CYBERSECURITY RISK MANAGEMENT REQUIREMENTS FOR ALL CORNING SUPPLIERS

1. Security Controls. Supplier must take all steps required to update and maintain its security and back-up processes and procedures, its hardware, software, systems, facilities and services, so that they are consistent with industry accepted best practices, such as Service Organization Controls (SOC) 2 Type 2 report, ISO 27001/27002, SSAE 18, or the NIST Cybersecurity Framework. Supplier must establish and maintain an information security program that is designed to: (i) ensure the security and confidentiality of Corning's information; (ii) protect against any anticipated threats or hazards to the security or integrity of Corning's information; (iii) protect against unauthorized access to or use of Corning's information; and (iv) ensure the proper disposal of Corning's information. Additionally, Supplier must protect all confidential information with security measures appropriate to the sensitivity of the confidential information while preserving its integrity and availability as required to perform the services or delivery products.

   In the event the Supplier is approved to use subcontractors, Supplier must ensure that any such subcontractor adheres to all the obligations and requirements in these Information Security Requirements.

2. Security Incidents.
   a. Defined. "Security Incident" is i) an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of Corning or the Supplier's information system or the information the system processes, stores, or transmits, that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies of either Corning or the Supplier or ii) an occurrence that materially impacts Supplier's ability to fulfill its supply or service obligations, including but not limited to a ransomware or Distributed Denial of Service attack on Supplier's operation impacting Supplier's ability to securely communicate with Corning.
   b. Notification and Response Requirements. In the event of a Security Incident, whether the incident is confirmed or suspected, Supplier must:
      i. initiate Supplier's security incident response process, which shall include:
         1. notification to Corning by telephone and email to Corning Security Operations Center, ITSecurity@corning.com (607-974-8407) within twenty-four (24) hours of discovery of such Security Incident;
         2. identifying to Corning a point of contact at Supplier with the requisite information security knowledge and skill regarding the Security Incident;
         3. promptly remediating the Security Incident to prevent any further harm to Corning;
         4. beginning a thorough investigation of the Security Incident, including any root cause analysis; and
         5. taking all reasonable actions to mitigate any future potential harm to Corning;
      ii. comply with all applicable laws and regulations requiring notification to individuals, provided that Supplier obtain Corning's prior written approval of the breach notification content and plan for distribution if any Corning employees must be notified; and

iii. promptly cooperate to provide Corning with any reasonably requested information in a timely manner, and after Supplier completes its investigation, promptly provide Corning with a report of the event, including a root cause assessment and mitigation plan.

4. Audit. Corning shall be entitled to perform, or to have performed, an on-site audit of Seller's information security program with Supplier's cooperation in such audit. In lieu of an on-site audit, upon request by Corning, Supplier shall complete, within thirty (30) days of receipt, an audit questionnaire provided by Corning regarding Supplier's information security program. No less than annually, Supplier must conduct an independent third-party audit of its information security program and, if so requested, provide such audit findings to Corning. Supplier shall implement any required safeguards as identified by information security program audits.

5. Business Continuity Planning, Service Continuity Management and Disaster Recovery. Supplier must maintain a business continuity plan that meets the minimum business continuity and disaster recovery requirements aligned to industry standards (e.g., ISO 22301) commensurate to the Supplier's size and complexity. Supplier must ensure that all applicable Supplier subcontractors have an appropriate and regularly reviewed and tested business continuity plan in place, and that each Supplier subcontractor is able to and will meet or exceed the industry standards to the extent it is applicable to such Supplier subcontractor. Not less than once per calendar year, Supplier must test its business continuity plan and provide Corning the results of such test. Supplier shall promptly remedy any test failures.