Contents

1 PURPOSE

The Vendor Information & Cyber Security Assurance Policy (the "Policy") sets forth how Tronox intends to manage the information and cyber security risks posed by the use of third party vendors. The Policy is intended to minimize the likelihood of security breaches and the associated potentially negative consequences for Tronox's operations, employees, customers and other stakeholders. Tronox relies on its third-party vendors for a wide range of various services and products and retains third parties for many reasons including to reduce costs, provide technical expertise not available internally, and increase speed to market with new products or offerings. However, working with third party vendors can increase Tronox's cyber vulnerability in numerous ways:

- Unauthorized access to our data and systems
- Loss of sensitive business data including intellectual property
- Potential privacy impacts relating to employees, customers or other third parties
- Impacts to business operations and product quality
- Accidental or malicious actions can impact upon site safety and local communities
- Reputational harm through the misuse of sensitive or confidential data
- Regulatory and Compliance impacts of security breaches

2 SCOPE

This Policy applies to all Tronox Vendors retained after October 31, 2022 and any existing vendor's whose agreement with Tronox is renewed October 31, 2022 ("Covered Vendors"). Additionally, Tronox will seek to identify existing vendors deemed High ITC Risk (as defined below) and take appropriate corrective action where permitted by existing agreements and local law to mitigate the risk of cyber breaches caused by such vendors.

3 POLICY

Risk Tiers

All Covered Vendors will be assessed by Tronox's cyber security organization or its designees and will be classified as High ITC Risk, Medium ITC Risk and Low ITC Risk.

High ITC Risk Vendors

High ITC Risk vendors pose the highest degree of risk and require the largest degree of ongoing due diligence. Vendors that fall under this tier generally have unfettered access to Tronox systems, facilities and/or hold large amounts of Tronox data and/or have the ability to impact upon safety and product quality.

High ITC Risk Vendors will be classified using criteria, including:

1. Does the Vendor supply a system providing a critical function that is likely to have a material impact upon site safety and product quality if that system or service doesn't function as expected?

2. Does the Vendor have remote access to and/or unsupervised access to Tronox's data storage systems, operational technology including process control systems whether virtually or on site?

Medium ITC Risk Vendors

Medium ITC Risk vendors have some access to company systems and data. Vendors that fall under this tier generally have controlled access to Tronox facilities / data or are a single source supplier or supplier of scarce goods/services.

Medium ITC Risk Vendors will be classified using criteria, including:

1. Does the Vendor have remote access to Tronox systems for administration or system management purposes?

2. Does the Vendor store and/or process Tronox sensitive data, including non-public information?

Low ITC Risk Vendors

Low ITC Risk vendors generally pose little risk to Tronox and hence do not warrant additional scrutiny above and beyond our Supplier Code of Conduct.

Management of Vendors

The security controls and assurances which Tronox will require of its Vendors will depend upon the classification of Vendor (i.e., High, Medium, Low); and the nature of the Services and/or Products they supply; and will be generally dictated by Tronox Vendor Security Standards and Procedures; and enforced by appropriate contractual measures; which may include but is not limited to:

- Evidence of technical security controls, including for networks, infrastructure and applications
- Evidence of non-technical security controls, policies, procedures and working practices
- Evidence of independent technical testing and third-party assurances
- Disclosure of Information Security Management System (ISMS), or equivalent

- Disclosure of Cyber Security Management System (CSMS), or equivalent
- Disclosure of Vendor personnel involved, including their qualifications, professional registrations and competencies
- Tronox right to audit
- Tronox right to veto Vendor personnel and systems
- Evidence of formal security certifications and accreditations, e.g., ISO 27001 certificates and Statement of Applicability (SoA)
- Depending on nature of risk, regular monitoring by Tronox to ensure up to date compliance, monitoring may include such things as:
    - Financial statements or annual reports
    - Control Audits such as SOC1, SOC2, or SSAE16
    - Insurance or bonding certificates
    - provide high if any limitation of liability
    - provide for indemnification in case of certain breaches
    - Disaster recovery tests or policies
    - Regular examination of vendor's facilities

Any noncompliance by a vendor with the Tronox Vendor Security Standards and Procedures will require an informed risk assessment decision made jointly by the Tronox procurement and cyber-security organizations.

4 CONSEQUENCES

A breach of this Policy may result in disciplinary action up to and including termination of employment. Violations of this policy may expose Tronox to significant business interruption, legal penalties and fines, and reputational harm. Intentional misconduct may also expose the Company and responsible employees to criminal enforcement action by government authorities.

5 POLICY REVIEW AND EXCEPTIONS

The Chief Information Officer will approve any revisions or exceptions to this policy.

6 RELATED INFORMATION

The policies related to IT can be found in the "Global Policy and Guidelines Library" section of the Intranet (https://intro.tronox.com/). Employees are responsible for reading the Company's policies.

.