VONTIER INFORMATION SECURITY POLICY STATEMENT

Our Information Security Mission

Vontier is committed to protecting the confidentiality, integrity, and availability of information and data that are critical to our products, services, customers, and stakeholder trust. This policy sets mandatory requirements to safeguard information assets, implement data protection controls, and manage cybersecurity risks. We are dedicated to the continuous improvement of our security posture, regularly assessing and enhancing controls, monitoring performance, and applying lessons learned to ensure compliance with applicable laws, regulations, and industry best practices.

Information Security Scope and Capabilities

The Information Security program covers both enterprise environments, including back-office systems and corporate infrastructure, and secure product development and delivery. Our unified approach safeguards all information assets supporting internal operations and customer-facing solutions.

Key capabilities and requirements applied consistently across enterprise and product domains include:

- **Secure Lifecycle Integration:** Embedding security controls throughout design, development, deployment, and maintenance, supported by threat modeling, risk assessments, and application security testing.
- **Robust Security Architecture:** Implementing technical and operational controls across systems, networks, and infrastructure to mitigate threats.
- **Identity and Access Management:** Enforcing strong authentication, least privilege access, and centralized account management to restrict access to authorized personnel across Vontier and its Operating Companies.
- **Endpoint and Network Security:** Applying encryption, patch management, malware protection, network segmentation, intrusion detection, and continuous monitoring.
- **Data Security and Privacy:** Protecting sensitive data through encryption, classification, secure disposal, and compliance with privacy laws and Vontier policies.
- **Operational Resilience:** Developing and regularly testing business continuity, disaster recovery, and incident response plans to ensure rapid recovery and operational continuity.

- **Third-Party Risk Management:** Assessing vendors and partners through formal security evaluations and contractual requirements. This includes assessing third parties to determine adherence to Vontier's data protection standards.
- **Continuous Monitoring and Vulnerability Management:** Conducting threat detection, vulnerability assessments, penetration testing, and coordinated incident response.
- **Security Awareness and Training:** Providing role-based cybersecurity education, including general training, phishing simulations, and specialized instruction for high-risk roles.

These capabilities apply to:

- Internal IT systems, networks, endpoints, applications, and data supporting Vontier and its Operating Companies.
- Back-office corporate environments.
- Secure product development processes, including supply chain security.

By integrating these capabilities, Vontier maintains a strong security posture that protects information confidentiality, integrity, and availability across all business areas. These capabilities and policies are regularly reviewed to keep pace with industry trends and practices.

Governance and Accountability

Information Security, Legal, and Risk leadership is responsible for enforcing this policy, managing compliance, and reporting security posture and risks to senior management and the Board of Directors.

Employee Responsibility

All employees, contractors, and partners must understand and comply with this policy as well as all related internal policies. Protecting information assets and maintaining trust requires vigilance and proactive engagement from everyone.

Policy History

Date of Change	Responsible Party	Summary of Change
26 September, 2025	Vontier Information Security	Initial Creation