FirstEnergy Information Assets Access Agreement

This Information Assets Access Agreement ("Access Agreement") is made and entered into by and between Supplier Display Name ("USER") with principal executive offices at Supplier Primary Address Street1, Supplier Primary Address City, Supplier Primary Address State Supplier Primary Address Postal Code on behalf of its employees effective as of Contract Start Date and FirstEnergy Service Company, for itself and on behalf of its affiliates ("COMPANY") with principal executive offices at 76 S. Main St., Akron, OH 44308.

WHEREAS, both USER and COMPANY agree that in order to perform "Work" (defined below) under ***[INSERT NAME OF MASTER SERVICE AGREEMENT between USER and COMPANY]*** ("MSA") USER needs access to COMPANY's Information Assets. As needed, the COMPANY is granting USER controlled and limited access to COMPANY'S Information Assets; and,

WHEREAS, USER recognizes and agrees the COMPANY'S Information Assets are valuable and sensitive assets of the COMPANY and may be severely damaged by misuse, even inadvertent misuse; and

WHEREAS, USER agrees that the COMPANY is required by law to protect its Information Assets and communications assets by requiring USER to be bound to the terms and conditions of this Access Agreement; and

WHEREAS, COMPANY will not allow any USER to access COMPANY'S Information Assets without assuming the obligations described below; and

NOW THEREFORE, in consideration of the COMPANY granting access to and USER agreeing to only access COMPANY'S Information Assets as specified and limited herein, and after acknowledging the accuracy of the foregoing recitals, the parties hereby agree to the following:

1. Definitions.
   (a) "Breach of Security" means unauthorized access to, acquisition of, or disclosure of, PII or any individual's information which was held in the custody or control of USER, or a reasonable belief by either party that such unauthorized access, acquisition, or disclosure has occurred.

   (b) "Data Protection Laws" means all applicable international, federal, state, provincial, and local laws, rules, regulations, directives, requirements, codes, and industry standards and guidelines, relating to the privacy, confidentiality, integrity, protection, or security of PII.

   (c) "Information Assets" shall be defined (per FirstEnergy's Cyber Security Program) as: A technology resource including electronic information, software, computing devices, network devices, or communication services used to create, modify, retrieve, transmit, or store information that:

   (i) Contains COMPANY non-public information, or;

   (ii) Is a COMPANY-owned asset, or;

   (iii) Is an asset operated by a third party that COMPANY grants access to USER to perform or fulfill Work contracted for by the COMPANY.

   (d) "Personally Identifiable Information" or "PII" means any information that identifies, relates to, describes, is reasonably capable of being associated with a particular individual or household, that is accessed or processed by USER pursuant to this Access Agreement, and that is deemed "personal data," "personal information," or the like under the Data Protection Laws.

   (e) "Work" means all goods, parts, materials, equipment, services, labor, data, and other obligations covered by, contemplated or intended for USER to supply or perform under a MSA or other agreement, as specified in the MSA or other agreement, together with miscellaneous expendable job supplies, installation-related equipment and/or tools, transportation, facilities and/or services necessary for USER to complete its obligations under a MSA or other agreement.

2. Access to COMPANY'S Information Assets. In consideration of and reliance upon USER assuming the obligations described herein, the COMPANY agrees to allow USER access to COMPANY'S Information Assets based on the COMPANY'S business need to complete Work, in one or more of the following manners:

   (a) Establish a remote access connection to the COMPANY'S Information Assets using a COMPANY-owned device provided to USER'S employees and using such COMPANY-OWNED device's associated remote access system;

   (b) Establish a remote access connection to the COMPANY'S Information Assets using USER-owned devices via a secure remote access terminal system from which information extraction is technically restricted. If such access is granted by COMPANY, USER agrees to configure all USER computer systems used to access COMPANY Information Assets in accordance with: (i) any technical standards provided to USER in writing; and (ii) COMPANY'S Exhibit A "Acceptable Use Practice for Accessing FirstEnergy Information Assets" (hereinafter "Exhibit A"), including any modifications thereto located at FE GRACE (rsa.com) which USER agrees to access from time to time;

(c) Establish per-service access to the COMPANY'S Information Assets using COMPANY-supplied credentials to USER;

(d) Establish site-to-site Virtual Private Network (VPN) connections between COMPANY and USER'S networks for the purposes of using the COMPANY'S Information Assets, or to securely transfer data between the parties. If such access is granted by COMPANY, USER agrees to configure all USER computer systems used to access COMPANY'S Information Assets in accordance with: (i) any technical standards provided to USER in writing; and (ii) Exhibit A, including any modifications thereto located at FE GRACE (rsa.com) which USER agrees to access from time to time;

Regardless of the type of access provided, USER is subject to strict compliance with the COMPANY'S security procedures and standards as the same may be deemed given to USER by USER accessing FE GRACE (rsa.com) from time to time. The current COMPANY security procedures and standards are detailed in Exhibit A and are incorporated herein by reference. The COMPANY may modify Exhibit A at any time and USER agrees that such modified security procedures and standards shall become part of this Access Agreement.

3. Denial of Access. The COMPANY reserves the right to deny or disable access to Information Assets at any time, without Notice (defined in Article 13.9), for its own convenience. The COMPANY shall deny or disable access to Information Assets without any prior Notice if USER does not implement and certify its implementation of the security procedures and standards set forth in Exhibit A and in any Notice within the applicable time specified in Exhibit A. Any denial or disabling of access to Information Assets shall be without prejudice to any other rights or remedies that the COMPANY may have in law or equity. Such denial or disabling of access to Information Assets shall not constitute a breach of this Access Agreement, or (if applicable) to any MSA or other agreement this Access Agreement supports, or any other obligation of the COMPANY to USER and, unless otherwise agreed, USER shall continue to perform its obligations under any MSA or other contract or agreement without interruption or delay.

4. Exceptions. If USER believes it cannot implement a Directive within the time required without adversely affecting its own network(s) or business, it may so inform the COMPANY by Notice, and the COMPANY will attempt to resolve USER concerns while still protecting Information Assets. The COMPANY may, in its sole and absolute discretion, allow USER to adopt measures equivalent in effectiveness to those to which exception has been taken. Such action on the part of the COMPANY shall not constitute a waiver or course of dealing that would permit the USER to avoid the implementation of any other Directive. Prior to denying access, the COMPANY is not obligated to extend the deadline for implementation of any Directive, to address or resolve USER'S concerns in a manner acceptable to USER, or at all. The COMPANY'S Chief Information Security Officer or authorized delegate shall make the final decision on any exception requested by USER.

5. Non-Use, Non-Disclosure Related to Information Assets Access.

(a) USER agrees and acknowledges that in the course of accessing COMPANY'S Information Assets, USER may either come to possess or be in possession of COMPANY'S Confidential Information. COMPANY'S "**Confidential Information**" includes Personally Identifiable Information ("PII"), scientific and technical information, data, formulas, devices, concepts, inventions, designs, drawings, methods, techniques, computer software, screens, user interfaces, system designs and documentation, marketing and commercial strategies, information concerning COMPANY'S or any of its affiliates' employees, customers, or suppliers, processes, data concepts, and know-how, and unique combinations of separate items that individually may or may not be confidential, which information is not generally known to the public and either derives economic value (actual or potential) from not being generally known, or has a character such that COMPANY or any of its affiliates has an interest in maintaining its secrecy.

(b) USER agrees to hold in confidence in the same manner as it holds its own Confidential Information; but in no event less than a commercially reasonable manner, all of COMPANY'S Confidential Information to which it has access pursuant to the Access Agreement. USER shall not use or disclose COMPANY'S Confidential Information for any reason or purpose without the prior written consent of the COMPANY. Notwithstanding the foregoing sentence, if applicable, USER may use Confidential Information for the sole purpose of the performance of Work for the benefit of the COMPANY without obtaining COMPANY'S prior written consent.

(c) Access to COMPANY'S Confidential Information shall be restricted to USER employees: (i) who have a need to know such information in connection with any Work; and (ii) for whom a Form No. X-3788 (*Contractor Background Request*) (or any successor form) has been completed; *provided that* COMPANY retains discretion to reject access for any such USER employee whom COMPANY deems to pose a threat to the security or integrity of COMPANY's Confidential Information or Information Assets (or as otherwise required or permitted by applicable law or regulation).

(d) All Confidential Information, including any copies thereof, in any media in the possession or control of the USER and all Confidential Information embodied or included in any software or data files loaded or stored on Information Assets in the possession or control of the USER shall be removed by USER and returned to COMPANY either upon demand, or if applicable no later than the completion of Work for COMPANY.

(e) USER shall not copy the Confidential Information in whole or in part or use all or any part of the Confidential Information to reverse engineer, duplicate the function, sequence or organization of the Information Assets for any purpose without the prior written permission of the COMPANY.

(f) Except for PII, the restrictions set forth in this Article shall not apply to information that: (i) is or has become generally known to, or readily ascertainable by, the public without the fault or omission of the USER or its employees; or (ii) was already known to USER prior to the first disclosure of such information to USER by COMPANY; or (iii) was received by USER without

restrictions as to its use from a third party who is lawfully in possession and not restricted as to the use thereof; or (iv) is required to be disclosed by law or by order of a court of competent jurisdiction; or (v) was independently developed by USER through persons who have not had, either directly or indirectly, access to or knowledge of similar information provided by COMPANY.

(g) Regarding PII, USER shall implement appropriate measures to ensure the security and confidentiality of all PII in its possession, including protecting against any threats or hazards to the security or integrity of the PII that USER should reasonably be able to anticipate, and against unauthorized access to or use of the PII. To the extent that USER has PII in their possession, USER shall implement a comprehensive written information security program containing organizational, administrative, physical and technical security measures that satisfies all relevant state and federal laws and regulations. USER shall allow COMPANY to review USER'S comprehensive written information security program as well as any audit reports, summaries of test results, or other documents related to security measures taken by USER, and, as deemed necessary by COMPANY, inspect the implementation of associated administrative, physical and technical security measures, as the case may be, to assess whether USER'S written information security program complies with information security requirements set forth by regulations. Such inspections will not include: (i) access by COMPANY to Confidential Information of USER'S other customers; or (ii) direct access to any USER systems.

(h) USER shall notify COMPANY within one (1) business day of becoming aware of any Breach of Security. USER'S Notice shall include the following: (i) date and time that USER discovered the Breach of Security and the date and time when the breach actually occurred, if discoverable; (ii) a detailed description of the Breach of Security; (iii) a list of the systems and data at risk, including a list of affected individuals; and (iv) a description of actions taken after the Breach of Security was discovered. Thereafter, USER shall provide COMPANY with periodic updates describing the investigation into the Breach of Security and all corrective or remedial actions taken or to be taken by USER.

(i) COMPANY may, in its sole discretion, take any and all actions necessary or reasonable to respond to a Breach of Security involving PII, including but not limited to conducting an investigation into the cause of the Breach of Security involving PII and notifying affected persons or government agencies accordingly. USER shall provide the COMPANY with all information reasonably necessary to: (i) aid COMPANY'S compliance with all Data Protection Laws and any other laws or regulations that may be applicable to a Breach of Security involving PII; and (ii) facilitate COMPANY'S determination of whether the breach was effectively mitigated. USER shall bear all costs and expenses incurred by COMPANY related to the Breach of Security of PII and compliance with law. Alternatively, USER may take action to remedy the Breach of Security involving PII at USER'S sole expense. This may include, for example, sending notice to all individuals affected by the Breach of Security of PII. For the sake of clarity, COMPANY shall make the final decision how and whether to notify third parties of any such Breach of Security, including individuals, law enforcement or governmental authorities, and/or the general public of such Breach of Security. Unless required to do so by applicable law, USER agrees that it will not inform any third party of any Breach of Security incident to the extent that it may be associated with or linked to COMPANY without first obtaining COMPANY'S prior written consent, other than to inform a complainant that the matter has been forwarded to COMPANY'S legal counsel.

(j) If USER is requested or required (by interrogatories, governmental request for information, request for production of documents, subpoena, Civil Investigative Demand or similar process, or otherwise required by applicable law) to disclose any COMPANY Confidential Information, USER shall provide COMPANY with prompt Notice of such request(s) so COMPANY may seek an appropriate protective order and USER shall use appropriate efforts to limit the disclosure and maintain confidentiality to the maximum extent possible.

(k) If USER breaches or threatens to breach this Article, the parties acknowledge that there may exist no adequate remedy at law, and hereby agree that COMPANY shall have the right to seek temporary and permanent injunctive relief to restrain a violation of this Article, without the necessity of posting a bond. COMPANY'S right to injunctive relief shall be cumulative and in addition to its right to seek and obtain other remedies, including monetary damages.

6. Compliance Audit Related to Information Assets Access. In the event that the COMPANY in its sole discretion reasonably concludes, that USER or any individual for whom it is responsible has breached its obligations under this Access Agreement, the COMPANY may at any time upon reasonable Notice request an audit be conducted by an independent third party to certify USER'S obligations under this Access Agreement have not been breached.

7. Notice of Unauthorized Access

   (a) USER shall notify the COMPANY by email and telephone as soon as possible but no later than twenty-four (24) hours of any breach of the security procedures and standards set forth in Exhibit A, any unauthorized access to Information Assets, or the introduction of any malicious code, such as, but not limited to, a virus, worm, malware, ransomware, backdoor, or undisclosed executable file into COMPANY'S Information Assets.

   (b) USER agrees to request access rights to COMPANY'S Information Assets only for USER'S employees for whom a Form No. X-3788 (Contractor Background Request) (or any successor form) has been completed; provided that COMPANY retains discretion to reject access for any such USER employee whom COMPANY deems to pose a threat to the security

or integrity of COMPANY's Confidential Information or Information Assets (or as otherwise required or permitted by applicable law or regulation).

8. DISCLAIMER OF WARRANTIES RELATED TO INFORMATION ASSETS ACCESS. ACCESS TO COMPANY'S INFORMATION ASSETS (AND ANY AND ALL HARDWARE, SOFTWARE, AND OTHER COMPONENTS THEREOF) IS PROVIDED "AS-IS" WITH NO WARRANTIES, EITHER EXPRESS OR IMPLIED. THE COMPANY HEREBY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT IN CONNECTION WITH THE PROVISION OF INFORMATION ASSETS ACCESS TO USER. USER ACKNOWLEDGES AND ACCEPTS ALL RISKS ASSOCIATED WITH ITS ACCESS TO AND USE OF THE COMPANY'S INFORMATION ASSETS.

9. USER'S INDEMNIFICATION OBLIGATIONS.
TO THE FULLEST EXTENT OF THE LAW, USER AGREES TO DEFEND, INDEMNIFY, AND HOLD HARMLESS THE COMPANY, ITS PARENT, SUBSIDIARIES, AND AFFILIATES, AND EACH OF THEIR RESPECTIVE OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUCCESSORS, AND ASSIGNS FROM AND AGAINST ANY AND ALL LOSSES, COSTS, EXPENSES, DAMAGES, CLAIMS, LIABILITIES, JUDGMENTS, FINES, OR PENALTIES (HEREINAFTER "LOSSES") ARISING OUT OF USERS' ACCESS TO THE COMPANY'S INFORMATION ASSETS; ANY USE OF THE COMPANY'S INFORMATION ASSETS BY USER; A BREACH OF SECURITY; OR THE BREACH OF THIS ACCESS AGREEMENT BY USER.

10. INSURANCE

A. USER'S Insurance. USER shall secure and maintain in force minimum policies of insurance of the types listed below and shall furnish to COMPANY, prior to accessing COMPANY'S Information Assets and throughout the duration of such access, certificates of insurance evidencing current coverage listed below (collectively, the "**Policies**").

1. Commercial General Liability (CGL) insurance including products-completed operations, independent contractors, and contractual liability coverages with minimum limits of $2,000,000 per occurrence, combined single limit for bodily injury (including disease or death), personal injury, and property damage (including loss of use) liability.
2. Automobile Liability insurance, including non-ownership and hired car endorsement, with minimum limits of $1,000,000 per occurrence, combined single limit.
3. Worker's Compensation coverage in the statutory amounts under the worker's compensation act(s) of the location(s) in which the Work is to be performed, for the current period.
4. Employer's Liability with a minimum limit of $1,000,000 for each accident or illness.
5. Cyber Liability Insurance with limits not less than $2,000,000 per occurrence.

Any of the above per-occurrence limits may be satisfied by a combination of primary and excess liability coverage.

B. Additional Insured. FirstEnergy Corp. and its subsidiaries and affiliates shall be included by USER as an additional insured to the Policies for the portion of any losses resulting from, or related to, the USER'S sole or concurrent negligence. The Policies shall provide primary and non-contributory coverage in relation to any insurance COMPANY carries for the same losses, and include a separation of insured's provisions. The limits of liability specified for the required insurance coverage herein are the minimum limits of liability that must be carried by USER. The limits of insurance required herein will in no way be deemed to limit any liabilities or obligations assumed by USER hereunder or under applicable law, except as provided by statute. A copy of the endorsement adding FirstEnergy Corp. and its subsidiaries and its affiliates as an additional insured (blanket endorsement is acceptable) shall be attached to the certificate of insurance providing general liability coverage.

C. Lapse of Coverage. The Policies shall not be canceled or allowed to lapse, and no material change shall be made altering, restricting or reducing the insurance provided or changing the name of the insured without giving immediate Notice in writing to *FirstEnergy Service Company, Insurance Risk Management, 76 South Main Street, Akron, Ohio 44308*, with receipt of Notice acknowledged. In the event of cancellation or lapse of or prohibited change in any Policy, COMPANY shall have the right to suspend USER'S access to COMPANY'S Information Assets until the Policy and certificates in evidence thereof are reinstated or arrangements acceptable to COMPANY are made pending issuance of new Policies and certificates. If any Policy shall be about to lapse or be canceled, USER shall obtain a new Policy with like coverage, and if USER fails to do so, COMPANY may terminate the Access Agreement.

D. Waiver of Subrogation. USER hereby waives (and any of its subcontractors shall waive) any rights of subrogation they or any of their insurers may have against COMPANY and each non-affiliated company disclosed in the Access Agreement, their respective agents or employees.

11. LIMITATION OF LIABILITY

IN NO EVENT WILL THE COMPANY BE LIABLE FOR ANY LOSSES ARISING OUT OF: USERS' ACCESS TO THE COMPANY'S INFORMATION ASSETS; ANY DAMAGES RESULTING FROM ANY DELAY, OMISSION, OR ERROR IN THE ELECTRONIC TRANSMISSION OR RECEIPT OF DATA; ANY FORCE MAJEURE EVENT; ANY USE OF

THE COMPANY'S INFORMATION ASSETS BY USER; A BREACH OF SECURITY; OR THE BREACH OF THIS ACCESS AGREEMENT BY USER, INCLUDING ANY LOSSES THAT ARE CATEGORIZED AS BEING DIRECT, SPECIAL, PUNITIVE, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES (INCLUDING LOSS OF USE, DATA, BUSINESS OR PROFITS) WHETHER SUCH LIABILITY ARISES FROM ANY CLAIM BASED UPON CONTRACT, WARRANTY, TORT (INCLUDING NEGLIGENCE), AND PRODUCT LIABILITY OR OTHERWISE, AND WHETHER OR NOT THE COMPANY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

12. TERMINATION; MODIFICATION

USER acknowledges and agrees that COMPANY has the right to immediately terminate this Access Agreement, or any access granted to USER, at any time with or without cause. COMPANY may modify the terms and conditions of this Access Agreement at any time upon thirty (30) days' written Notice to USER. If USER does not wish to continue its access to the COMPANY'S Information Assets under such modified terms and conditions, USER may terminate this Access Agreement by written Notice delivered to COMPANY prior to the effective date of the modification.

13. MISCELLANEOUS RELATED TO INFORMATION ASSETS ACCESS.

13.1 This Access Agreement constitutes the entire agreement between the parties with respect to accessing COMPANY's Information Assets and supersedes any prior understanding or agreement relating to the same subject matter.

13.2 This Access Agreement may not be modified unless approved in writing by COMPANY.

13.3 Severability. If for any reason a court of competent jurisdiction finds any provision or portion of this Access Agreement to be unenforceable, that provision of the Access Agreement will be enforced to the maximum extent permissible so as to effect the intent of the parties, and the remainder of this Access Agreement will continue in full force and effect.

13.4 Waiver. The failure of any party to enforce any of the provisions of this Access Agreement will not be construed to be a waiver of the right of such party thereafter to enforce such provisions.

13.5 Assignment. USER may not assign any Information Assets access granted under this Access Agreement, in whole or in part, including by operation of law. COMPANY may assign or otherwise transfer this Access Agreement to an affiliate or subsidiary without the prior consent of USER.

13.6 Relation to Other Agreements. In case of any conflict between the provisions of the MSA or other agreements of the parties and this Access Agreement, the provisions of this Access Agreement shall control as to the USER'S access to COMPANY'S Information Assets.

13.7 Gifts and Gratuities/Conflicts of Interest. COMPANY'S employees are subject to conflicts of interest and gifts and gratuities policies, which generally prohibit such employees and/or their family members from giving or receiving gifts, favors, services, or privileges (including travel, entertainment, and discounts that would not be available to the general public) from existing or potential customers, suppliers, or contractors that: (1) have more than a nominal value; (2) exceed the level of standard business courtesies; or (3) the acceptance of cash, gift certificates, or loans in any amount. The conflicts of interest policy generally prohibits COMPANY'S employees and/or their family members from serving as an officer, director, employee, consultant, agent of, or from owning any beneficial interest in an organization having a business relationship with COMPANY as a supplier or contractor, if the COMPANY employee is in a position to influence decisions concerning the relationship. The entire text of these policies may be found within the COMPANY'S Supply Chain Section at https://www.firstenergycorp.com/supplychain.html. USER and prospective suppliers to COMPANY are expected to be aware of these policies in their dealings with COMPANY'S employees and their family members. *Any suspected or actual violations of these policies should be reported; and, may be reported anonymously and confidentially by a customer, supplier, contractor, or employee by calling the FirstEnergy Employee Concerns Line (1-800-683-3625), 24 hours a day, 7 days a week.*

13.8 Jurisdiction; Governing Law. The parties agree to the jurisdiction of the federal or state courts located in Summit County, Ohio and that the laws of the State of Ohio shall apply to the interpretation and construction of this Access Agreement for both substantive and procedural matters without giving effect to its rules regarding conflicts of laws.

13.9 Notice.

If Notice is to the COMPANY:
FirstEnergy Service Company
76 S. Main Street
Akron, OH 44308
Supplier Primary Address Postal Code
ATTN: Supply Chain, A-GO-9
Phone: 330-384-2424

And

If Notice is to USER: Supplier Display Name
Name:
Address: Supplier Primary Address Street1
City, State, Zip: Supplier Primary Address City, Supplier Primary Address State

ATTN:
Phone:
Fax:

FirstEnergy Service Company
Chief Information Security Officer
76 S. Main St.
Akron, OH 44308
ATTN: Chief Information Security Officer A-GO-18
Phone: 330-761-4700 (24/7 Security Operations Center watch number)

13.10 Survival. In addition to those rights and obligations which by their nature would survive termination or expiration the following provisions of this Access Agreement shall survive any termination or expiration: Articles related to: Non-Use, Non-Disclosure Related to Information Assets Access; Disclaimer of Warranties Related to Information Assets Access; USER'S Indemnification Obligations; Limitation of Liability; and Miscellaneous Related to Information Assets Access.

13.11 This Access Agreement may be executed simultaneously in two (2) or more counterparts, each of which will be considered an original, but all of which together will constitute one and the same instrument. Execution and delivery of this Access Agreement may be evidenced by facsimile transmissions and will be sufficient to bind the parties to the terms and conditions of this Access Agreement.

IN WITNESS WHEREOF, the parties hereto have executed this Information Assets Access Agreement, by their duly authorized representatives below.

FirstEnergy Service Company (COMPANY)	Supplier Display Name (USER)
_____	_____
Name: _____	Name:_____
Title: _____	Title: _____

EXHIBIT A

ACCEPTABLE USE PRACTICE FOR THIRD PARTIES ACCESSING FIRSTENERGY INFORMATION ASSETS

Last Modified: [08-07-2023]

1. Introduction

FirstEnergy Service Company (the "**COMPANY**," "**we**," "**us**", "**our**") provides access to its Information Assets to USER ("**you**" or "**your**") on a short-term basis as a courtesy and convenience to you on an as-is basis. Use of our Information Assets is at your own risk. Capitalized terms used but not defined herein have the same meanings as ascribed to such terms in the FirstEnergy Information Assets Access Agreement ("Access Agreement").

This Acceptable Use [PRACTICE] (this "**AUP**"), along with the Access Agreement (as applicable), governs your access to and use of our Information Assets. COMPANY reserves the right to amend, alter, or modify your conduct requirements as set forth in this AUP at any time. By executing the Access Agreement, you accept and agree to be bound and abide by this AUP. If you do not want to agree to this AUP, you must not access or use our Information Assets.

2. Implementation of Security Procedures.

You must, prior to establishing any connection to our Information Assets, implement and comply with the following policies, security procedures and standards:

(a) Background Checks

USER hereby represents and warrants that each USER employee with access to our Information Assets has had a background check consisting of, at a minimum, an identity verification (e.g. Social Security Number verification in the U.S.) and a seven (7) year criminal check that revealed no evidence of a criminal conviction; and that, to the best of USER's knowledge, each such USER employee does not pose a threat to the security or integrity of COMPANY's Information Assets. To the extent that USER becomes aware of any such potential threat to COMPANY's Information Assets, USER shall immediately remove such USER employee from accessing our Information Assets and USER shall provide immediate Notice to COMPANY. At any time during access to our Information Assets, COMPANY may request USER to verify that its USER employees are in compliance with the background check requirements set forth herein.

Each such USER employee must have completed *FirstEnergy Form X-3788 Contractor Background Request* (REV 05-23 or later) prior to any access being granted to our Information Assets or any COMPANY-owned devices being provided, *provided that* COMPANY retains discretion to reject access for any such USER employee whom COMPANY deems to pose a threat to the security or integrity of COMPANY's Confidential Information or Information Assets (or as otherwise required or permitted by applicable law or regulation).

(b) Internet Use Policy

You agree that any use of the Internet or electronic communications as provided by us will be solely for business purposes. Your use of Internet or electronic communications provided by us is covered by *FirstEnergy Business Practice 9.4 Electronic Mail, Voice Mail, Internet, Internal Web, and Messaging Services*. We reserve the right to monitor your use of the Internet and electronic communications to assure compliance with these policies and standards at any time and without Notice.

(c) Remote Access Security

All access to our Information Assets must be in accordance with our policies regarding system, access, and cryptographic security requirements. All network traffic may be monitored by us at any time and without Notice. USERS accessing Information Assets and not using COMPANY-owned equipment must use reasonably secured endpoints with industry-standard security technologies and protections applied, provided, and managed by the Supplier of the Work.

Remote access using individually assigned accounts is non-delegable by USER to anyone else. USERS are prohibited from using remote access technologies not provided or approved by COMPANY to expose, proxy, or remotely control active connections to our Information Assets.

(d) Security of COMPANY-owned devices provided to USER

If COMPANY-owned devices are provided, you may not disable or tamper with any security setting or software on the provided Information Asset, including but not limited to anti-virus/anti-malware software, log aggregation, log forwarding, security auditing, and endpoint incident response.

(e) Security of USER-owned devices accessing Information Assets

If USER-owned devices are used to access Information Assets, you must deploy COMPANY-approved anti-virus/anti-malware protection software on all general-purpose computing platforms used by you to connect to our Information Assets.

(f) Security of COMPANY-provided individual accounts

When the COMPANY provides USER with individual accounts, you shall not share or otherwise disclose passwords, multi-factor codes, or other such security-related information to any person other than to the individual for whom the account was granted. This includes USER information technology support staff or other security support staff.

USER individual accounts that access our Information Assets are governed by the FirstEnergy Cyber Security Policy or its successor policy document. As noted, COMPANY retains discretion to reject access to any USER employee whom COMPANY deems to pose a threat to the security or integrity of COMPANY's Confidential Information or Information Assets (or as otherwise required or permitted by applicable law or regulation).

(g) Training for access to Information Assets

COMPANY may require initial and ongoing training of USER'S employees with access to our Information Assets. Such training may be required on a periodic basis to maintain ongoing access to our Information Assets. USER acknowledges that USER'S employees will complete such training in a timely and efficient matter when so required by us. We agree that training will be limited to such training that is identified by us as fulfilling requirements for the COMPANY to remain in compliance with various federal and state regulatory and legal requirements.

(i) Malicious Code. USER shall not: (i) introduce any malicious or surreptitious code into our Information Assets, including any virus, worm, malware, ransomware, backdoor, or undisclosed executable file; (ii) use any means to circumvent any COMPANY system security measure; (iii) attempt to access any COMPANY system resource that we have not authorized for USER'S access.

(j) Third Party Access. Except for "Work" as specified in a MSA or other agreement, USER shall not allow any third party, including but not limited to subcontractors, temporary employees or, in the case where USER is a business entity, other persons who are not full-time employees of USER, to access our Information Assets through USER'S computer systems or networks unless specifically authorized by the COMPANY in writing. We, in our sole discretion, may require such other person or persons to separately execute a copy of our Access Agreement prior to granting access to our Information Assets. USER shall take all steps necessary to secure its own networks and its access to our Information Assets to prevent any person not authorized by the COMPANY from gaining access to our Information Assets.

3. Prohibited Uses

You may use our Information Assets only for lawful purposes and in accordance with this AUP. You agree not to use our Information Assets:

(a) In any way that violates any applicable federal, state, local, or international law or regulation (including, without limitation, any laws regarding the export of data or software to and from the U.S. or other countries).

(b) For the purpose of exploiting, harming, or attempting to exploit or harm, minors in any way by exposing them to inappropriate content, asking for their Personally Identifiable Information, or otherwise.

(c) To send, knowingly receive, upload, download, use, or re-use any material which violates the rights of any individual or entity established in any jurisdiction.

(d) To transmit, or procure the sending of, any advertising or promotional material, including any "junk mail," "chain letter," "spam," or any other similar solicitation.

(e) To impersonate or attempt to impersonate the COMPANY, a COMPANY employee, another user, or any other person or entity (including, without limitation, by using e-mail addresses or screen names associated with any of the foregoing).

(f) To engage in any other conduct that restricts or inhibits anyone's use of our Information Assets, or which, as determined by us, may harm the COMPANY or users of our Information Assets or expose them to liability.

Additionally, you agree **not** to:

(g) Use our Information Assets in any manner that could disable, overburden, damage, or impair our Information Assets or

interfere with any other party's use of our Information Assets, including their ability to engage in real time activities through our Information Assets.

(h) Use any robot, spider, or other automatic device, process, or means to access our Information Assets for any purpose, including monitoring or copying any traffic on our Information Assets or resources available on our Information Assets.

(i) Use any manual process to monitor or copy any traffic on our Information Assets or for any other unauthorized purpose without our prior written consent.

(j) Use any device, software, or routine that interferes with the proper working of our Information Assets, or any server, computer, database, or other resource or element connected to our Information Assets.

(k) Violate, attempt to violate, or knowingly facilitate the violation of the security or integrity of our Information Assets.

(l) Otherwise attempt to interfere with the proper working of our Information Assets.

(m) To damage, destroy, or otherwise render unusable or unrecoverable any COMPANY information.

(n) Connect any device or peripheral to an Information Asset, including any COMPANY-owned endpoint provided to the USER, that is not owned by COMPANY or has been otherwise approved by the COMPANY.

(o) Use any Information Asset to connect to a third party's system for purposes other than fulfillment of "Work" as specified in a MSA or other agreement or for limited personal use as described in *FE Business Practice 9.5 Personal Use of Computer Equipment and Software Practice* or its successor practice document.

4. <u>Content Standards</u>

You agree not to use our Information Assets to send, knowingly receive, upload, download, use, or re-use any material which:

(a) Contains any material that is defamatory, obscene, indecent, abusive, offensive, harassing, violent, hateful, inflammatory, or otherwise objectionable.

(b) Promotes sexually explicit or pornographic material, violence, or discrimination based on race, sex, religion, nationality, disability, sexual orientation, or age.

(c) Infringes any patent, trademark, trade secret, copyright, or other intellectual property, or other rights of any other person.

(d) Violates the legal rights (including the rights of publicity and privacy) of others or contains any material that could give rise to any civil or criminal liability under applicable laws or regulations.

(e) Is likely to deceive any person.

(f) Promotes any illegal activity, or advocates, promotes, or assists any unlawful act.

(g) Impersonates any person, or misrepresents your identity or affiliation with any person or organization.

(h) Involves commercial activities or sales, such as contests, sweepstakes, and other sales promotions, barter, or advertising.

(i) Gives the impression that they emanate from or are endorsed by COMPANY or any other person or entity, if this is not the case.

5. **<u>Revision of Security Procedures and Standards</u>**

COMPANY may from time-to-time revise requirements in the AUP. USER will implement and maintain the requirements of such

revisions within the time frames set forth below depending on the nature of the instructions (the "Directives") in the Notice given by the COMPANY. A Notice may be made at any time by the COMPANY and directed to the person designated in Article 13.9 or to the USER's address specified above, at the election of the COMPANY. Notices may be deemed provided to USER by USER accessing FE GRACE (rsa.com), or by COMPANY sending an email, hardcopy first class mail, or by facsimile, at the election of the COMPANY.

(a) Directives contained in Notices identified as "Emergency" shall be implemented immediately;
(b) Directives contained in Notices identified as "Urgent" shall be implemented within forty-eight (48) hours;
(c) Directives contained in Notices identified as "Important" shall be implemented within seven (7) days;
(d) All other Notices shall be implemented within thirty (30) days.

USER shall provide immediate written confirmation to the COMPANY, signed by an officer of the USER, that it has implemented the security procedures and standards set forth in each Notice.

6. Monitoring and Enforcement

COMPANY, in its sole discretion, will determine whether your conduct is in compliance with this AUP. We have the right to:

(a) Monitor your use of our Information Assets for any purpose in our sole discretion and as we see fit.

(b) Take any action we deem necessary or appropriate in our sole discretion if we believe your conduct violates this AUP, infringes any intellectual property right or other right of any person or entity, threatens the personal safety of users of our Information Assets, or the public, or could create liability for the COMPANY.

(c) Disclose your identity or other information about you to any third party who claims that material posted by you violates their rights, including their intellectual property rights or their right to privacy.

(d) Take appropriate legal action, including without limitation, referral to law enforcement, for any illegal or unauthorized use of our Information Assets for any or no reason, including without limitation, any violation of this AUP.

Without limiting the foregoing, we have the right to fully cooperate with any law enforcement authorities or court order requesting or directing us to disclose the identity or other information of anyone who accesses or uses our Information Assets. YOU WAIVE AND HOLD HARMLESS THE COMPANY AND ITS PARENT, SUBSIDIARIES, AND AFFILIATES FROM ANY CLAIMS RESULTING FROM ANY ACTION TAKEN BY THE COMPANY OR ANY OF THE FOREGOING PARTIES DURING, OR TAKEN AS A CONSEQUENCE OF, INVESTIGATIONS BY EITHER THE COMPANY, THE FOREGOING PARTIES, OR LAW ENFORCEMENT AUTHORITIES.