Supplier Information Security Policy

Update: 20240514 Version 1.0

1. Introduction

VicOne Inc. recognizes the importance of information security in today's digital landscape. As part of our commitment to safeguarding sensitive data and maintaining the trust of our customers and partners, we establish this Supplier Information Security Policy to outline the expectations and requirements for our suppliers regarding information security.

2. Scope

This policy applies to all suppliers, vendors, contractors, and partners who have access to or process sensitive information on behalf of VicOne Inc.

3. Policy Statement

- Suppliers must comply with all relevant legal and regulatory requirements related to information security.
- Suppliers must implement appropriate measures to protect the confidentiality, integrity, and availability of information assets entrusted to them by VicOne Inc.
- Suppliers must ensure that their employees and subcontractors are aware of and trained in information security best practices relevant to their roles.
- Suppliers must promptly report any security incidents, breaches, or vulnerabilities that may impact VicOne Inc. to our designated point of contact. The information security contact team can be reached by sending an email to security@vicone.com.
- Suppliers must adhere to any additional requirements outlined in contractual agreements or service level agreements (SLAs).

4. Information Security Controls

Suppliers are expected to implement the following information security controls:

- Access Control: Restrict access to sensitive information on a need-to-know basis and enforce strong authentication mechanisms.
- Data Protection: Encrypt sensitive data both in transit and at rest and implement appropriate data retention and disposal procedures.
- Security Awareness: Provide regular training and awareness programs to employees on information security policies and procedures.
- Incident Response: Maintain incident response plans to effectively detect, respond to, and recover from security incidents.
- Third-Party Risk Management: Assess and manage the security risks associated with subcontractors or third-party service providers.

5. Compliance

Suppliers must demonstrate compliance with this policy and any relevant security standards or frameworks, for example, TISAX (Trusted Information Security Assessment Exchange), upon request by VicOne Inc.

6. Review and Revision

This Supplier Information Security Policy will be periodically reviewed and updated as necessary to reflect changes in technology, regulations, or business requirements.