Confidential Information Protection Requirements for Corteva Suppliers

Purpose

This document sets forth Corteva requirements for protecting and maintaining confidential information provided to Corteva Suppliers.

Definition

Confidential information means all technical or business information (including data and documentation) that: (a) is disclosed to, accessed by or otherwise learned by a Supplier in connection with the provision (or potential provision) of services or products to Corteva; (b) is marked or indicated as confidential (or with words of similar meaning) or would reasonably be expected to be confidential; and (c) is not information:

(i) that is or becomes known to the public through no fault of the Supplier, its employees, or agents;
(ii) that is disclosed to the Supplier by a third party who has a lawful right to disclose the information;
(iii) that is already known to the Supplier prior to receipt of the information from or through Corteva as shown by the Supplier's prior written records; or
(iv) that is independently developed by or for the Supplier without the use of the disclosed information.

Confidential Information Classifications

Confidential information made available to a Supplier will be classified as "Confidential" or "Special Control". These classifications determine what control measures are required for proper maintenance of the confidential information. The measures that a Supplier must take to maintain the confidentiality of Corteva confidential information are based on the classification of the information.

- **Confidential.** Non-public information designated as confidential or proprietary or that would be reasonably expected to be confidential.
- **Special control**. Non-public information of high sensitivity that is designated as special control.

All Corteva non-public information provided to a Supplier is intended to be kept internal to Corteva and to third parties under obligation to maintain confidentiality. Accordingly, the Supplier should maintain all nonpublic Corteva information as *Confidential* unless specifically marked otherwise.

General Protection Requirements

- **Need-to-know**. "Confidential" and "Special Control" information may be disclosed only to those individuals who need access to the information in order to be prepared to take a specific action or to perform a specific task in accordance with their assigned job functions and responsibilities. Others must not be given access to the information.
- **Maintenance and Disposal**. Supplier must handle Corteva "Confidential" and "Special Control"
  information according to the classification of the information. See Handling of Information below. Supplier must provide prompt notice to Corteva of any inadvertent disclosures of Corteva "Confidential" or "Special Control" information.
- **CISO/DISO Access Agreement**. Before being granted access to any portion of the Corteva electronic network, Supplier must sign a Corteva Information Security Organization (("CISO,") (formerly DuPont Information Security Organization ("DISO"))) access agreement (DISO 4E).
- **Computer Equipment.** Computers of Supplier that are used to connect to the Corteva Network are subject to CISO security policies; and laptop computers on which Corteva "Confidential" or "Special Control" are stored must be disk encrypted.

- **Electronic Transmission**. Each fax transmission and e-mail message sent by Supplier that includes “Confidential” or “Special Control” information obtained from Corteva must include a message that the outgoing fax or e-mail may contain privileged or confidential information, and that if the fax or e-mail is received by someone other than the intended recipient, the communication should be disregarded and the fax or e-mail message should be returned to the Supplier.
- **Travel**. Supplier shall not travel with Corteva information classified as “Confidential” or “Special Control” unless the information is required to complete the business purpose of the travel. When travel with such information is required, Supplier must maintain control of the information at all times.
- **Recording**. Supplier shall not use recording devices such as cameras (including cameras in cellular telephones) and tape recorders on Corteva premises except with the clear written approval of Corteva site management.
- **Entry Control.** All Supplier employees must present identification as required by the Corteva site. A Corteva issued ID is preferred. Supplier employees must follow site policy regarding display of ID.
- **Limited Access.** Access to Corteva plants, buildings and areas where confidential information is generated or stored is restricted to those Supplier employees having access authorization of Corteva site management.
- **Third Party Confidential Information.** Supplier employees shall not enter Corteva premises with any third party confidential information without the express consent of the third party owning the confidential information.
- **Training.** Supplier employees who will have access to Corteva “Confidential” or “Special Control” information shall be made aware of these Confidential Information Protection Requirements for Corteva Suppliers. Additionally, if a DISO 4E electronic access agreement is required for the work being performed by the Supplier or their employees or agents, Suppliers must train their employees on Corteva electronic information security rules prior to being granted access to Corteva electronic systems.
- **Completion of Assignment.** When an employee of Supplier who has had access to Corteva “Confidential” or “Special Control” information completes an assignment for Corteva, Supplier shall remind the employee that:
  - Corteva “Confidential” or “Special Control” information has been disclosed to them;
  - Supplier employee is obligated not to reveal Corteva “Confidential” or “Special Control” information and not to use such information for themselves or others;
  - Supplier employee must not retain Corteva “Confidential” or “Special Control” information in any form; and
  - Supplier employee must return any Corteva “Confidential” or “Special Control” information to Corteva.

Handling of Information

Protective measures for information handling vary by classification. These are detailed in the table below. Suppliers with questions about the appropriate actions they should take related to Corteva information should contact their contract administrator. If further assistance is required, Supplier should contact their Corteva Sourcing buyer of record.

Process	Confidential	Special Control
Access Control		
Hard Documents	Control access to paper copies to those with a need to know	Control access to those with a need to know and log paper copies by name
Electronic Documents	Control electronic access to those with a need to know	Control electronic access to those with a need to know and log who accesses
Web Site Access	Limit access to those who need to know	Control and log accesses by name and password
Encryption	Stored electronic information should be encrypted	Stored electronic information shall be encrypted
Electronic Transmission	Consider encryption when sending electronically	Use encryption when sending electronically
Computer Room Physical Security	Secure computer room with Access control	Secure computer room with accesses logged
Physical Protection		
PC Protection	Device startup login with password required. Computer locking software (including screen blanking) required	Device startup login with password required. Computer locking software (including screen blanking) required
Laptop Computer Protection	Encryption required	Encryption required
Cellular & Cordless Phone Usage	Encryption recommended	Encryption required
Information Disposal Policy	Incinerate or shred paper so that it cannot be reassembled for reading, reformat or physically destroy removable storage media & clean hard drives	Incinerate or shred paper so that it cannot be reassembled for reading, reformat or physically destroy removable storage media & clean hard drives
Paper Mail	Sealed, confidential envelopes for internal mail with full return address. For external mail, use a secure delivery service such as USPS Registered Mail	Preferred overnight couriers that provide tracking capability (both internal and external mail)
Access Control for Hard Copies	Store hardcopy & removable electronic media in lockable furniture.	Store hardcopy & removable electronic media in lockable furniture.
Backup Storage	Physically store backup copy off site	Physically store backup copy off site
Disaster Recovery, if applicable		
Backup Frequency &Testing	Backup as needed to protect against loss, but at least every two days; test at least yearly	Backup as needed to protect against loss, but at least daily; test at least yearly
Plan	Recommended to have written plan	Must have written plan
Testing of Plan	Test at least yearly if plan exists	Test at least yearly (2 times per year recommended)
Prevention/Mitigation	Disaster prevention/mitigation techniques are required	Disaster prevention/mitigation techniques are required
Backup Power Systems	Time limited protection - test yearly	Long time protection – test monthly