Policy Name: Information Security Policy - Supplier Rules of Engagement	Document Owner: Ball, Laura
Associated Policy:	Last Updated: 12/11/2023
Audience: All Corning	Version: V3

Information Security Policy – Supplier Rules of Engagement

Purpose:

This Information Security Policy sets the minimum standards for all Corning suppliers to protect Corning's information. This includes all Corning information in any form, including but not limited to, verbal, pictorial, audible, electronic, or tangible, regardless of media, format or material; including intellectual property and transactional output created, received, and used in the normal course of business and maintained by Corning or a 3rd party on Corning's behalf that has value to Corning and must be appropriately managed and secured through its lifecycle.

Applicability:

This policy applies to all worldwide locations of Corning Incorporated, affiliates, suppliers and employees of said entities. An affiliate is defined as any entity or company of which Corning Incorporated owns, directly or indirectly, more than fifty percent (50%) of the equity. "Employees" in this policy include contingent labor.

Enforcement:

Compliance with this policy is mandatory. Failure to comply (gives Corning the right to pursue appropriate disciplinary or legal action up to and including removal of access to Global Supply Management (GSM) tools, garnishment of wages or termination of employment. Escalation of disciplinary actions will be based on specific geographical rules and the severity and / or frequency of infractions by an individual.

Information Security Policy – Supplier Rules of Engagement

1) Supplier shall ensure that its personnel with access to Corning INFORMATION are aware of Corning's information security requirements set forth in these rules of engagement and complete the training called GSM IS Policy and Procedure

Supplier Training. **http://www.corning.com/worldwide/en/about-us/suppliers/supplier-download-library.html**

2) Supplier shall ensure Corning Information is only disclosed to its personnel on a "Need to Know" basis and only for Corning business

3) Supplier shall ensure that all hardcopy Corning Information in its possession is secured at the end of each workday

4) Supplier shall ensure all Corning Information printed or copied include the following:

a. A watermark prominently displayed on the document.

b. All drawings and documents containing Corning INFORMATION, created by the supplier or supplier's subcontractor, shall be clearly marked "Corning Restricted" (unless otherwise instructed by the supplier's sponsor).

5) All Corning INFORMATION must be disposed of properly. Approved disposal methods include:

a. Permanent deletion of electronic files so that they cannot be recovered.

b. Hard drives on all electronic storage devices (e.g., computer, USB thumb drives, copiers, etc.) that contain Corning INFORMATION must be properly erased or physically destroyed before disposal.

c. Paper documents containing Corning INFORMATION shall be destroyed by incineration or shredded using a cross-cut shredder with a cross-cut size of no greater than 3/16 inch by 2 inches or smaller.

6) Corning INFORMATION is not to be left unattended in conference rooms or on white boards, flip charts, hand-outs at meetings, copiers, or printers.

7) Supplier must not release Corning INFORMATION to any other supplier without the prior written consent of Corning.

8) At the end of a project, all Corning INFORMATION, including items referring or relating in any way to Corning INFORMATION, whether in electronic, printed or other format must either be destroyed beyond recognition or returned to Corning. Documentation of return or destruction will be provided to Corning upon request.

9) COMPUTING SYSTEMS

a. All laptops and portable electronic storage devices that contain Corning INFORMATION shall be physically secured

b. All laptops and portable electronic storage devices must be secured with a cable lock to an immovable object or locked in a secure location.

c. Supplier employees, when working on Corning INFORMATION, must employ the computer screen lock when their computers are left unattended, and use privacy screens during use (if visible to others).

d. Any electronic storage devices containing Corning INFORMATION must be password protected and encrypted.

e. Supplier shall ensure that Corning INFORMATION is only shared via Corning approved secure methods.

f. Supplier shall ensure that no Corning INFORMATION is stored in a cloud-based environment without prior written approval from Corning

g. If using a Corning approved and supplied computer, the supplier must comply with all Corning IT Use Policy rules.

10) SECURE BEHAVIORS

a. Supplier is not to discuss Corning INFORMATION in public where it might be overheard by a third party (e.g., airports, buses, restaurants, bars etc.).

b. Supplier is not to post Corning INFORMATION on the internet or on any social media (e.g., networking websites, blogs, Wikis, chat rooms, virtual worlds etc.)

c. Supplier must notify Corning of any attempts by any third party to
   i. obtain Corning INFORMATION
   ii. request quotes or attempt to order Corning custom equipment or materials.

d. Supplier must report any improper disclosure or loss of Corning INFORMATION within reasonable amount of time of detection to Corning, whether inadvertent or otherwise. The supplier is expected to cooperate in full with Corning in the investigation of the disclosure or loss.

11) PHYSICAL SECURITY

a. Supplier locations (including any off-site) must have appropriate physical access controls to include:

1. Facility access control to prevent unauthorized entry
2. Visitor management procedures
3. Restricted areas within a facility to prevent unauthorized access or view to Corning work in progress

b. IMAGING & MOBILE DEVICES

1. Supplier must have an imaging policy in place. At minimum this policy should address how the following are controlled:

   a. Imaging devices (e.g., camera)
   b. Storage media for images (e.g., SD cards)

c. Images (e.g., actual pictures)

2. The use of smart devices (e.g., smart phones, tablets) is also restricted as follows:

a. No image capture of Corning equipment or information
b. No storage of Corning information; this includes email if the device is not remote-wipe capable
c. No mobile hot spot turned on in a Corning restricted area

12) OVERSIGHT

Corning reserves the right to:

a. Require a written plan of compliance with these Rules of Engagement prior to receiving any Corning INFORMATION.

b. Audit its suppliers for compliance to these Rules of Engagement and any additional site-specific rules that are made to protect Corning INFORMATION.

c. Require a corrective action plan for any identified compliance deficiencies.

13) USE OF SUBCONTRACTORS (THIRD PARTIES)

a. Supplier must obtain a Non-Disclosure Agreement ("NDA") with all subcontractors or significant third-party suppliers who have access to Corning INFORMATION that are substantially similar in form and substance to the Corning NDA requirements and restrictions.

b. If subcontractor will be working on a Corning site, the subcontractor must also sign a separate NDA with Corning.

c. Corning reserves the right to audit supplier's subcontractors for compliance to these Rules of Engagement, the Supplier Information Security Policy, and any additional site-specific rules that are made to protect Corning INFORMATION.

d. Regardless of any third-party agreement to the contrary, the supplier is solely responsible for ensuring that all of its subcontractors strictly comply with these Rules of Engagement.

14) WHEN ON A CORNING SITE

a. Supplier must comply with Corning's site access control policies and procedures.

b. Imaging or other copying and scanning devices (including but not limited to picture-capable cell phones and portable copy or scanning devices), of any kind, are prohibited on any Corning site without prior application for an "Imaging Device Pass" approved by Corning personnel at the particular location.

c. No mobile hot spot turned on in a Corning restricted area.

d. Supplier shall only access Corning sites upon receipt of a Corning issued badge. Plant access will be limited to the areas directly related to the work being done by the supplier.

e. Supplier is not to discuss Corning INFORMATION using unsecured communication (e.g., two-way radios, cell phones etc.).

f. Corning reserves the right to require scanning of any computing or storage devices brought into a Corning facility for the purpose of interaction with Corning facility or manufacturing equipment. Once scanned and approved by Corning for use in the facility, these devices will be quarantined in the facility for the duration of the work, will not be connected to the

internet. Corning reserves the right to inspect and delete data acquired during the time the devices was on site up to and including a full re-formatting of the device memory.

Record of Revisions (managed by Document Administration):

Version #	Date Revised (xx/xx/20xx)	Revision Summary: Page(s) affected	Initiator (Last name, First name)	Approvals (N/A, Policy Owner Name, Document Owner Name, Full Approval- list all names)
V1	7/26/2019	Annual Review 2019 – Links updated	Estep, Jeanne E	Estep, Jeanne E
V2	11/2/2021	Project Shield update	Ball, Laura	Ball, Laura
V3	12/11/2023	Annual update – 2023	Bray, Stella	Bray, Stella – Director Supply Management Sustainability; Weeks, Amber – IT Manager