VONTIER™

Information Security Policy

Information Security Policy

Version 1.0 Final
(Effective Date: 1/1/2023)

Contents

1. Introduction

1.1. Purpose

The purpose of the Information Security Policy is to establish requirements for the Vontier Information Security department and program to address risks related to the Confidentiality, Integrity, and Availability of Vontier information and systems. The Information Security Policy is the primary document for the Information Security Policy Portfolio. The underlying policies, standards and related documents are designed to address specific areas of information security and related requirements.

1.2. Scope

This Policy applies to all Vontier and its Operating Companies ("OpCos") employees globally, including any subsidiary or joint venture in which Vontier has a majority interest or otherwise controls (hereafter individually or collectively, "Vontier"). This includes contractors, consultants, temporary employees who handle or maintain Vontier information.

1.3. Ownership

The Vontier Chief Information Security Officer (CISO) is owner of Corporate-level Information Security policies and standards and therefore authorized to track and store exceptions and responsible for providing interpretations. The CISO may delegate a function within the Information Security department to provide interpretations on their behalf, where appropriate. The Vontier Information Security Executive Committee (Executive Committee) has oversight on Corporate-level policies and standards.

1.4. Compliance

To the extent local regulatory requirements governing information security or privacy are more stringent than those contained herein, such local requirements will prevail.

Any areas of non-compliance with this policy must be documented and follow the Vontier Information Security policy and standard exception process. The Information Security department is authorized to track and store Information Security policy and standard non-compliance.

Failure to comply with this policy could result in disciplinary actions including, but not limited to termination of employment.

1.5. Review

Information Security will review the contents of this Policy at a minimum annually. At the discretion of the CISO, more frequent reviews may occur if warranted by organizational and/or industry standard changes.

3. Information Security Program

An Information Security program shall be established with intent of mitigating Cybersecurity risk posed by threats to the confidentiality, integrity, and availability of Vontier information systems and business operations. The program will:

- Define a governance structure, including policies, standards, guidelines, and procedures.

  Governance is the responsibility of Executive Management and consists of leadership, organizational structures, and processes to ensure that Vontier's information technology sustains and extends its strategies and objectives.

  Information Security policies and standards represent the foundation for Vontier's Information Security program, and establish overarching requirements for the use, management, and implementation of information security throughout Vontier. Procedures will be established, based on requirements from the framework chosen.

- Establish Executive Steering committee

  Executive Management has formed an Executive Committee to lead the efforts to ensure Vontier is appropriately protected from Information Security and Governance, Risk and Compliance deficiencies. The Executive Committee will have the authority to recommend Policies and Standards for approval or revision, determine needs for other guiding documents, and ensure gaps are closed or minimized.

  The authority granted by Executive Management to the CISO for evaluating and advising on information security risks is not superseded by this Steering Committee. Any guidance provided to the CISO, and Executive Management is advisory only in nature. The CISO can grant the Committee authority over organizational-level initiatives, at his written request.

- Maintain qualified leadership and staff

  Vontier shall designate an executive role to be responsible for the Information Security function. This role shall be referred to as the Chief Information Security Officer (CISO) or equivalent. Among the many duties of a CISO will be implementing and overseeing Vontier's cybersecurity program; aligning cybersecurity and business objectives; reporting on cybersecurity and promoting a strong culture of information security. The CISO, at his discretion, may delegate some of these responsibilities to the Executive Committee for execution. The CISO must maintain a team of qualified Information Security professionals to support the Vontier Information Security Program.

- Define information security strategy

  Information Security shall 1) Define and document the information security strategy, that identifies key strategic projects and initiatives, 2) Demonstrates their alignment to the business strategy and 3) Provide a clear roadmap for information security aligned with the risk appetite of the Corporation.

- Monitor and report information security risk and status to Vontier senior leadership and Board.

  Information Security Program shall monitor operations and organization-wide initiatives to identify information security risk. The CISO shall report as necessary security posture and risks to company leadership up to and including the Board of Directors.

- Ensure operational resilience through Incident Response and Continuity of Operations capabilities

  Business Continuity (BC), Disaster Recovery (DR), Incident Response (IR) and Enterprise Resilience capabilities with clearly defined roles & responsibilities, training, reporting processes, playbooks, and a centralized communication plan for internal and external stakeholders during and following an event (collectively known as a Plan) will be created, or existing plans updated. This includes establishing DR, BC, IR, and Enterprise Resilience processes to include Business Impact Assessments (BIA) with Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for critical applications. These Plans are to be tested and updated based on lessons learned.

- Provide awareness of the Information Security Program

  Information Security shall make users aware of the Vontier Information Security Program, information security risk and actions, best practices and techniques users may take to protect themselves and Vontier.

- Communication with the Information Security Program

  Information Security shall maintain communication methods for reporting security issues and inquiries and take steps to make users aware of these methods and escalation protocols as required by the Vontier Escalation Policy.

4. Decision Authority Related to Information Security Program

The confidentiality, integrity, and availability of Vontier systems and data is critical to on-going, successful operations of the organization. Whether conducting normal operations or responding to a cyber incident the CISO and his/her delegates within the Vontier Information Security team have decision authority related to cybersecurity controls and countermeasures, including but not limited to:

- **Disablement / removal of information security controls**

  Disabling information security controls shall be reviewed by Information Security before executed. Examples of controls may include anti-malware controls, security monitoring, creating permissive firewall rules, excluding systems/accounts from security controls, etc.

- **Making information security risk decisions**

  When a risk is identified, deciding on how to address an information security risk requires caution. The appropriate stakeholders shall decide on the treatment actions (acceptance, avoidance, mitigation and sharing or transfer) so that accountability is established for risk management. (Refer to IS Risk Assessment Standard for additional information.)

- **Remediation actions related to information security risk**

  Remediating information security issues or gaps (changes to IT systems to address vulnerabilities, reinforce security monitoring, apply multi-factor authentication, deploy security tooling, etc.) shall require information security oversight to ensure that remediation actions follow the information security recommendation and don’t introduce other vulnerabilities/weaknesses. (Refer to IS Risk Assessment Standard for additional information.)

5. Document Change History

Version	Revision Date	Summary of Changes
1.0	11/10/2022	Initial approved version

5.1. Document Creation and Approval

Author(s)	**Name / Group**
	Lee Coone - Information Security – Governance, Risk & Controls
Reviewer Name	**Group**
Larry Sobers	Information Security – CISO
Michael Sheedy, Lee Coone, Hongseok Km	Information Security – Governance, Risk & Controls
Date Approved	**Name / Group**
1/11/2023	Larry Sobers, VP & Chief Information Security Officer

5.2. Document Owner and Contact

Name/Group	Contact Details
Information Security	infosec@vontier.com

5.3. Document Effective & Review Dates

Effective Date	Next Review Date
1/1/2023	TBD

Appendix

A. Definitions

None

B. Applicable Policies, Standards, and Guidelines

Acceptable Use Policy
Asset Management Policy
Business Continuity Policy
Incident Response Policy
Application Development Security Standard
Cloud Security Standard
Cryptography Standard
Database Security Standard
Endpoint Security Standard
Identity and Access Management Standard
Information Security Risk Management and Assessment Standard
IT Disaster Recovery Standard
Network Security Standard
Security Awareness Standard
Security Baseline Configuration Standard

Third Party Cyber Risk Management Standard
Vulnerability Management Standard

C. References

NIST Special Publication 800-53, Revision 5 - Security and Privacy Controls for Information Systems and Organizations