FirstEnergy Network Access Agreement
for
Project Scope Contractors

This Network/System Access Agreement ("Agreement") is made and entered into by and between _____***[INSERT NAME OF SUPPLIER]*** ("SUPPLIER") with principal executive offices at ___***[INSERT ADDRESS OF SUPPLIER]*** on behalf of its employees, agents, or contractors (each a "USER" and collectively, "USERS") effective as of the _____ day of _____, 20__ 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.

Both SUPPLIER and COMPANY agree that in order to perform under _____***[INSERT NAME OF TERMS AND CONDITIONS between SUPPLIER and COMPANY]*** ("Terms and Conditions"), the SUPPLIER and USERS need to establish a high speed, secure connection to the COMPANY network. The COMPANY is granting USERS controlled and limited access either (1) to the COMPANY external connection via Virtual Private Network ("VPN") or (2) to the COMPANY network to support the USERS' information technology needs; and,

WHEREAS, SUPPLIER and USERS recognize and agree the COMPANY'S networks are valuable and sensitive assets of the COMPANY and may be severely damaged by misuse, even inadvertent misuse; and

WHEREAS, SUPPLIER and USERS agree that the COMPANY is required by law to protect its information systems and communications assets by requiring SUPPLIER and USERS to be bound to the terms and conditions of this Agreement; and

WHEREAS, COMPANY will not allow SUPPLIER nor any USERS to access the Network (defined below) without SUPPLIER assuming the obligations described below; and,

WHEREAS, such access will indirectly benefit SUPPLIER and USERS.

NOW THEREFORE, in consideration of the COMPANY granting access as specified and limited herein and after acknowledging the accuracy of the foregoing recitals, the parties hereby agree to the following terms:

1. Definitions.

   (a) Any defined term that is not defined in this Agreement shall be attributed the definition in the related Terms and Conditions.

   (b) All terms relating to Background Checks, Substance Abuse, Gifts and Gratuities/Conflicts of Interest from Terms and Conditions are incorporated herein.

2. Access to Network. In reliance upon SUPPLIER and USERS assuming the obligations described below, the COMPANY agrees to allow SUPPLIER and its USERS, from time to time to establish a VPN connection to the COMPANY network, information systems or communications assets (collectively, the "Network") using an IPSec compliant communications protocol subject to strict compliance with the COMPANY'S security procedures and standards as the same may be given by notice to SUPPLIER from time to time by the COMPANY. The current COMPANY security procedures and standards are detailed in Section 3 below. The COMPANY may modify these at any time and SUPPLIER agrees that such modified security procedures and standards shall become part of this Agreement when the COMPANY provides written notice (herein referred to as the "Notice") of the revised or modified security procedures and standards to SUPPLIER and USERS. Each USER will be required to complete and sign a form of a Network/System Access Request for Project Scope Contractors (Form X-3468 REV 03-13).

3. Implementation of Security Procedures. SUPPLIER and USERS shall, prior to establishing any connection to the Network, implement and comply with the following policies, security procedures and standards:

   (a) Internet Use Policy

   SUPPLIER and USERS agree that any use of the Internet or electronic communications through the Network will be solely for business purposes. In accordance with the COMPANY'S existing Internet usage policies, SUPPLIER and the USERS shall not knowingly access any gambling, pornography, hate or violence sites, shall not forward any chain letters, fraudulent virus alerts, executable ready to run files or other files or codes which may damage the Network. The COMPANY reserves the right to monitor SUPPLIER'S and USERS' use of the Internet to assure compliance with these policies and standards.

   (b) Substance Abuse Policy

   SUPPLIER and USERS agree to comply with all applicable state and federal laws regarding drug-free workplace, as well as Purchaser's rules and regulations governing the same, available upon request. SUPPLIER and USERS are responsible for ensuring that all USERS, while working in the Network, will not be under the influence, purchase, transfer, use or possess illegal drugs or alcohol or abuse prescription drugs in any way.

   (c) VPN Security Procedures and Standards

   Router filters and/or firewall rules will be applied to limit the networking protocols and number of Network devices accessing the COMPANY resources across the VPN connection to the minimum required to provide the needed business function. The implementation of the VPN connection will be in accordance with the COMPANY remote access policy pertaining to VPN access. Network traffic flowing across the VPN connection will be monitored. Virus protection software must be present,

configured with current virus signature files and engine, and be active on any machine accessing the COMPANY resources across the VPN connection. Remote control software will not be installed on any machine accessing the VPN connection.

4. Revision of Security Procedures. As provided above, the COMPANY may from time to time revise requirements in Section 3 above. SUPPLIER will implement and maintain the requirements of the revisions at its sole cost and expense 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 Section 14.7 below or to the address of the SUPPLIER specified above, at the election of the COMPANY. Notices may be sent by email, hardcopy first class mail or by facsimile, at the election of the COMPANY.

    - Directives contained in Notices identified as "Emergency" shall be implemented immediately
    - Directives contained in Notices identified as "Urgent" shall be implemented within 48 hours
    - Directives contained in Notices identified as "Important" shall be implemented within 7 days
    - All other Notices shall be implemented within 30 days

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

5. Denial of Access. The COMPANY reserves the right to disconnect the VPN or direct connection at any time, without notice, for its convenience. The COMPANY may deny access to its Network without any prior notice if SUPPLIER does not implement and certify its implementation of the security procedures and standards set forth herein and in any Notice within the applicable time specified above. Any denial of access shall be without prejudice to any other rights or remedies that the COMPANY may have. Such denial of access shall not constitute a breach of this Agreement, Terms and Conditions this Agreement supports, or any other obligation of the COMPANY to SUPPLIER and, unless otherwise agreed, SUPPLIER shall continue to perform its obligations under any contract or agreement without interruption or delay.

6. Exceptions. If SUPPLIER believes it cannot implement a Notice within the time required without adversely affecting its own network(s) or business, it may so inform the COMPANY by notice given pursuant to Section 3 above, and the COMPANY will attempt to resolve SUPPLIER concerns while still protecting the Network. The COMPANY may, in its sole and absolute discretion, allow SUPPLIER 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 SUPPLIER 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 SUPPLIER'S concerns in a manner acceptable to SUPPLIER, or at all. The COMPANY'S Information Security Manager shall make the final decision on any exception taken by SUPPLIER.

7. Non-Use, Non-Disclosure Related to Network/System Access.

    In addition to the CONFIDENTIALITY terms in the related Terms and Conditions, the following apply to the use of the Network:

    (a) All information, including any copies thereof, in any media, in the possession or control of the SUPPLIER and USERS and all information embodied or included in any software or data files loaded or stored on computers in the possession or control of the SUPPLIER and USERS shall be removed by SUPPLIER and USERS and returned to COMPANY either upon demand or no later than the completion of work for COMPANY.

    (b) Neither SUPPLIER nor USERS shall copy the information in whole or in part or use all or any part of the information to reverse engineer, duplicate the function, sequence or organization of the Information for any purpose without the prior written permission of the COMPANY.

8. Malicious Code. Neither SUPPLIER nor USERS shall (i) introduce any malicious or surreptitious code into the Network, including any virus, worm, Trojan Horse, backdoor or undisclosed executable file.; (ii) use any means to circumvent any COMPANY system security measure or; (iii) attempt to access any COMPANY system resource that the COMPANY has not authorized for SUPPLIER'S or USERS' access.

9. Third Party Access. Notwithstanding the Terms and Conditions, neither SUPPLIER nor USERS shall allow any third party, including but not limited to subcontractors, temporary employees or, in the case where SUPPLIER is a business entity, other persons who are not full time employees of SUPPLIER, to access the Network through SUPPLIER or USERS computer systems or networks unless specifically authorized by the COMPANY in writing. The COMPANY, in its sole discretion, may require such other person or persons to separately execute a copy of this Agreement prior to granting access. SUPPLIER shall take all steps necessary to secure its own networks and its access to the Network to prevent any person not authorized by the COMPANY from gaining access to the Network.

10. Compliance Audit Related to Network/System Access. In the event that the COMPANY reasonably concludes, that SUPPLIER or any individual for whom it is responsible has breached its obligations under this Agreement, the COMPANY may at any time upon reasonable notice and during normal business hours enter onto SUPPLIER'S premises and conduct an audit (in cooperation with SUPPLIER) of SUPPLIER's Security obligations under this agreement to determine SUPPLIER'S and USERS' compliance with the COMPANY'S security procedures and standards. The COMPANY shall be limited to accessing portions of SUPPLIER'S records as is reasonably necessary to determine whether SUPPLIER has complied with its obligations contained in this Agreement. SUPPLIER shall certify its and its USERS' compliance, and the USERS shall each certify their compliance with this Agreement upon the request of COMPANY.

11. Notice of Unauthorized Access/Export Control.

(a) SUPPLIER shall notify the COMPANY by email and by facsimile as soon as possible and but no later than 24 hours of any breach of the security procedures and standards, any unauthorized access to the Network through the VPN, or the introduction of any malicious code, such as, but not limited to, a computer virus, Trojan horse or worm, into the Network. SUPPLIER understands and agrees that the Network contains information that is controlled and restricted from export by various Federal laws and regulations (the "Controlled Information"). Export controls include restrictions on "deemed export" of Controlled Information. Generally, deemed export occurs when Controlled Information is made available, displayed to or otherwise observed or overheard by persons who are not citizens or permanent residents of the United States.

(b) SUPPLIER agrees to request of the COMPANY access rights for only employees of SUPPLIER who are citizens or permanent residents of the United States of America. SUPPLIER will implement security and control procedures necessary to prevent deemed exports of Controlled Information of COMPANY. SUPPLIER further agrees to prevent any deemed export of the COMPANY Controlled Information in connection with its access to the Network or otherwise in its authorized use of the COMPANY Controlled Information. SUPPLIER understands that by entering into this Agreement with SUPPLIER, the COMPANY is not providing or authorizing any access to the Network or Controlled Information to any person who is not a citizen or permanent resident of the United States. SUPPLIER AGREES THAT SUPPLIER'S BREACH OF ANY OF THE REQUIREMENTS OF THIS SECTION SHALL BE A MATERIAL BREACH OF CONTRACT AND MAY CONSTITUTE A VIOLATION OF FEDERAL CRIMINAL AND/OR CIVIL STATUTES.

(c) In the case where a USER is an individual who is not a citizen or permanent resident of the United States, such USER shall not be granted access until the COMPANY can determine if the proposed access to the Network can be implemented in a manner to exclude access to Controlled Information. If COMPANY, in its sole discretion, determines that such access cannot be accommodated, USER shall not be provided access to the Network. In the case where SUPPLIER is a business entity and SUPPLIER proposes that the COMPANY provide Network access for a USER that is not a citizen or permanent resident of the United States, SUPPLIER must provide written notice to the COMPANY, no less than 30 days prior to the date the proposed Network access rights would become effective. The COMPANY will, in its sole discretion, determine if the proposed Network access can be implemented in a manner to exclude access to Controlled Information and notify the SUPPLIER if such access can be provided. If such access cannot be provided, SUPPLIER shall not permit USER to gain access to the Network.

12. DISCLAIMER OF WARRANTIES RELATED TO NETWORK/SYSTEM ACCESS. THE COMPANY HEREBY DISCLAIMS ALL IMPLIED WARRANTIES,INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE IN CONNECTION WITH THE PROVISION OF ACCESS TO SUPPLIER AND USERS. SUPPLIER ACCEPTS ALL RISKS ASSOCIATED WITH ITS ACCESS AND USERS' ACCESS TO AND USE OF THE COMPANY SYSTEMS AND NETWORK. ACCESS IS PROVIDED AS-IS WITH NO WARRANTIES.

13. LIMITATION OF LIABILITY AND INDEMNITY OF SUPPLIER AND ITS USERS.

(a) IN NO EVENT WILL THE COMPANY BE LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES (INCLUDING LOSS OF USE, DATA, BUSINESS OR PROFITS) ARISING OUT OF OR IN CONNECTION WITH THIS NETWORK ACCESS AGREEMENT, OR THE PROVISION OF ACCESS TO SUPPLIER, INCLUDING WITHOUT LIMITATION, ANY DAMAGES RESULTING FROM ANY DELAY, OMISSION OR ERROR IN THE ELECTRONIC TRANSMISSION OR RECEIPT OF DATA, 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. SUPPLIER AND ITS USERS AGREETHAT THE TOTAL LIABILITY OF THE COMPANY FOR ANY REASON ARISING OUT OF THE PERFORMANCE OR BREACH OF THIS AGREEMENT BY THE COMPANY SHALL NOT EXCEED FIVE HUNDRED DOLLARS ($500.00).

(b) SUPPLIER AGREES TO INDEMNIFY AND HOLD HARMLESS THE COMPANY FROM ANY LOSS, DAMAGE, LIABILITY, JUDGMENT, FINE, OR PENALTY ARISING OUT OF ANY USE OF THE COMPANY SYSTEMS AND NETWORK, SUPPLIER'S AND USERS' ACCESS TO THE COMPANY SYSTEMS AND NETWORK OR THE BREACH OF THIS AGREEMENT BY SUPPLIER OR ITS USERS.

14. MISCELLANEOUS RELATED TO NETWORK/SYSTEM ACCESS.

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

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

14.3 Assignment. SUPPLIER may not assign any Network access granted under this Agreement, in whole or in part.

14.4 Force Majeure Related to Network/System Access. The COMPANY shall not be liable for any failure to perform its obligations in connection with any Transaction or any Document if such failure results from any act of God or other cause beyond

COMPANY'S reasonable control (including, without limitation, any mechanical, electronic or communications failure) which prevents a party from transmitting or receiving any Documents.

14.5 Relation to Other Agreements. In case of any conflict between the provisions of the other agreements of the parties and this Agreement, the provisions of this Agreement shall control as to the SUPPLIER'S and USERS' Network access.

14.6 Governing Law. The parties agree to the jurisdiction of the Federal and County courts located in Summit County, Ohio and that the laws of the State of Ohio shall apply to the interpretation and construction of this Agreement without giving effect to its rules regarding conflicts of laws

14.7 Notice.

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

And

FirstEnergy Service Company
Information Systems Opts Center
253 White Pond Drive
Akron, OH 44320
ATTN: Mgr. Cyber Security/IT
Phone: 330-436-2005
Fax: 330-315-9281

If Notice is to SUPPLIER:
Name:
Address:
City, State, Zip:
ATTN:
Phone:
Fax:

14.8 Survival. The following provisions of this Agreement shall survive any termination or expiration: Sections 6, 9, 10, 11, 12, &13.