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.

サプライヤー情報セキュリティポリシー

初版: 2024年5月14日　バージョン1.0

1. はじめに

VicOne 株式会社（以下「VicOne」）は、今日のデジタル環境における情報セキュリティの重要性を認識しています。機密データを保護し、お客様とパートナーの信頼を維持するという当社の取り組みの一環として、情報セキュリティに関する当社のサプライヤーへの期待と要件を概説する本サプライヤー情報セキュリティポリシー（以下「本ポリシー」）を策定します。

2. 適用範囲

本ポリシーは、VicOneに代わって機密情報にアクセスしたり、機密情報を処理するすべてのサプライヤー、ベンダー、請負業者、パートナーに適用されます。

3. ポリシーステートメント（方針条項）

- サプライヤーは、情報セキュリティに関連するすべての関連法規およびガイドラインその他の規制要件を遵守しなければなりません。
- サプライヤーは、VicOneから委託された情報資産の機密性、完全性、可用性を保護するために、適切な措置を実施しなければなりません。
- サプライヤーは、自社の従業員および下請業者が、各自の役割に関連する情報セキュリティのベストプラクティスを認識し、訓練を受けていることを保証しなければなりません。
- サプライヤーは、VicOneに影響を及ぼす可能性のあるセキュリティインシデント、違反、または脆弱性について、当社の指定窓口に速やかに報告しなければなりません。
  情報セキュリティ連絡チームへの連絡は、security@vicone.com まで電子メールを送信してください。
- サプライヤーは、契約またはサービスレベル契約（SLA）に記載されている追加要件を遵守しなければなりません。

4. 情報セキュリティ管理

サプライヤーは、以下の情報セキュリティ管理を実施することが必要です：

- アクセス制御：機密情報へのアクセスを必要かつ最小限の情報に限定し、強固な認証メカニズムを導入します。
- データ保護：機密データを送信中および保管中の両方において暗号化し、適切な

データ保持および廃棄手順を実施します。

- セキュリティ意識の向上：情報セキュリティ方針および手順に関する従業員への定期的な研修と意識向上プログラムを提供します。
- インシデント対応：セキュリティインシデントを効果的に検出、対応、復旧するためのインシデント対応計画を維持します。
- サードパーティのリスク管理：下請業者またはサードパーティのサービスプロバイダに関連するセキュリティリスクを評価し、管理します。

5. コンプライアンス

サプライヤーは、VicOneの要求に応じて、本ポリシーおよび関連するセキュリティ標準またはフレームワーク（例えば、TISAX（Trusted Information Security Assessment Exchange）など）への準拠を証明する必要があります。

6. 見直しと改訂

本ポリシーは、技術、規制、またはビジネス要件の変更を反映するため、定期的に見直され、必要に応じて更新されます。

7. 言語

本ポリシーは、英語で作成され、日本語に翻訳されたものです。英文版が正本であり、日本語版は参考として参照されるものです。これら両言語版の間に矛盾抵触がある場合、英文版が優先されますので、英文版も合わせて確認する必要があります。