1.0 Change History

Revision	Date	Change Details	Who Changed
A	06/10/2026	Initial Release	M. Cavinder

2. Purpose

Core Molding Technologies Inc. expects its suppliers, contractors, service providers, consultants, and cooperation partners to protect Core information, systems, equipment, facilities, and confidential business information when providing goods or services to Core.

These requirements define the minimum information security and confidentiality responsibilities expected of suppliers working with Core.

3. Scope

These requirements apply to any supplier, contractor, service provider, consultant, cooperation partner, or subcontractor that:

- Receives Core information;
- Accesses Core systems, networks, applications, equipment, or facilities;
- Processes, stores, transmits, or manages Core information;
- Provides external IT, cloud, hosted, managed, or shared services to Core;
- Has access to confidential, internal, customer, technical, financial, employee, production, or business information.

4. Confidentiality and Non-Disclosure

Suppliers must protect Core information from unauthorized access, use, disclosure, modification, loss, destruction, or misuse.

Where required by Core, suppliers must sign a non-disclosure agreement or ensure confidentiality obligations are included in an approved contract, purchase terms, statement of work, or other written agreement before confidential information is shared.
Suppliers may only use Core information for the approved business purpose for which it was provided.

5. Supplier Information Security Responsibilities

Suppliers are expected to maintain appropriate information security controls based on the nature of the service provided and the sensitivity of the information accessed.

Suppliers must, where applicable:

- Limit access to Core information to authorized personnel with a business need;
- Protect accounts, passwords, credentials, and privileged access;
- Use reasonable technical and organizational controls to protect Core information;
- Prevent unauthorized disclosure, alteration, loss, or destruction of Core information;

- Comply with applicable legal, regulatory, contractual, and customer requirements;
- Ensure personnel handling Core information understand their confidentiality and security responsibilities;
- Notify Core of material changes that may affect the security of the service provided.

6. External IT, Cloud, Hosted, and Shared Services

Suppliers providing external IT services, cloud services, SaaS platforms, hosted systems, managed services, or shared infrastructure must ensure Core information is appropriately protected.

Where applicable, suppliers must maintain controls for:

- Access control and authentication;
- Secure administration and privileged access;
- Segregation of Core information from other customers or tenants;
- Encryption or equivalent protection for sensitive information;
- Logging, monitoring, and incident detection;
- Backup, recovery, and availability of services;
- Secure deletion, return, or export of Core information when the service ends.

7. Subcontractors

Suppliers must not provide Core information or system access to subcontractors unless permitted by contract or approved by Core.

Where subcontractors are used, suppliers remain responsible for ensuring subcontractors protect Core information and comply with confidentiality and information security requirements at least equivalent to those agreed with Core.

8. Security Evidence and Review

Core may request evidence that a supplier has appropriate information security controls in place.

Evidence may include, but is not limited to:

- Security questionnaire responses;
- SOC 2 report;
- ISO 27001 certificate;
- TISAX label;
- Security attestation;
- Audit report;
- Other equivalent evidence acceptable to Core.

Core may review supplier security requirements periodically or when there are material changes to the supplier relationship, service, access, or information handled.

9. Security Incident Notification

Suppliers must promptly notify Core of any actual or suspected security incident that may affect Core information, systems, services, accounts, or access.

The notification should include known details of the incident, information affected, actions taken, and any support required from Core.

10. Return or Deletion of Core Information

When the supplier relationship, service, contract, or approved access ends, suppliers must return, delete, or securely dispose of Core information as required by Core or by contract.

Suppliers must also support removal of access to Core systems, facilities, applications, or data where applicable.

11. Compliance

Failure to meet these requirements may result in corrective action, suspension or removal of access, contract action, or termination of the supplier relationship.

Core may update these requirements periodically to reflect changes in business, legal, regulatory, customer, or information security requirements.