U.S. governmental entity or program, (b) to any entity when necessary to preserve the reliability of the Bulk Electric System (BES) as determined by Duke Energy in its sole discretion, or (c) any entity required by applicable law.

12. Problem Reporting.

12.1 The Supplier shall provide a secure process for users to submit problem reports and remediation requests. This process shall include tracking history and corrective action status reporting.

12.2 Upon Duke Energy submitting a problem report to the Supplier, the Supplier shall review the report, develop and communicate to Duke Energy an initial action plan, and provide status reports of the problem resolution to Duke Energy at the frequency requested by Duke Energy for the reported problem.

12.3 The Supplier shall provide Duke Energy with access to documentation related to its responsible disclosure and threat reporting policies and procedures (e.g., Computer Emergency Response Teams ("CERTs"), which shall address public disclosure protections implemented by the Supplier.

13. Patch Management and Updates.

13.1 The Supplier shall provide access to documentation of its patch management program and update process (including third party software and firmware). This documentation shall include resources and technical capabilities to sustain this program and process. This includes the Supplier's method or recommendation for how the integrity of the patch is validated by Duke Energy. This documentation shall also include the Supplier's approach and capability to remediate newly reported zero-day vulnerabilities.

13.2 The Supplier shall verify and provide access to documentation that Software (including third party software and firmware) have appropriate updates and patches installed prior to delivery to Duke Energy, or if Supplier is unable to apply such updates and patches, Supplier shall provide Duke Energy any available updates and patches that should be installed within 7 days after delivery. Documentation shall include instructions for applying the updates and patches.

13.3 For duration of the Agreement, the Supplier shall provide or arrange for the provision of appropriate Software updates and patches to remediate newly discovered vulnerabilities or weaknesses within 30 days. Updates to remediate critical vulnerabilities shall be provided within a shorter period than other updates, within 10 days. If updates cannot be made available by the Supplier within these time periods, the Supplier shall provide mitigations, methods of exploit detection, and/or workarounds within 14 days.

13.4 When third party software and firmware is provided by the Supplier to Duke Energy, the Supplier shall provide or arrange for the provision of appropriate software and firmware updates to remediate newly discovered vulnerabilities or weaknesses, if applicable to Duke Energy's use of the third party product in its system environment, within 30 days. Updates to remediate critical vulnerabilities applicable to Duke Energy's use of third party product in its system environment shall be provided within a shorter period than other updates, within 10 days of availability from the original supplier and/or patching source. If these third party updates cannot be integrated, tested and made available by the Supplier within these time periods, the Supplier shall provide or arrange for the provision of recommended mitigations and/or workarounds within 14 days.

13.5 Supplier 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 Duke Energy. To the extent Supplier is providing third party software or patches, Supplier will use reasonable effort to ensure (a) the third party investigates whether computer viruses or malware are present in any software or patches providing them to Duke Energy or installing them on Duke Energy's information networks, computer systems, and information systems and (b) the third party 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. When install files, scripts, firmware, or other Supplier delivered Software solutions are flagged as malicious, infected, or suspicious by an anti-virus vendor, Supplier must provide or arrange for the provision of technical justification as to why the "false positive" hit has taken place to ensure their code's supply chain has not been compromised. If a virus or other malware is found to have been coded or otherwise introduced as a result Supplier's Software or patches, Supplier shall immediately and at its own cost (i) take all necessary remedial action and provide assistance to Duke Energy to eliminate the virus or other malware throughout Duke Energy's information networks, computer systems, and information systems, regardless of whether such systems or networks are operated by or on behalf of Duke Energy; and (ii) If the virus or other malware causes a loss of operational efficiency or any loss of data (A) where Supplier is obligated under the Agreement to back up such data, take all steps necessary and provide all assistance required by Duke Energy and its affiliates, and (B) where Supplier is not obligated under the 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.

13.6 Unless otherwise approved by Duke Energy in writing, current or supported version of Supplier Software shall (a) 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 purchase, (b) provide support of the latest versions of operating systems on which Software functions within twenty-four (24) months from official public release of that operating system version, and (c) 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.).

14. Supplier Personnel Management.

14.1 The Supplier shall provide access to summary documentation to attest to its workforce receiving position-appropriate cybersecurity training and awareness. This includes specialized training for those involved in the design, development, manufacture, testing, shipping, installation, operation, and maintenance of products or services procured by Duke Energy, as part of the Supplier's Security Program.

15. Secure Hardware and Software Delivery.

15.1 The Supplier shall establish, document, and implement risk management practices for information and communication technology ("ICT") supply chain delivery of Software (including patches). Supplier shall provide access to documentation on its (a) chain-of-custody practices, (b) integrity management program for patches provided by sub-suppliers, (c) instructions on how to request upgrades and patches, and (d) maintenance commitment to ensure that for at least 5 years, or as otherwise agreed to by both parties, patches shall be made available by the Supplier.

15.2 The Supplier 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 Duke Energy deems that it is warranted, the Supplier shall apply encryption to protect procured products throughout the delivery process.

15.3 Supplier 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 Duke Energy to use the hash value as a checksum to independently verify the integrity of the Software and patches and avoid potentially downloading the Software or patches from Supplier's website that has been surreptitiously infected with a virus or otherwise corrupted without the knowledge of Supplier.

15.4 The Supplier shall demonstrate a capability for detecting unauthorized access throughout the delivery process.

16. End-Point Protection.

16.1 The Supplier shall provide either a configured end-point protection solution or access to the information needed for Duke Energy to configure the solution.

17. Cryptographic System Management.

17.1 The Supplier shall make available documentation on how cryptographic system supporting the Suppliers Software procured under the Agreement protects the confidentiality, data integrity, authentication, and non-repudiation of devices and data flows in the underlying system. This documentation shall include, but not be limited to (a) the cryptographic methods (hash functions, symmetric key algorithms, or asymmetric key algorithms) and primitives (e.g., Secure Hash Algorithm (SHA), Advanced Encryption Standard (AES), RSA, and Digital Signature Algorithm (DSA)) that are implemented in the system, and how these methods are to be implemented and (b) the lifecycle management of key establishment, deployment, ongoing validation, and revocation.

17.2 The Supplier shall only use "Approved" cryptographic methods as defined in the Federal Information Processing Standard (FIPS) Security Requirements for Cryptographic Modules (FIPS 140-2).

17.3 The Supplier shall provide an automated remote key-establishment (update) method that protects the confidentiality and integrity of the cryptographic keys.

17.4 The Supplier shall ensure that (a) the system implementation includes the capability for configurable cryptoperiods (the life span of cryptographic key usage) in accordance with current revision of the Suggested Cryptoperiods for Key Types found in Table 1 of NIST 800-57 Part 1, (b) the key update method supports remote re-keying of all devices within 30 days as part of normal system operations, and (c) emergency re-keying of all devices can be remotely performed within 7 days.

17.5 The Supplier shall provide a method for updating or replacing cryptographic primitives or algorithms.

Attachment C - Supplement B
HARDWARE SECURITY SUPPLEMENT

This Hardware Security Supplement applies to any Supplier, which may be referenced in the Agreement as Consultant, Contractor, or Seller, that provides Hardware to Duke Energy. Hardware shall include any information system, operational system, communications system or, other cyber asset computer, device, equipment that may be connected to Duke Energy Internal Network ("Hardware") provided with Supplier's goods, products, or Services.

1. Hardware and Services.

1.1 The Supplier shall provide access to summary documentation of the Hardware's security features and security-focused instructions on product maintenance, support, and reconfiguration of default settings.

2. Access Control.

2.1 The Supplier shall provide access to documentation and recommended methods to prevent unauthorized changes to the Basic Input/Output System (BIOS) and other firmware. If it is not technically feasible to protect the BIOS to reduce the risk of unauthorized changes, the Supplier shall provide documentation of this case and provide mitigation recommendations.

2.2 The Supplier shall verify and, upon Duke Energy's request, provide documentation for the Hardware, attesting that unauthorized logging devices are not installed (e.g., key loggers, cameras, and microphones).

3. Communication Restrictions.

3.1 For IP addressable products, the Supplier shall verify that the procured product allows use of unique routable network address spaces (i.e., address spaces other than 192.168.0.0/16, 172.16.0.0/12, and 10.0.0.0/8 must be supported) that work within Duke Energy's network. Where this is not available, the Supplier shall offer an alternative approach, with mitigating security measures, that is acceptable to Duke Energy.

4. Malware Detection and Protection.

4.1 Upon Duke Energy's request, the Supplier shall provide, or specify how to implement, the capability to automatically scan any removable media that is introduced to Hardware being acquired.

4.2 The Supplier shall ensure that the Hardware product is compatible and supported with Duke Energy current malware detection capabilities. In the event Supplier procured product is not capable of operating with Duke Energy malware detection capabilities, the supplier share obtain Duke Energy approval and implement at least one of the following: (a) Provide a host-based malware detection capability, quarantine (instead of automatically deleting) suspected infected files, provide an updating scheme for malware signatures, and test and confirm compatibility of malware detection application patches and upgrades, (b) if the Supplier is not providing the host-based malware detection capability, the Supplier shall suggest malware detection products to be used and provide guidance on malware detection and configuration settings that will work with Supplier products, or (c) if the Supplier is not providing a host-based malware detection capability, nor suggesting malware detection products, and if specified by Duke Energy, the Supplier shall provide an application whitelisting solution that is tested, validated, and documented that shall only permit approved applications to run.

4.3 The Supplier shall validate that cybersecurity services running on the Hardware (e.g., virus checking and malware detection) do not conflict with other such services running on the Hardware.

5. Heartbeat Signals.

5.1 If Hardware provides heartbeat signal capabilities, the Supplier shall identify heartbeat signals or protocols available, provide packet definitions of the heartbeat signals and examples of the heartbeat traffic, and provide recommendations on which should be included in network monitoring. At a minimum, a last gasp report from a dying component or equivalent shall be included in network monitoring.

6. Reliability and Adherence to Standards.

6.1 The Supplier shall verify that the addition of security features does not adversely affect the solution's ability to meet Supplier benchmarks for performance or service level agreements. Upon request, Supplier shall provide documentation on the test criteria, platforms and results.

7. Secure Development Practices.

7.1 The Supplier shall provide access to summary documentation of its secure product development life cycle including the standards, practices (including continuous improvement), and development environment (including the use of secure coding practices) used to create or modify Supplier-provided Hardware.

8. Vulnerabilities and Material Defects.

Supplier shall develop and implement policies and procedures to address the disclosure and remediation by Supplier of vulnerabilities and material defects related to the products and services provided to Duke Energy under the Agreement including the following:

8.1 Prior to the delivery of the Hardware, Supplier shall provide or direct Duke Energy to an available source of summary documentation of publicly disclosed vulnerabilities and material defects related in the Hardware, the potential impact of such vulnerabilities and material defects, the status of Supplier's efforts to mitigate those publicly disclosed vulnerabilities and material defects, and Supplier's recommended corrective actions, compensating security controls, mitigations, and/or procedural workarounds.

8.2 Supplier shall provide or direct Duke Energy to an available source of summary documentation of vulnerabilities and material defects in the Hardware within seven (7) calendar days after such vulnerabilities and material defects become known to Supplier. This includes summary documentation on vulnerabilities that have not been publicly disclosed or have only been identified after the delivery of the procured 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.

8.3 Whether or not publicly disclosed by Supplier, and notwithstanding any other limitation in the Agreement, Duke Energy may disclose any vulnerabilities or material defects in the procured products and services provided by Supplier to (a) the Electricity Information Sharing and Analysis Center (E-ISAC), the United States Cyber Emergency Response Team (CERT), Department of Homeland Security, or Federal Bureau of Investigation, or any equivalent U.S. governmental entity or program, (b) to any entity when necessary to preserve the reliability of the Bulk Electric System (BES) as determined by Duke Energy in its sole discretion, or (c) any entity required by applicable law.

9. Problem Reporting.

9.1 The Supplier shall provide a secure process for users to submit problem reports and remediation requests. This process shall include tracking history and corrective action status reporting.

9.2 Upon Duke Energy submitting a problem report to the Supplier, the Supplier shall review the report, develop and communicate to Duke Energy an initial action plan, and provide status reports of the problem resolution to Duke Energy at the frequency requested by Duke Energy for the reported problem.

9.3 The Supplier shall provide Duke Energy with access to documentation related to its responsible disclosure and threat reporting policies and procedures (e.g., Computer Emergency Response Teams ("CERTs"), which shall address public disclosure protections implemented by the Supplier.

10. Patch Management and Updates.

10.6 Unless otherwise approved by Duke Energy in writing, current or supported version of Supplier procured Hardware shall (a) not be required to use on end-of-life operating systems, or any operating system that will go end-of-life six (6) months from the date of purchase, (b) provide support of the latest versions of operating systems on which the Hardware functions within twenty-four (24) months from official public release of that operating system version, and (c) 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.).

11. Supplier Personnel Management.

11.1 The Supplier shall provide access to summary documentation to attest to its workforce receiving position-appropriate cybersecurity training and awareness. This includes specialized training for those involved in the design, development, manufacture, testing, shipping, installation, operation, and maintenance of products or services procured by Duke Energy, as part of the Supplier's Security Program.

12. Secure Hardware and Software Delivery.

12.1 The Supplier shall establish, document, and implement risk management practices for supply chain delivery of Hardware. Supplier shall provide access to documentation on its (a) chain-of-custody practices, (b) inventory management program (including the location and protection of spare parts), (c) information protection practices, (d) integrity management program for components provided by sub-suppliers, (e) instructions on how to request replacement parts, and (f) maintenance commitment to ensure that for at least 5 years, or as otherwise agreed to by both parties, spare parts shall be made available by the Supplier.

12.2 The Supplier shall use trusted channels to ship Hardware requiring an authorized signature on delivery.

12.3 The Supplier shall demonstrate a capability for detecting unauthorized access throughout the delivery process.

12.4 The Supplier shall provide access to chain-of-custody documentation for Hardware and require tamper-evident packaging.

13. Wireless Technologies.

If any Hardware from Supplier is provided to Duke Energy under the Agreement have the capabilities to communicate through wireless technologies, Supplier shall:

13.1 Provide access to documentation on specific protocols and other detailed information required for wireless devices to communicate with the Duke Energy network, including other wireless equipment that can communicate with the Supplier-supplied devices.

13.2 Provide access to documentation on use, security capabilities, and limits for the wireless devices.

13.3 Provide access to documentation on the power and frequency requirements of the wireless devices (e.g., microwave devices meet the frequency requirements of Generic Requirements (GR)-63 Network Equipment Building System (NEBS) and GR-1089).

13.4 Provide access to documentation on the range of the wireless devices and verify that the range of communications is minimized to reduce the possibility of signal interception from outside the designated security perimeter.

13.5 Provide access to documentation that the wireless technology and associated devices comply with applicable IEEE standards, such as 802.11.

13.6 Demonstrate, through providing access to summary test data, that known attacks (e.g., those documented in the Common Attack Pattern Enumeration and Classification ("CAPEC") list, such as malformed packet injection, man-in-the middle attacks, or denial-of-service attacks) do not cause the receiving wireless devices to crash, hang, be compromised, or otherwise malfunction.

13.7 Provide access to documentation of the configuration control options that enable varying of the security level of the devices.

14. Cryptographic System Management.

14.1 The Supplier shall make available documentation on how cryptographic system supporting the Suppliers Hardware procured under the Agreement protects the confidentiality, data integrity, authentication, and non-repudiation of devices and data flows in the underlying system. This documentation shall include, but not be limited to (a) the cryptographic methods (hash functions, symmetric key algorithms, or asymmetric key algorithms) and primitives (e.g., Secure Hash Algorithm (SHA), Advanced Encryption Standard (AES), RSA, and Digital Signature Algorithm (DSA)) that are implemented in the system, and how these methods are to be implemented and (b) the lifecycle management of key establishment, deployment, ongoing validation, and revocation.

14.2 The Supplier shall only use "Approved" cryptographic methods as defined in the Federal Information Processing Standard (FIPS) Security Requirements for Cryptographic Modules (FIPS 140-2).

14.3 The Supplier shall provide an automated remote key-establishment (update) method that protects the confidentiality and integrity of the cryptographic keys.

14.4 The Supplier shall ensure that (a) the system implementation includes the capability for configurable cryptoperiods (the life span of cryptographic key usage) in accordance with current revision of the Suggested Cryptoperiods for Key Types found in Table 1 of NIST 800-57 Part 1, (b) the key update method supports remote re-keying of all devices within 30 days as part of normal system operations, and (c) emergency re-keying of all devices can be remotely performed within 7 days.

14.5 The Supplier shall provide a method for updating or replacing cryptographic primitives or algorithms.

Attachment C - Supplement C
HOSTING SERVICES SECURITY SUPPLEMENT

This Hosting Services Security Supplement applies to any Supplier, which may be referenced in the Agreement as Consultant, Contractor, or Seller, that provides or use any managed hosting services in the performance of Services for or on behalf of Duke Energy. Hosting Services shall include, but not limited to, any Cloud Service provider, Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), Application Services Provider (ASP), or any supplier that may otherwise receive, store, or process any Duke Energy data (collectively "Hosting Services").

1. Hosting Services.

1.1 The Supplier shall provide access to summary documentation of the Hosting Services security features and security-focused instructions on access, user configurations, and support.

2. Access Control.

2.1 The Supplier shall configure each component of the Hosting Services environment to operate using the principle of least privilege. This includes operating system permissions, file access, user accounts, application-to-application communications, and information system services. The Supplier shall configure the Hosting Services, or provide Duke Energy documentation detailing how to configure Hosting Services, such that when a session is initiated from a less privileged application, access shall be limited and enforced at the more critical side.

2.2 The Supplier shall provide access to documentation of available options for defining access and security permissions, user accounts, and applications with associated roles. If the Supplier performs the configuration, the Supplier shall configure these options as specified by Duke Energy. User accounts shall allow configurable access and permissions associated with one or more organizationally defined user role(s), where roles are used. If roles are used, the Supplier shall provide a system administration mechanism for changing user(s') role (e.g., group) associations.

2.3 The Supplier shall provide access to documentation describing methods used to prevent unauthorized changes to the Basic Input/Output System (BIOS) and other firmware. If it is not technically feasible to protect the BIOS to reduce the risk of unauthorized changes, the Supplier shall provide documentation of this case and provide mitigation controls implemented.

2.4 The Supplier shall verify and, upon Duke Energy's request, provide documentation for the Hosting Services, attesting that unauthorized logging devices are not installed or utilized (e.g., key loggers, cameras, and microphones).

3. Account Management.

3.1 The Supplier shall provide access to documentation for all accounts (including, but not limited to, generic and/or default) that need to be active for proper operation of the Hosted Services. Where technically feasible, Supplier default accounts not needed for normal or maintenance operations shall be removed or deactivated. When Supplier default accounts cannot be removed or deactivated, then Supplier shall ensure (a) where technically feasible, the account is renamed (b) passwords are changed to complex password controls, (c) usage is limited to only authorized personnel, and (d) accounts are not used for individual access.

3.2 Account password controls must be provided for all accounts unless otherwise agreed to in writing by both parties. Password controls shall include (a) passwords must be complex and have a minimum of 15 characters, (b) passwords must not be easily associated with Duke Energy or any individual person, including but not limited to account name, user name, social security number, employee number, (c) force users to change passwords at least every sixty days, (d) users must not use cyclical or patterned passwords, such as when changing passwords, users must not add a number at the end of the password in sequence, (e) password history controls to disallow the user from reusing one of their passwords previously used in the last 10 password changes, and (f) password changes will have a minimum lifetime of 24 hours. Complex password requirements shall include at least three of the following four characteristics: (1) Uppercase letters (A-Z), (2) Lowercase letters (a-z), (3) Numbers (0-9), and (4) Special characters (i.e. "!, @, #, $, %, ^, &, *, and +).

4. Session Management.

4.1 The Supplier shall not permit user credentials to be transmitted or shared in clear text. The Supplier shall not store user credentials in clear text unless the Supplier and Duke Energy agree that this is an acceptable practice given the protection offered by other security controls. The Supplier shall only allow access protocols that encrypt or securely transmit login credentials (e.g., tunneling through Secure Shell Terminal Emulation ("SSH"), Transport Layer Security ("TLS")).

4.2 Unless specifically requested by Duke Energy, the Supplier shall not allow multiple concurrent logins using the same authentication credentials, allow applications to retain login information between sessions, provide any auto-fill functionality during login, or allow anonymous logins.

4.3 The Supplier shall provide configurable session logout and timeout settings (e.g., alarms and human-machine interfaces).

5. Authentication / Password Policy and Management.

5.1 The Supplier shall provide access to documentation of the levels, methods, and capabilities for authentication and authorization.

5.2 The Supplier shall provide integration with Duke Energy's Active Directory for authentication and authorization or provide a centralized and local account management capability with a configurable account password management system that allows for, but is not limited to, the following: (a) Changes to passwords (including default passwords), (b) Selection of password length, (c) Frequency of change, (d) Setting of required password complexity, (e) Number of login attempts prior to lockout, (f) Inactive session logout, (g) Comparison to a library of forbidden strings, (h) Derivative use of the user name / user ID, and (i) Denial of repeated or recycled use of the same password. The Supplier shall ensure passwords are not stored in clear text and not hardcoded into software or scripts.

5.3 If single-sign on is provided, the Supplier shall (a) ensure that account access for single sign-on is equivalent to that enforced as a result of direct login, (b) use a secure method of authentication (e.g., strong two-factor authentication) to allow single sign-on to a suite of applications, (c) protect key files and access control lists used by the single-sign-on system from non-administrative user read, write, and delete access, (d) I provide access to documentation on configuring a single-sign-on system, as well as documentation showing equivalent results in running validation tests against the direct login and the single sign-on.

6. Logging and Auditing.

6.1 The Supplier shall provide access to a list of all log management capabilities that the Hosted Services is capable of generating, the format of those logs, recommended log management and Security Information and Event Management ("SIEM") integration methods (e.g., syslog) with Duke Energy's existing logging system, and identification of which of those logs are enabled by default. Logging capabilities provided by the Supplier shall cover the following events, at a minimum (as appropriate to their function): (a) Information requests and server responses, (b) Successful and unsuccessful authentication and access attempts, (c) Account changes, (d) Privileged use, (e) Application start-up and shutdown, (f) Application failures, and (g) Major application configuration changes

6.2 The Supplier shall provide standard time synchronization in the Hosted Services (e.g., Global Positioning System ("GPS"), Network Time Protocol ("NTP"), and IEEE 1508-2008). If the Supplier is not providing standard time synchronization and is providing an authoritative time source, the procured product shall be configured to synchronize to the authoritative time source.

6.3 The Supplier shall provide for the confidentiality, integrity, and availability of log files. All audit trails and log files shall include time stamp of each event.

6.4 The Supplier shall provide access to documentation regarding recommended or implemented approach for collecting and retaining logs for a period of time that will provide a complete audit trail should events require a forensics investigation.

7. Communication Restrictions.

7.1 The Supplier shall provide documentation on the design and configuration of network security zones within the Hosted Services.

7.2 The Supplier shall provide access to information on all communications (e.g., protocols) required between network security zones and Duke Energy, whether inbound or outbound, and identify each network component of the Hosted Services initiating communication.

7.3 The Supplier shall provide a method to restrict communication traffic between different network security zones, verify and document that disconnection points are established between the network security zones and provide the methods to isolate the zones to continue limited operations.

7.4 The Supplier shall provide a means to document that network traffic is monitored, filtered, and alarmed (e.g., alarms for unexpected traffic through network security zones) and provide filtering and monitoring rules.

7.5 The basis of all firewall rule sets shall be "deny all," with exceptions explicitly identified by the Supplier.

8. Malware Detection and Protection.

8.1 Upon Duke Energy's request, the Supplier shall implement practices to automatically scan any removable media that is introduced to their network and remove any viruses, malware or other identified threats to Duke Energy information.

8.2 The Supplier shall provide summary documentation of its malware detection capabilities. Capabilities must include at least the following: (a) The Supplier shall quarantine (instead of automatically deleting) suspected infected files, (b) the Supplier shall apply up to date malware signatures, or (c) the Supplier shall test and confirm compatibility of malware detection application patches and upgrades.

9. Secure Development Practices.

9.1 The Supplier shall provide access to summary documentation of its secure product development life cycle including the standards, practices (including continuous improvement), and development environment (including the use of secure coding practices) used to create or modify Supplier-provided Hosted Services.

9.2 The Supplier shall identify the country (or countries) of origin of the Hosted Services and its components (including hardware, software, and firmware). The Supplier shall identify the countries where the development, manufacturing, maintenance, and services are provided. The Supplier shall notify Duke Energy of changes in the list of countries where development, maintenance, and services are provided in support of the Hosted Services. This notification shall occur within 180 days prior to initiating a change in the list of countries.

9.3 Supplier shall implement a Quality Assurance program and validate that the software and firmware of the Hosted Services have undergone Quality Control testing to identify and correct potential cybersecurity weaknesses and vulnerabilities. Supplier shall use positive and appropriate negative tests to verify that the Hosted Services operates in accordance with requirements and without extra functionality, as well as monitor for unexpected or undesirable behavior during these tests. For all web-based applications, interfaces and other modules, the Supplier shall provide access to documentation of all input validation testing including, but not limited to, measures for prevention of command injection, Structured Query Language ("SQL") injection, directory traversal, Remote File Include, Cross-Site Scripting ("XSS"), and buffer overflow. Supplier shall provide access to summary documentation of the results of the testing that includes unresolved vulnerabilities and implemented mitigation measures.

10. Vulnerabilities and Material Defects.

Supplier shall develop and implement policies and procedures to address the disclosure and remediation by Supplier of vulnerabilities and material defects related to the Hosted Services provided to Duke Energy under the Agreement including the following:

10.1 Prior to providing the Hosted Services to Duke Energy, Supplier shall provide or direct Duke Energy to an available source of summary documentation of publicly disclosed vulnerabilities and material defects related in the Hosted Services, the potential impact of such vulnerabilities and material defects, the status of Supplier's efforts to mitigate those publicly disclosed vulnerabilities and material defects, and Supplier's plans for corrective actions, compensating security controls, mitigations, and/or procedural workarounds.

10.2 Supplier shall provide or direct Duke Energy to an available source of summary documentation of vulnerabilities and material defects in the Hosted Services within seven (7) calendar days after such vulnerabilities and material defects become known to Supplier. This includes summary documentation on vulnerabilities that have not been publicly disclosed or have only been identified after the initial usage of the Hosted Services. The summary documentation shall include a description of each vulnerability and material defects and its potential impact, root cause, and plans for corrective actions, compensating security controls, mitigations, and/or procedural workarounds.

10.3 Whether or not publicly disclosed by Supplier, and notwithstanding any other limitation in the Agreement, Duke Energy may disclose any vulnerabilities or material defects in the Hosted Services provided by Supplier to (a) the Electricity Information Sharing and Analysis Center (E-ISAC), the United States Cyber Emergency Response Team (CERT), Department of Homeland Security, or Federal Bureau of Investigation, or any U.S. governmental equivalent entity or program, (b) to any entity when necessary to preserve the reliability of the Bulk Electric System (BES) as determined by Duke Energy in its sole discretion, or (c) any entity required by applicable law.

11. Problem Reporting.

11.1 The Supplier shall provide a secure process for users to submit problem reports and remediation requests. This process shall include tracking history and corrective action status reporting.

11.2 Upon Duke Energy submitting a problem report to the Supplier, the Supplier shall review the report, develop and communicate to Duke Energy an initial action plan, and provide status reports of the problem resolution to Duke Energy at the frequency requested by Duke Energy for the reported problem.

11.3 The Supplier shall provide Duke Energy with access to documentation related to its responsible disclosure and threat reporting policies and procedures (e.g., Computer Emergency Response Teams ("CERTs"), which shall address public disclosure protections implemented by the Supplier.

12. Patch Management and Updates.

12.1 The Supplier shall provide access to documentation of its patch management program and update process (including third party hardware, software, and firmware). This documentation shall include resources and technical capabilities to sustain this program and process. This includes the Supplier's method to verify the integrity of any patch is validated prior to implementation. This documentation shall also include the Supplier's approach and capability to remediate newly reported zero-day vulnerabilities.

12.2 For duration of the Agreement, the Supplier shall provide or arrange for the provision of appropriate software and firmware updates to remediate newly discovered vulnerabilities or weaknesses within 30 days. Updates to remediate critical vulnerabilities shall be provided within a shorter period than other updates, within 10 days. If updates cannot be made available by the Supplier within these time periods, the Supplier shall provide mitigations, methods of exploit detection, and/or workarounds within 14 days.

12.3 When third party hardware, software, and firmware is provided by the Supplier to Duke Energy, the Supplier shall provide or arrange for the provision of appropriate hardware, software, and/or firmware updates to remediate newly discovered vulnerabilities or weaknesses, if applicable to Duke Energy's use of the third party product in its system environment, within 30 days of availability from the original supplier and/or patching source. Updates to remediate critical vulnerabilities applicable to Duke Energy's use of the third party product in its system environment shall be provided within a shorter period than other updates, within 10 days of availability from the original supplier and/or patching source. If these third party updates cannot be integrated, tested and made available by the Supplier within these time periods, the Supplier shall provide or arrange for the provision of recommended mitigations and/or workarounds within 14 days.

12.4 Unless otherwise approved by Duke Energy in writing, Hosted Services shall (a) not reside on end-of-life operating systems, (b) provide support of the latest versions of operating systems on which software functions within twenty-four (24) months from official public release of that operating system version, and (c) not use of out-of-date, unsupported, or end-of-life version of third party components (e.g., Java, Flash, Web browser, etc.).

13. Supplier Personnel Management.

13.1 The Supplier shall provide access to summary documentation to attest to its workforce receiving position-appropriate cybersecurity training and awareness. This includes specialized training for those involved in the design, development, testing, installation, operation, and maintenance of Hosted Services procured by Duke Energy, as part of the Supplier's Security Program.

14. End-Point Protection.

14.1 The Supplier shall provide either a configured end-point protection solution or access to the information needed for Duke Energy to configure the solution.

15. Network Intrusion Detection.

15.1 Supplier must provide guidance on methods to implement, maintain and implement processes designed to ensure that Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS) can effectively monitor and respond to the most recent threats and vulnerabilities. The Supplier shall provide traffic profiles with expected communication paths, network traffic, and expected utilization boundaries for behavior-based (also called anomaly based) Network Intrusion Detection Systems (NIDS).

16. Physical Access to Information System Components.

16.1 The Supplier shall provide lockable or locking enclosures or rooms for information systems and system components (e.g., servers, clients, and networking hardware) and for the systems used to manage and control physical access (e.g., servers, lock controllers, and alarm control panels). The Supplier shall provide a method for tamper detection on lockable or locking enclosures.

16.2 The Supplier shall remove ability for physical access to the systems and facilities from any personnel immediately upon employment termination.

17. Communication Inside the Physical Security Perimeter.

17.1 The Supplier shall verify and provide access to documentation that physical communication channels are secured from physical intrusion.

17.2 The Supplier shall verify and provide access to documentation that communication channels are as direct as possible (e.g., communication paths between devices in the same network security zone do not pass through devices maintained at a lower security level or unnecessarily cross into zones of lower physical security).

18. Cryptographic System Management.

18.1 The Supplier shall make available documentation on how cryptographic system supporting the Suppliers Hosting Services procured under the Agreement protects the confidentiality, data integrity, authentication, and non-repudiation of devices and data flows in the underlying system. This documentation shall include, but not be limited to (a) the cryptographic methods (hash functions, symmetric key algorithms, or asymmetric key algorithms) and primitives (e.g., Secure Hash Algorithm (SHA), Advanced Encryption Standard (AES), RSA, and Digital Signature Algorithm (DSA)) that are implemented in the system, and how these methods are to be implemented and (b) the lifecycle management of key establishment, deployment, ongoing validation, and revocation.

18.2 The Supplier shall only use “Approved” cryptographic methods as defined in the Federal Information Processing Standard (FIPS) Security Requirements for Cryptographic Modules (FIPS 140-2).

18.3 The Supplier shall provide an automated remote key-establishment (update) method that protects the confidentiality and integrity of the cryptographic keys.

18.4 The Supplier shall ensure that (a) the system implementation includes the capability for configurable cryptoperiods (the life span of cryptographic key usage) in accordance with current revision of the Suggested Cryptoperiods for Key Types found in Table 1 of NIST 800-57 Part 1, (b) the key update method supports remote re-keying of all devices within 30 days as part of normal system operations, and (c) emergency re-keying of all devices can be remotely performed within 7 days.

18.5 The Supplier shall provide a method for updating or replacing cryptographic primitives or algorithms.

Attachment C - Supplement D
SERVICES SECURITY SUPPLEMENT

This Services Security Supplement applies to any Supplier, which may be referenced in the Agreement as Consultant, Contractor, or Seller, that (a) has access to Duke Energy Confidential Information, Vendor Network, Internal Network, or (b) provide Services in the development, maintenance, or support of Duke Energy Software.

1. Authentication / Password Policy and Management.

1.1 The Supplier shall ensure all user accounts and passwords are not stored in clear text and not hardcoded into software or scripts.

2. Malware Detection and Protection.

2.1 Upon Duke Energy's request, the Supplier shall implement practices to automatically scan any removable media that is introduced to their network and remove any viruses, malware or other identified threats that could be introduced to Duke Energy information or network.

2.2 The Supplier shall provide summary documentation of its malware detection capabilities. Capabilities must include at least the following: (a) the Supplier shall quarantine (instead of automatically deleting) suspected infected files, (b) the Supplier shall apply up to date malware signatures, or (c) the Supplier shall test and confirm compatibility of malware detection application patches and upgrades.

3. Secure Development Practices.

3.1 The Supplier shall provide access to summary documentation of its secure product development life cycle including the standards, practices (including continuous improvement), and development environment (including the use of secure coding practices) used to create or modify Supplier-provided information system hardware, software, and firmware.

3.2 The Supplier shall identify the country (or countries) of origin of the procured product and its components (including hardware, software, and firmware). The Supplier shall identify the countries where the development, manufacturing, maintenance, and service for the product and Services are provided. The Supplier shall notify Duke Energy of changes in the list of countries where product maintenance or other Services are provided in support of the procured product or Services. This notification shall occur within 180 days prior to initiating a change in the list of countries.

3.3 Supplier shall implement a Quality Assurance program and validate that the software and firmware of the procured product or Services thereto have undergone Quality Control testing to identify and correct potential cybersecurity weaknesses and vulnerabilities. Supplier shall use positive and appropriate negative tests to verify that the procured product operates in accordance with requirements and without extra functionality, as well as monitor for unexpected or undesirable behavior during these tests. For all web-based applications, interfaces and other modules, the Supplier shall provide access to documentation of all input validation testing including, but not limited to, measures for prevention of command injection, Structured Query Language ("SQL") injection, directory traversal, Remote File Include, Cross-Site Scripting ("XSS"), and buffer overflow. Supplier shall provide access to summary documentation of the results of the testing that includes unresolved vulnerabilities and recommended mitigation measures.

4. Vulnerabilities and Material Defects.

4.1 Supplier shall develop and implement policies and procedures to address the disclosure and remediation by Supplier of vulnerabilities and material defects related to the products and Services provided to Duke Energy under the Agreement.

4.2 Whether or not publicly disclosed by Supplier, and notwithstanding any other limitation in the Agreement, Duke Energy may disclose any vulnerabilities or material defects in the procured products and Services provided by Supplier to (a) the Electricity Information Sharing and Analysis Center (E-ISAC), the United States Cyber Emergency Response Team (CERT), Department of Homeland Security, or Federal Bureau of Investigation, or any U.S. governmental equivalent entity or program, (b) to any entity when necessary to preserve the reliability of the Bulk Electric System (BES) as determined by Duke Energy in its sole discretion, or (c) any entity required by applicable law.

5. Problem Reporting.

5.1 The Supplier shall provide Duke Energy with access to documentation related to its responsible disclosure and threat reporting policies and procedures (e.g., Computer Emergency Response Teams ("CERTs"), which shall address public disclosure protections implemented by the Supplier.

6. Patch Management and Updates.

6.1 The Supplier shall provide access to documentation of its patch management program and update process (including third party hardware, software, and firmware). This documentation shall include resources and technical capabilities to sustain this program and process. This includes the Supplier's method or recommendation for how the integrity of the patch is validated by Duke Energy. This documentation shall also include the Supplier's approach and capability to remediate newly reported zero-day vulnerabilities.

6.2 For duration of the Agreement, the Supplier shall provide or arrange for the provision of appropriate software and firmware updates to remediate newly discovered vulnerabilities or weaknesses within 30 days to any equipment used to provide Services. Updates to remediate critical vulnerabilities shall be provided within a shorter period than other updates, within 10 days. If updates cannot be made available by the Supplier within these time periods, the Supplier shall provide mitigations, methods of exploit detection, and/or workarounds within 14 days.

7. Supplier Personnel Management.

7.1 The Supplier shall provide access to summary documentation to attest to its workforce receiving position-appropriate cybersecurity training and awareness. This includes specialized training for those involved in the design, development, manufacture, testing, shipping, installation, operation, and maintenance of products or Services procured by Duke Energy, as part of the Supplier's Security Program.

8. Physical Access to Information System Components.

8.1 The Supplier shall provide lockable or locking enclosures or rooms for information systems and system components (e.g., servers, clients, and networking hardware) where Duke Energy information is stored, accessed, or processed and for the systems used to manage and control physical access (e.g., servers, lock controllers, and alarm control panels). The Supplier shall provide a method for tamper detection on lockable or locking enclosures.

8.2 The Supplier shall remove ability for physical access to the systems and facilities from any personnel immediately upon employment termination.

Purchase Order

Mail Invoice To:

Follow Invoice Instructions
As Shown Below

Purchase Order	:	**03209687**
Revision	:	
Printed	:	**11/20/2025**
Issue Date	:	**11/20/2025**

Report Criteria

File Name, URL, DBServer & DB: Report Name: ST3937 Purchase Order Report
Report URL: http://NUCWRPTWEBP7:80/ReportServer
Server Name: NUCWDBDWP2\PROD
Database: Passport_ODS

UserID: NAM\NucNASCRP_SVC_p

Parameters: PONumber: 03209687

SQA Qualified Report, Commensurate with SWQL C