CORNING

Supplier Information Security

Information protection is everyone's responsibility

Stop.Think.Protect

As a Corning supplier, it is important to understand, and know how to apply, Corning's Information Security policy and procedures, including our Rules of Engagement.

Corporate Espionage – The Threat is Real!

?!

Corporate espionage carries a very high cost. Exact figures are not known, but it is estimated that on an average annual basis, it costs the global economy hundred of billions of dollars, millions of jobs, and creates a significant drag on GDP growth. Corning's competitors are interested in learning as much as they can about us as they try to gain a competitive advantage. We appreciate demonstrated secure behaviors by our suppliers and factor this into our supplier selections.

What Our Competitors Want to Know

Information regarding Corning technology and custom equipment	Commercial / financial analyses	Corporate financial health	Raw materials used by Corning	Sales and market share data	Details about new Corning Incorporated products that are not public knowledge

Key Tips from Corning's Rules of Engagement

Failure to comply with Corning's Supplier Rules of Engagement may result in penalties or implications for future business.

1. Ensure Corning information is shared only on a "Need to Know" basis as required to complete Corning assignments.
2. At the end of a project, all Corning information must be certified as permanently destroyed or returned to Corning.
3. Do not leave Corning information unattended and secure all hard copy Corning information at the end of each day.
4. Secure all electronic versions of Corning information via encryption and password protection.
5. Transmit Corning information only via secure methods approved by Corning.
6. Mark all Corning information with the proper document classification (see page 2).
7. Control physical spaces to prevent unauthorized access to areas with Corning equipment or work-in-progress.
8. Never discuss Corning information in public, post on the internet/social media, or release to another supplier without prior written consent.
9. Comply with Corning's on-site access control policies and procedures.
10. Report any improper disclosure of Corning information to Corning promptly.
11. Authorized subcontractors are obligated to protect Corning's confidential information and will comply with Corning's rule of engagement

Global Supply Management

CORNING

CORNING

Supplier Information Security

Information protection is everyone's responsibility

Stop.Think.Protect

Know the Key Roles & Responsibilities for Information Security

All three parties must understand Corning's Rules of Engagement (RoE) for Supplier Information Security

Supplier

- Comply with all confidentiality agreements
- Be prepared for audits

Corning Team

- Monitor Supplier's compliance with Corning's contractual obligations

Corning's Buyer

- Manage the overall commercial interaction

Follow Corning's Document Classification Guidelines

Applies to: Information in any form
Indicates: Corning's ownership of the document, its sensitivity, and how to handle it.
General – Corning (L4) includes: all Corning work unless specifically included in other classifications

Non-Corning	General – Corning (L4)	Confidential Corning (L3)	Highly Confidential – Corning (L2)
What Is It? For non-Corning documents (not subject to NDA obligations), such as information that is created by a supplier or third party and provided to Corning as part of the normal course of business, or non-business information saved on a Corning system.	**What Is It?** All Corning employee work products, unless specifically included in other classifications. This information may require an NDA to be shared.	**What Is It?** Information developed by Corning to be shared only on a need-to-know basis with appropriate security controls (e.q. TSVR3; personal data such as names, phone numbers, addresses, etc.). This information requires an NDA to be shared.	**What Is It?** Highly sensitive information to be shared only on a need-to-know basis with additional security controls for storage, access, and disposal. This information requires an NDA to be shared.
When to Use (EXAMPLES): • Information created by supplier or 3rd-party • Vendor documents • Customer Documents • Non-business documents (e.g., grocery list, etc.)	**When to Use** (EXAMPLES): • Job Descriptions • Communication to vendor for first time • Meeting notes – dependent on topic • Organization Announcements • Intranet content	**When to Use** (EXAMPLES): • Product development plans • Plant SOPs • Budgets & forecasts • Personal data (e.q. names, addresses, etc.) • TSVR3	**When to Use** (EXAMPLES): • Manufacturing costs, margins and pricing • Capital & financial planning • Critical supplier lists • Proprietary Corning equipment drawings • TSVR2

Microsoft Information Protection Controls			
Unencrypted *Use when saving content in repositories MIP can't be used or for sharing unrestricted content*	**Encrypted** *Used for internal only (@corning.com)*	**Custom** *Used to restrict access to content to a specific subset of people*	**Do Not Forward** *Used to control access of email content*

Thank you for doing your part to protect Corning's information!