

**VENDOR REQUIREMENTS FOR
IT SYSTEM ACCESS, CONTROLLED INFORMATION AND DATA SECURITY**

Nucor Corporation (with its affiliates and subsidiaries, “Nucor”) requires that each vendor, contractor and supplier (individually a “Vendor” and, collectively, “Vendor”) complies with the following Vendor Requirements for IT System Access, Controlled Information and Data Security.

IT SYSTEM ACCESS. In the event Vendor, any of its subcontractors and/or their respective employees (collectively, “Vendor Personnel”), requires access to any Nucor computer, computer network, software, hardware or information system (collectively, the “Nucor System”) in connection with the provision goods and/or services, or in the event any goods, materials or equipment transmit data and information or otherwise accesses the Nucor System, the following shall apply:

(a) In no event shall Vendor (or any Vendor Personnel) use the Nucor System to: (i) perform, conduct or assist in any illegal activities; (ii) receive and/or transmit threatening or hostile communications; (iii) receive and/or transmit pornographic or other explicit materials; (iv) solicit business, sell products and services, or otherwise engage in commercial activities other than those expressly required for the provision of goods and/or services to Nucor; or (v) perform any other activity that is not required for provision of goods and/or services to Nucor. Vendor’s use of the Nucor System shall at all times comply with all applicable laws, rules and regulations. Vendor shall not, without the prior written consent of Nucor, test or attempt to bypass or compromise any virus protection software or security controls of the Nucor System, including, without limitation, any physical or electronic measures used by Nucor to limit Nucor System access and/or use;

(b) Vendor’s access rights to the Nucor System shall terminate immediately upon the earlier of: (i) notice from Nucor that such access has been terminated; or (ii) completion of the provision of goods and/or services to Nucor. Vendor acknowledges and agrees that Nucor, in its sole discretion, may terminate, cancel, restrict or otherwise modify Vendor’s (or any Vendor Personnel’s) access to the Nucor System at any time; and

(c) At all times, Vendor shall use up-to-date malicious code protection and virus protection software in accordance with industry best practices for all Vendor computer systems and devices used to provide goods and/or services (collectively, “Vendor Devices”). All Vendor Devices containing Nucor’s confidential, proprietary or protected information (“Confidential Information”) must be secured by Vendor from theft and unauthorized use. Vendor shall immediately report to Nucor all information security incidents, including, without limitation, the introduction of Harmful Code (as defined below) onto the Nucor System, unauthorized or inappropriate use of the Nucor System, unauthorized access or disclosure of Confidential Information, loss, or theft of any Vendor Device, etc.

CONTROLLED INFORMATION. To the extent Nucor, in its sole discretion, permits Vendor access to Controlled Information, Vendor shall ensure that it and any Vendor Personnel who receive such Controlled Information comply with all applicable safeguarding and dissemination requirements, including, without limitation, those set forth in DFARS 252.204-7012, DFARS 252.204-7021, the Export Administration Regulations (15 C.F.R. Parts 730-774), the International Traffic in Arms Regulations (22 C.F.R. Parts 120-130), and any other applicable requirements regarding the protection, handling, marking, transmission, storage, and destruction of Controlled Information, as may be amended, including any restrictions regarding release of such information to foreign persons. Nucor, in its sole discretion and at any time may: (a) request that Vendor provide a list of all Vendor Personnel who have access to Nucor’s Confidential Information and the location of such Vendor Personnel; (b) prohibit any Vendor Personnel located outside the United States from accessing and/or processing Nucor’s Confidential Information; and (c) prohibit any Vendor Personnel from accessing and/or processing certain types or categories of Nucor’s Confidential Information

(including, without limitation, any Controlled Information (as defined below)), and/or revoke any previously granted access to the same. As used herein, “Controlled Information” means: (i) Controlled Unclassified Information (“CUI”) as defined under 32 C.F.R. § 20002.4(h) and categorized by the National Archives and Records Administration; (ii) Export-Controlled Information, which is defined as information, technical data, technology, or other materials that are subject to export control laws or regulations, including, without limitation, the International Traffic in Arms Regulations (22 C.F.R. Parts 120-130) and the Export Administration Regulations (15 C.F.R. Parts 730-774); and (iii) any other information that is subject to safeguarding, dissemination, access, or use restrictions under any applicable federal, state, or local law, regulation, contract, or government-wide policy. Without limitation, Controlled Information shall be considered Confidential Information of Nucor.

DATA SECURITY.

(a) Neither any materials or equipment furnished as part of the services, nor any goods (including any software (including any programmable logic controller) embedded or otherwise used in the goods (“Software”)), nor the source code and other human readable materials relating to the Software (“Source Materials”) shall contain: (i) computer instructions, circuitry or other technological means, such as a computer “virus,” computer “worm,” computer “time bomb,” “Trojan horse,” “back door,” “malware” or any blended or convergent combination thereof (“Harmful Code”), for the purpose of damaging or interfering with Nucor’s operations, and that Vendor will not introduce any Harmful Code into the Nucor System; or (ii) any third-party open source software that would (x) require Vendor or Nucor to grant to any third party any rights in any Confidential Information or Nucor’s products, services or any patent, copyright, trade secret, know-how, trademark or other proprietary or intellectual property right (collectively, “Intellectual Property Rights”) of any person or entity, (y) require the licensing, disclosure or distribution of any source code, data, information, materials, products or services developed by or for Nucor, or (z) create restrictions on or immunities to Nucor’s enforcement of its Intellectual Property Rights.

(b) Vendor shall promptly and without delay – but in no event later than forty-eight (48) hours from the occurrence or earlier, if required by law or regulation – report to Nucor any unauthorized use, loss or disclosure of any Confidential Information or any other information, data or materials provided to Vendor by Nucor or otherwise gathered by Vendor in connection with its provision of goods and/or services to Nucor. Vendor shall cooperate fully with Nucor in investigating any such unauthorized use, loss or disclosure, and will take all actions as may be necessary or reasonably requested by Nucor to mitigate the problem, including notifying affected individuals and/or governmental entities, and minimize any resulting damage. Unless required to do so by applicable law, Vendor agrees that it will not notify Nucor-related affected individuals and/or governmental entities without first obtaining written instruction from Nucor. Prior to such intended notification, Vendor shall provide written notice to Nucor Corporation’s General Counsel and Nucor shall have ten (10) business days to object to such notification.

(c) Confidential Information shall be accessed, transmitted, stored, maintained and processed by Vendor only as necessary to provide the relevant goods and/or services to Nucor. Vendor shall make commercially reasonable and industry standard efforts to ensure that any Confidential Information or any other information, data or materials provided to Vendor by Nucor or otherwise gathered by Vendor in connection with its provision of goods and/or services to Nucor that is accessed, transmitted, stored, maintained or processed by Vendor is not intercepted or otherwise obtained by unauthorized third parties. Vendor shall (i) have a written information security program in place that is actively assessed and managed as part of ordinary course of business; and (ii) monitor industry-standard information channels for newly identified vulnerabilities and fix or patch based upon risk. Prior to the provision of any goods and/or services to Nucor, Vendor shall provide Nucor with the opportunity to review and discuss with Vendor its written information security program. Without limiting the foregoing, Vendor’s information security program must, at a minimum, be designed to: (w) ensure the security, integrity and confidentiality of Confidential

Information; (x) protect against any anticipated threats or hazards to the security or integrity of Confidential Information; (y) protect against unauthorized access to or use of Confidential Information that could result in substantial harm or inconvenience to Nucor or the person or entity to whom such information relates; and (z) ensure the proper disposal of Confidential Information in accordance with the requirements of any applicable agreement between Nucor and Vendor. Should use or operation of the goods require or result in the transfer of any data or information either to or from the goods via the Internet or any other wireless means, then Vendor shall provide written notice to Nucor of such requirement or result, and shall obtain Nucor's prior written approval of such transmission. Vendor shall cooperate with Nucor in ensuring such transfer occurs in accordance with Nucor's requirements, including that such transfer occurs via Nucor's internal network or other Nucor System. No transmission of any data (including, without limitation, direct cellular data connections) shall bypass traffic inspection via perimeter firewalls, and all encrypted tunnels in or out of the Nucor System must terminate on a Nucor perimeter firewall and only allow access to an approved secure site.