# PRIVACY POLICY

## 1. PURPOSE AND SCOPE OF THIS POLICY

This Privacy Policy (the "Policy") sets forth Trinseo's commitment to protect the privacy of personal information that Trinseo collects from employees, contractors, suppliers, customers or business partners in the course of operating its business. The Policy, along with the Information Security Policy, is intended to prevent and mitigate any unauthorized disclosure of personal information or identity, guide the response to any such information security breaches, and establish proper destruction practices for paper and electronic records containing personal information.

Trinseo is committed to complying with all legal requirements regarding the privacy of personal information, including notice, transfer, security, data integrity, and access. Trinseo will periodically review its personal information collection, use, retention and disclosure practices, and revise as necessary, in order to assure compliance with laws and regulations.

In general, the personal information protected under this Policy is information capable of being associated with a particular individual through one or more identifiers. Common identifiers include a Social Security number, a driver's license number, a state identification card number, a bank account number, a credit or debit card number, a passport number, an alien registration number or a health insurance identification number. Personal information generally does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media. To the extent allowed by applicable legal requirements, employees and contractors using Trinseo computers and other devices for personal use, should have no expectation of privacy with respect to such information.

**Notice of the Use of Personal Information**

Trinseo necessarily provides certain personal information of its employees to several health, dental and life insurance companies, and possibly to other providers of services or products for our employees' benefit. In doing so, it is Trinseo's policy to select and retain only third-party service providers that are committed to and appear capable of reliably maintaining appropriate security measures to protect personal information.

Trinseo will give notice when personal information is collected for other purposes consistently with applicable law. All notices will explain the need for the information and describe how the information will be used. To the extent required by applicable law, Trinseo will maintain procedures to assure that sensitive information is collected with explicit consent.

Trinseo will collect and use personal information consistent with the notices that have been provided. However, Trinseo may decide to remove identifiable features from collected personal information and the resulting information may then be used for statistical, historic, scientific or other purposes consistent with applicable law. Trinseo will maintain reasonable procedures

consistent with applicable law for individuals to gain access to their collected personal information and, when appropriate, correct any information that is inaccurate or incomplete, or have their personal information deleted.

Trinseo will require others who acquire or provide personal information from or to Trinseo, including those engaged to provide support services, to appropriately protect personal information. Trinseo will, as permitted or required by law or court order, collect, use, transfer and/or disclose personal information pursuant to procedures that do not require giving notice (for example, in connection with law enforcement investigations).

## 2. MEASURES TO PROTECT PERSONAL INFORMATION

### Building Security

Trinseo's facilities are required to have building security measures that restrict the ability of non-employees to enter Trinseo premises where personal information may be located, without authorization or supervision. Trinseo's data centers are subject to additional security precautions and security arrangements to prevent any unauthorized access to, review of, or usage of personal information contained in those locations. Personal information that Trinseo collects must be contained in secure cabinets or computer files, all of which are to be locked when unattended or not in use. In addition, Trinseo will make all commercially reasonable efforts to assure that any off-site storage facilities used to maintain personal information are secure.

### Limitations on Disclosure and Collection of Personal Information

This Policy prohibits the disclosure of personal information or confidential information of any kind to unauthorized persons, and to any person for any purpose which has not been duly authorized under Trinseo's corporate governance procedures.

Trinseo or its vendors also use security measures that limit access to personal information contained on the payroll system, in Workday, and on Company computer hard drives.

In addition, under this Policy Trinseo seeks to request of applicants, employees, vendors and customers only personal information necessary to its business purposes and to safeguard that information from unauthorized or inadvertent disclosure as set forth above.

## 3. COMPUTER SYSTEM AND DEVICE SECURITY REQUIREMENTS

### In General

It is Trinseo's policy to protect personal information and confidential information by an extensive range of security measures. These measures may include, at a particular Trinseo facility, any of the following: (1) secure user identification protocols; (2) secure access control measures; (3) encryption of records and data containing personal information; and (4) encryption of personal information stored on laptops and portable devices. Trinseo's Information Security Policy and supporting standards further provide for the development of effective standards and guidelines to protect Trinseo information assets and personal information and respond to security breaches. These standards and guidelines include user identification protocols, asset acceptable

use and device protection standards, access control measures and virus protection and each employee and contractor are required to strictly adhere to these policies and standards.

## Prevention of Potential Identity Theft

Trinseo, of necessity, collects some personal information on its employees and applicants for employment. Trinseo may, from time to time, receive and maintain at least some personal information concerning individual contractors, vendors or customers. Measures to prevent any such theft or misuse are set forth in Trinseo's Information Security Policy.

# 4. MITIGATION OF HARM AND EMPLOYEE DISCIPLINE

### Notices from Employees, Customers, Theft Victims or Law Enforcement

If Trinseo receives information regarding possible theft, misuse or improper disclosure of personal information from an employee, from another potential identity theft victim or from law enforcement officials, Trinseo will respond promptly to that notice. Trinseo will exercise all commercially reasonable efforts to prevent, alleviate or mitigate any harm that may result from the theft, misuse or improper disclosure of personal information. Trinseo will also comply with applicable notification or remediation requirements of the jurisdiction in which any theft or misuse occurs. To the extent any personal information is improperly disclosed by Trinseo, Trinseo will comply with applicable laws, rules and regulations governing such disclosure. Appropriate standards for security breach prevention and response will be provided under Trinseo's Information Security Policy.

### Complaints

Any complaints regarding potential deviations from its established procedures for protecting personal information should be immediately reported to your supervisor, the Chief Compliance Officer or your Human Resources Manager. Complaints may also be reported anonymously to the Trinseo Hotline toll free at 1-866-853-3802 in the United States or Canada The Ethics Hotline is also available in other languages and countries, with a list available at https://secure.ethicspoint.com/domain/media/en/gui/28803/index.html

### Employee Discipline

A breach or violation of this Privacy Policy may result in discipline of any employee(s) involved, up to and including termination of employment. In addition, it is possible that a breach or violation of this Policy may result in civil litigation against or criminal prosecution of the employee(s) involved.

## 5. DESTRUCTION OF PERSONAL INFORMATION RECORDS

This Policy requires the proper and effective disposal of records containing personal information at the end of their retention period. Specifically, personal information on paper records should be redacted, burned, pulverized or shredded prior to disposal. Similarly, electronic data containing personal information should be destroyed or erased so that personal information cannot practicably be read, retrieved or reconstructed.

## 6. CHANGES TO POLICY AND NOTICE OF ADDITIONAL USE

If the terms of this Policy are modified, expanded or otherwise altered, the changes will promptly be posted on Trinseo's Intranet and Trinseo will take other measures reasonably designed to assure that Trinseo employees receive notice of any such changes to the Policy. If Trinseo should be legally required, or determines that it is necessary and legally permissible, to use personal information for a purpose other than or in addition to the purpose for which the information was originally collected, Trinseo will notify and/or obtain the consent of such employee, contractor, vendor or supplier to the extent that such notice and/or consent is legally permissible and appropriate in the circumstances.