**INFORMATION SECURITY RISK MANAGEMENT REQUIREMENTS FOR ALL CORNING SUPPLIERS**

**Purpose:**

The document sets the standards to 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 framework applies to all worldwide locations of suppliers and it's employees include contingent labor.

**Enforcement:**

Compliance with this guidelines is mandatory. Failure by Supplier personnel or subcontractors to comply may result in corrective action, removal of access to Corning Information, termination of engagement, or other actions as required by Corning.

**Supplier Rules of Engagement**

1. Supplier shall ensure that all personnel with access to Corning Information are aware of Corning's information security requirements and complete any required information security training as specified by Corning.
2. Supplier shall ensure that Corning Information is disclosed only to authorized personnel on a strict Need-to-Know basis and solely for Corning business purposes.
3. Supplier shall ensure that all hardcopy Corning Information is secured at the end of each workday.
4. Supplier shall ensure that all Corning Information printed or copied:
    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 classified as Confidential- Corning (L3) (unless otherwise instructed by the supplier's sponsor).
5. Supplier shall ensure that all Corning information is disposed of properly using approved methods, including:
    a. Permanent deletion of electronic files so they cannot be recovered
    b. Secure erasure or physical destruction of electronic storage devices
    c. Destruction of paper documents via incineration or crosscut shredding (maximum 3/16 inch × 2 inches)
6. Corning Information shall not be left unattended in conference rooms, on whiteboards, flip charts, hand-outs, copiers, or printers.
7. Supplier shall not release Corning Information to any other supplier or third party without prior written consent from Corning.
8. At the end of a project or engagement, Supplier shall ensure that all Corning Information , weather is 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 containing Corning Information are physically secured
    b. Devices are secured using cable locks or stored in secure location
    c. Screen locks are used when systems are unattended and privacy screens are used where applicable
    d. Electronic storage devices containing Corning Information are password-protected and encrypted
    e. Corning Information is shared only via Corning-approved secure methods
    f. No Corning Information is stored in cloud-based environments without prior written approval from Corning
    g. Any Corning-provided systems are used in compliance with Corning IT policies
10. Secure Behaviors
    a. Not discuss Corning Information in public or unsecured locations
    b. Not post Corning Information on the internet or social media
    c. Immediately notify Corning of any attempt by a third party to:
        i. Obtain Corning Information
        ii. Request quotes or attempt to order Corning custom equipment or materials
    d. Report any improper disclosure, loss, or suspected compromise of Corning Information promptly and cooperate fully in investigations
11. Physical Security
    a. Supplier locations must have implement appropriate physical security controls, including:
        i. Facility access controls
        ii. Visitor management procedures
        iii. Restricted areas to prevent unauthorized access to Corning work
12. Imaging & Mobile Devices
    a. Supplier shall maintain an imaging policy that controls:
        i. Imaging devices (e.g., cameras)
        ii. Image storage media
        iii. Image handling and retention
    b. Use of smart devices is restricted as follows:
        i. No image capture of Corning equipment or information
        ii. No storage of Corning Information on non-approved devices
        iii. No mobile hotspots in Corning restricted areas

13. Oversight

Supplier acknowledges that Corning reserves the right to:

a. Require a written compliance plan prior to providing Corning Information
b. Audit Supplier compliance with these Rules of Engagement
c. Require corrective action plans for any identified deficiencies

14. Use of Subcontractors (Third Parties)

Supplier shall:

a. Ensure all subcontractors with access to Corning Information are bound by NDAs equivalent to Corning requirements.
b. Ensure subcontractors working on Corning sites execute separate NDAs with Corning where required.
c. Accept full responsibility for subcontractor compliance with this policy.
d. Acknowledge Corning's right to audit subcontractors.

15. When on a Corning Site

Supplier personnel shall:

Comply with all Corning site access policies

a. Not bring imaging or scanning devices without an approved Imaging Device Pass
b. Not enable mobile hotspots in restricted area
c. Access only authorized areas using Corning-issued badge
d. Not discuss Corning information using unsecured communications
e. Comply with Corning device scanning, quarantine, and inspection requirements