Supplier Information Security Policy

Update: 20260831 Version: 1.1

1. Introduction

VicOne Corporation and its subsidiaries, affiliates, and associated entities (collectively, "VicOne") recognize the importance of information security. This Supplier Information Security Policy sets out the minimum information security requirements that suppliers must meet when they access VicOne systems or receive, access, store, transmit, process, or otherwise handle information owned, controlled, possessed, or used by VicOne (VicOne Information").

2. Scope

This Policy applies to all suppliers, vendors, contractors, partners, and their personnel and subcontractors that access VicOne systems or handle VicOne Information. All suppliers within the scope of this Policy shall comply with its minimum requirements. VicOne may require additional controls based on the sensitivity of the information, system access, services provided, and potential impact on VicOne.

3. Minimum Information Security Requirements

3.1 Governance and Security Awareness

- Maintain the knowledge, skills, standards, practices, procedures, and resources necessary to operate a secure IT environment.
- Maintain a documented information security policy and communicate it to personnel with access to VicOne Information or relevant systems.
- Provide information security awareness training before or promptly after access is granted and at least annually thereafter.

3.2 Access Control

- Authorize access before it is granted and restrict access to the minimum necessary for the authorized purpose and role.
- Maintain a current record of personnel, contractors, agents, and service accounts with access to VicOne Information or relevant systems and provide that record to VicOne upon reasonable requests.
- Review access periodically and promptly revoke or adjust access when it is no longer required or when a person's role or employment changes.
- Implement multi-factor authentication ("MFA") for all remote access to systems that process or store VicOne Information, and for privileged access where technically feasible.

3.3 Information Handling, Retention, and Disposal

- Retain VicOne Information only for as long as necessary for the authorized purpose or as required by applicable law or contract.
- Upon VicOne's request or termination of the applicable engagement, securely return or destroy VicOne Information, including copies, to the extent reasonably practicable, and provide written certification upon request.
- Where information remains in backups or archives, protect it from further use and delete it in accordance with the supplier's documented retention cycle, unless retention is legally required.

3.4 Data Location and Transfer

- Access, store, or process VicOne Information only at locations and through services disclosed to and authorized by VicOne where such authorization is required by contract or applicable law.
- Provide prior written notice before materially changing the country or region from which VicOne Information is accessed or in which it is stored or processed and ensure that all transfers comply with applicable data protection and cross-border transfer requirements.
- Encrypt VicOne Information transmitted across public or otherwise untrusted networks using industry-standard protocols, including TLS 1.2 or higher where TLS is used, or an equivalent secure protocol.
- Apply appropriate industry-standard encryption to sensitive VicOne Information at rest, considering the information's classification and risk.

3.5 Third Parties and Subcontractors

- Do not disclose VicOne Information to a third party except as authorized in writing by VicOne or permitted by the applicable contract.
- Before a subcontractor handles VicOne Information, conduct appropriate risk assessment and bind the subcontractor to confidentiality, security, privacy, incident notification, return, and destruction obligations no less protective than those applicable to the supplier.
- Remain responsible for the subcontractor's compliance with those obligations.

3.6 System and Vulnerability Security

- Implement reasonable measures to prevent, detect, and remove malicious software and unauthorized code.
- Maintain logging and security audit arrangements appropriate to the risk, including records sufficient to identify access to systems and VicOne Information, and protect logs against unauthorized alteration.
- Conduct vulnerability assessments at a frequency appropriate to the risk and promptly remediate identified vulnerabilities.
- Apply critical security patches without undue delay and within a risk-based timeframe documented by the supplier. Where immediate remediation is not feasible, implement and document effective compensating controls.

3.7 Business Continuity and Physical Security

- Maintain business continuity and disaster recovery arrangements proportionate to the services provided and the potential impact on VicOne. For critical services, test relevant plans at least annually and provide a summary of results to VicOne upon reasonable request.
- Protect facilities and IT environments against unauthorized physical access, theft, fire, flood, environmental hazards, and power disruption using controls appropriate to the risk.

3.8 Security Incident Management

- Maintain documented procedures to detect, assess, respond to, contain, investigate, recover from, and learn from security incidents.
- Notify VicOne at security@vicone.com immediately upon becoming aware of any confirmed or reasonably suspected security incident affecting VicOne systems, VicOne Information, or services provided to VicOne, and no later than 24 hours after such awareness.

- The initial notification shall, to the extent known, describe the nature and scope of the incident, affected information and systems, likely consequences, containment or remediation actions, and a point of contact. The supplier shall provide timely updates and preserve relevant evidence.
- Do not make public statements identifying VicOne or notify third parties on VicOne's behalf unless legally required or authorized in writing by VicOne.

4. Personal Data Protection

When processing personal data for or on behalf of VicOne, suppliers shall comply with applicable data protection laws and contractual requirements; process the data only for authorized purposes; keep the data confidential; implement technical and organizational measures appropriate to the risk; assist VicOne with data subject requests, security incidents, regulatory inquiries, and required assessments where applicable; and return or securely destroy the data as required.

5. Compliance and Assurance

Upon reasonable request, suppliers shall provide information and evidence necessary to demonstrate compliance with this Policy, such as relevant policies, training records, risk assessments, access review records, vulnerability and patch management summaries, business continuity test summaries, independent audit reports, or certifications. VicOne may consider recognized standards or frameworks, including ISO/IEC 27001 and TISAX, but certification does not by itself relieve a supplier of its obligations.

Where a supplier cannot meet a requirement, it should notify VicOne without undue delay, explain the reason and risk, and propose compensating controls. Any exception must be documented and approved in writing by VicOne's authorized representative before reliance on the exception.

6. Order of Precedence

This Policy establishes minimum requirements. If an applicable law, contract, security schedule, SLA, or written VicOne requirement imposes a higher standard, the higher standard applies. In the event of a conflict, the applicable contract's order-of-precedence clause governs.

7. Review and Revision

VicOne may periodically review and update this Policy to reflect changes in technology, threats, laws, regulations, standards, or business requirements. Suppliers shall review updates communicated by VicOne and implement applicable changes within the timeframe specified by VicOne or the applicable contract.

8. Language

This Policy is prepared in English and translated into Japanese. The English version is the authoritative version, and the Japanese version is provided for reference. If there is any conflict, inconsistency, or discrepancy between the two versions, the English version prevails.

サプライヤー情報セキュリティポリシー

改訂日: 2026 年 8 月 31 日　バージョン: 1.1

1. はじめに

VicOne Corporation ならびにその子会社、関連会社および関係法人（以下、総称して「VicOne」）は、情報セキュリティの重要性を認識しています。本サプライヤー情報セキュリティポリシーは、サプライヤーが VicOne のシステムにアクセスする場合、または VicOne が所有、管理、保有もしくは使用する情報（以下「VicOne 情報」）を受領、閲覧、保存、送信、処理その他取り扱う場合に遵守すべき最低限の情報セキュリティ要件を定めるものです。

2. 適用範囲

本ポリシーは、VicOne のシステムにアクセスし、または VicOne 情報を取り扱うすべてのサプライヤー、ベンダー、請負業者、パートナー、ならびにその要員および再委託先に適用されます。本ポリシーの適用対象となるすべてのサプライヤーは、本ポリシーに定める最低要件を遵守しなければなりません。VicOne は、情報の機微度、システムへのアクセス、提供されるサービス、および VicOne に及ぼし得る影響に応じて、追加の管理策を求めることがあります。

3. 最低限の情報セキュリティ要件

3.1 ガバナンスおよびセキュリティ意識向上

- 安全な IT 環境の運用に必要な知識、技能、基準、慣行、手順および資源を維持すること。
- 文書化された情報セキュリティポリシーを維持し、VicOne 情報または関連システムへのアクセス権を有する要員に周知すること。
- アクセス付与前または付与後速やかに情報セキュリティ意識向上研修を実施し、その後少なくとも年 1 回実施すること。

3.2 アクセス制御

- アクセス権を付与する前に承認を行い、承認された目的および役割に必要な最小限の範囲に制限すること。
- VicOne 情報または関連システムにアクセスできる要員、請負業者、代理人およびサービスアカウントの最新の記録を維持し、VicOne から合理的な要請があった場合に提供すること。
- アクセス権を定期的に見直し、不要となった場合、または役割もしくは雇用関係に変更（退職を含む）があった場合には、速やかに取消しまたは変更すること。
- VicOne 情報を処理または保存するシステムへのすべてのリモートアクセスに多要素認証（MFA）を導入し、技術的に実行可能な場合は特権アクセスにも導入すること。

3.3 情報の取扱い、保存および廃棄

- VicOne 情報は、承認された目的に必要な期間、または適用法令もしくは契約により必要とされる期間に限り保持すること。
- VicOne からの要請時または該当する業務または契約の終了時に、合理的に実行可能な範囲で、複製物を含む VicOne 情報を安全に返却または廃棄し、要請に応じて書面による証明を提出すること。

- バックアップまたはアーカイブに情報が残存する場合、法令上保持が必要な場合を除き、当該情報がそれ以上利用されないよう保護し、文書化された保存・削除サイクルに従って削除すること。

3.4 データの所在および移転

- VicOne 情報へのアクセス、保存および処理は、VicOne に開示され承認された場所およびサービスを通じてのみ行うこと（契約または適用法令により当該承認が求められる場合）。
- VicOne 情報へのアクセス元、保存先または処理先となる国もしくは地域に重要な変更を行う前に書面で通知し、すべての移転について適用されるデータ保護および越境移転要件を遵守すること。
- 公衆ネットワークその他信頼できないネットワークを介して VicOne 情報を送信する場合、業界標準のプロトコルを用いて暗号化すること。TLS を使用する場合は TLS 1.2 以上、または同等の安全なプロトコルを使用すること。
- 情報分類およびリスクを考慮し、保管されている機微な VicOne 情報に適切な業界標準の暗号化を適用すること。

3.5 第三者および再委託先

- VicOne が書面で承認した場合、または適用される契約で許可される場合を除き、VicOne 情報を第三者に開示しないこと。
- 再委託先に VicOne 情報を取り扱わせる前に適切なリスク評価を行い、サプライヤーに適用されるものと保護水準が同等以上の、機密保持、セキュリティ、プライバシー、インシデント通知、返却および廃棄に関する義務を課すこと。
- 再委託先による当該義務の遵守について責任を負うこと。

3.6 システムおよび脆弱性のセキュリティ

- 悪意のあるソフトウェアおよび不正なコードを防止、検知および除去するための合理的な措置を講じること。
- リスクに応じたログ取得およびセキュリティ監査の体制を維持すること。ログには、システムおよび VicOne 情報へのアクセスを特定するために十分な記録を含め、当該ログを不正な改変から保護すること。
- リスクに応じた頻度で脆弱性評価を実施し、特定された脆弱性を速やかに是正すること。
- 重大なセキュリティパッチを不当に遅延させることなく、サプライヤーが文書化したリスクベースの期限内に適用すること。直ちに是正できない場合は、有効な代替管理策を実施し、文書化すること。

3.7 事業継続および物理的セキュリティ

- 提供するサービスおよび VicOne に及ぼし得る影響に応じた事業継続および災害復旧の体制を維持すること。重要なサービスについては、関連計画を少なくとも年 1 回テストし、VicOne から合理的な要請があった場合に結果の概要を提供すること。
- 施設および IT 環境を、不正な物理アクセス、盗難、火災、洪水、環境上の危険および停電から、リスクに応じた管理策により保護すること。

3.8 セキュリティインシデント管理

- セキュリティインシデントの検知、評価、対応、封じ込め、調査、復旧および教訓の反映を行うための手順を文書化し、維持すること。
- VicOne のシステム、VicOne 情報、または VicOne に提供するサービスに影響を及ぼす、確認済みまたは合理的に疑われるセキュリティインシデントを認識した場合、直ちに、かつ当該認識後 24 時間以内に、security@vicone.com 宛てに VicOne へ通知すること。
- 初回通知には、判明している範囲で、インシデントの性質および範囲、影響を受けた情報およびシステム、発生する可能性のある結果、封じ込めまたは是正措置、ならびに連絡担当者を含めること。その後も適時に情報を更新し、関連証拠を保全すること。
- 法令により義務付けられる場合、または VicOne が書面で承認した場合を除き、VicOne が特定される公表を行わず、VicOne を代理して第三者へ通知しないこと。

4. 個人データの保護

VicOne のために、または VicOne に代わって個人データを処理する場合、サプライヤーは、適用されるデータ保護法令および契約上の要件を遵守し、承認された目的のためにのみ処理し、秘密として取り扱い、リスクに応じた技術的および組織的措置を講じなければなりません。また、該当する場合、データ主体からの請求、セキュリティインシデント、規制当局の照会および必要な評価に関して VicOne を支援し、要求に従って当該データを返却または安全に廃棄しなければなりません。

5. 遵守およびアシュアランス

サプライヤーは、VicOne から合理的な要請があった場合、本ポリシーの遵守を証明するために必要な情報および証拠を提供しなければなりません。これには、関連ポリシー、教育記録、リスク評価、アクセスレビュー記録、脆弱性・パッチ管理の概要、事業継続テストの概要、独立監査報告書または認証などが含まれます。VicOne は ISO/IEC 27001 および TISAX を含む公認の基準またはフレームワークを考慮することがありますが、認証のみをもってサプライヤーの義務が免除されるものではありません。

要件を満たすことができない場合、サプライヤーは不当に遅延することなく VicOne へ通知し、その理由およびリスクを説明し、代替管理策を提案しなければなりません。例外を適用する前に、その内容を文書化し、VicOne の権限ある代表者から書面による承認を得なければなりません。

6. 優先順位

本ポリシーは最低要件を定めるものです。適用法令、契約、セキュリティ付属文書、SLA または VicOne の書面による要件がより高い基準を定める場合は、当該基準が適用されます。抵触が生じた場合は、該当する契約の優先順位条項に従います。

7. 見直しおよび改訂

VicOne は、技術、脅威、法令、規制、基準または事業上の要件の変化を反映するため、本ポリシーを定期的に見直し、更新することがあります。サプライヤーは、VicOne から通知さ

れた更新内容を確認し、VicOne または適用される契約が指定する期限内に、該当する変更を実施しなければなりません。

8. 言語

本ポリシーは英語で作成され、日本語に翻訳されています。英文版を正本とし、日本語版は参考訳とします。両言語版の間に矛盾、不一致または相違がある場合は、英文版が優先されます。