SUMITOMO ELECTRIC GROUP

January 2022

Sumitomo Electric Group

CYBER SECURITY REQUIREMENTS POLICY FOR SUPPLIERS

Sumitomo Electric Group Supplier Code of Conduct

This Cyber Security Requirements Policy for Suppliers ("**Policy**") sets out Sumitomo Electric Group's ("SEG") expectations for cyber security protection with respect to our suppliers, including suppliers, subcontractors, agents, consultants, distributors or any other party that is part of the SEG supply chain with respect to its products or services (referred to hereinafter as the "Supplier").

At SEG we recognize that our suppliers play an important role in our overall success. We appreciate the contributions our suppliers make to our business. We choose to do business with suppliers who share our commitment to cyber security. SEG asks our suppliers to conduct their business in a manner consistent with the principles set out below and to ensure that their supply chains do the same.

This Policy and any subsequent versions shall be available at [https://www.sews-e.com].

Compliance requirements and supplier commitment

The Supplier is responsible for taking all actions and measures necessary to comply with the requirements set out in this Policy.

SEG reserves the right to request evidence and documentation, as well as the right to perform a compliance audit, in order to determine whether the Supplier has adequately complied with this Policy.

Security of supply chain

The Supplier shall establish, document and implement initiatives in line with commonly accepted industry standards and practices to build cyber security into its systems (meaning the computer systems, including all hardware, software and peripheral equipment used by the Supplier, including any third party hardware, software or services that the Supplier uses from time to time referred to hereinafter as "Systems") and its supply chain to ensure that it is not susceptible to avoidable cyber-attacks. The Supplier shall proactively take measures to constantly improve the quality of the cyber security of its Systems.

Malware, backdoor accounts and accounts

The Supplier shall ensure that its Systems do not contain any malware, backdoor or other technological routine, device or code that could adversely affect the security or confidentiality of the Supplier's Systems or any information and data of its Systems.

The Supplier shall undertake regular penetration testing and disaster recovery testing on its Systems.

Cyber security incidents

The Supplier shall inform the relevant SEG subsidiary by telephone call of any cyber-security incident (such as a breach of its System's security policy that affects its integrity or availability or the unauthorised access or attempted access to its Systems) as soon as possible, but in any event within twenty-four (24) hours of the Supplier discovering such cyber-security incident.

If any cyber-security incidents occur, the Supplier shall:

1. provide the relevant SEG subsidiary with a summary of known information about such cyber-security incident,
2. use its best endeavours to attempt to remedy the effects of such cyber-security incident,
3. provide reasonable information about the cyber-security incident and response upon request by SEG, and
4. within twenty-four (24) hours of completion of the investigation of the cyber-security incident, provide a report to the relevant SEG subsidiary outlining: a description of the cyber-security incident, the cases of such events and how the Supplier has mitigated against future events of a similar kind, the timeline of the incident, the suspected perpetrators, what information or data of the SEG subsidiary may have been affected, or any financial impact to SEG. Any corrective actions identified as contributing to cyber-security incident shall be implemented no later than one (1) month after the completion of the investigation for such cyber-security incident.

Data security

The Supplier shall implement and maintain appropriate technical and organizational measures and other protections for the proper security of all information or data belonging to SEG, including, without limitation, not loading any confidential information provided by the SEG subsidiary to the Supplier on (a) any laptop computers or (b) any portable storage media that can be removed from the Supplier's premises unless in each case such data has been encrypted and such data is loaded onto the portable storage media solely for the purpose of moving such data to off-site storage.

The Supplier will use reasonable endeavours to prevent password theft or loss or unauthorized access to or use of any data or information of the SEG subsidiary in the possession of the Supplier and the Supplier shall notify the relevant SEG subsidiary promptly of any password theft or loss or unauthorized access or use of any data or information of SEG. The Supplier will enforce safety and physical security procedures with respect to its access and maintenance of confidential information or data of the SEG subsidiary that are (i) at least equal to industry standards for such types of locations, and (ii) which provide reasonably appropriate technical and organizational safeguards against accidental or unlawful, loss, alteration or unauthorized disclosure or access to confidential information or data of SEG.

Sub-suppliers and sub-contractors

The Supplier shall ensure that all sub-suppliers and sub-contractors that contribute to the supply to the SEG subsidiary comply with the requirements set out in this Policy.

Notwithstanding the above, the Supplier shall be fully responsible for all acts and omissions of its sub-suppliers and/or sub-contractors as if they were its own acts or omissions in relation to its supply to SEG.

Without prejudice to the Supplier's obligations above, the Supplier shall take adequate measures to mitigate the risks associated with sub-suppliers and sub-contractors that do not meet the listed (or equivalent) requirements.

Changes to these cyber security requirements

This Policy may be amended or modified from time to time at SEG's discretion. Any such amendments or modification will be applicable from the date of release on the the SEG subsidiary website at: [https://www.sews-e.com]