コーポレートポリシー7
グローバル情報・システムセキュリティ

目的

本ポリシーの目的は、適用法を遵守したストライカーの情報、システムおよび業務における、適切なセキュリティ管理へのストライカーの誓約を表明することにあります。

適用範囲

本ポリシーは、勤務地に関わらず、ストライカーの全従業員ならびにストライカーの代理として行動する第三者（例：ベンダー、請負業者、代理店など）に適用されます。本ポリシーの条項でストライカーの特定の事業体に適用される法律に準拠しないものがある、当該事業体は、必要な範囲において、本ポリシーの補則を策定し現地や地域の法律に準拠させることができます。ただし、改定されたポリシーは、可能な限り本ポリシーに整合することを条件とします。こうした補則には、CISO の承認が必要です。現地や地域の補則が策定されていない場合、適用される法律に準拠する本ポリシーのすべての条項は原文のまま効力を有します。

基本ポリシー

ストライカーは、当社製品およびシステムのセキュリティを規制するあらゆる法律を遵守します。さらに、ストライカーは、以下に明記した基準を遵守することを誓約します。

1. **チーフインフォメーションセキュリティオフィサー（CISO）の任命**：CISOは、ストライカーの効果的なグローバル情報セキュリティプログラムの制定と実施、そしてセキュリティイニシアティブとエンタープライズプログラムおよび事業目標との連携を通じて、情報資産、製品、システム、そしてテクノロジーを保護する責任を負っています。

2. **セキュリティポリシーおよび運営・ガバナンス機構の実施**：ストライカーは、該当する品質管理システム、情報セキュリティ管理システム、情報ガバナンス基準、標準利用規約、インシデントレスポンス計画、さらに関連基準および手順を通じて、適切な運営上の技術・物理的なセキュリティ管理を実施します。

3. **第三者へのアクセス**：グローバルセキュリティ評価プロセスは、ストライカーのネットワークもしくは電子機密データにアクセスできる第三者、またはインターネットベースのソリューションもしくはソフトウェアを社内利用目的に提供する第三者、また、これをストライカーの製品またはサービスで利用する第三者を、採用する前に実施する必要があります。

4. **ストライカーの機器およびシステムの利用**：ストライカーの機器およびシステムにアクセスできるストライカーの従業員もしくは第三者は、かかる機器およびシステムを該当する利用要件に従って使用します。

責任

本ポリシーならびに施行される適用基準と手順の遵守は、ストライカーの全従業員および第三者の責任です。CISOは、他の適切な事業部門およびビジネスユニットと協力して、本ポリシーの遵守に必要な追加の基準と手順を特定すると共に、かかる基準と手続きを策定し、実施します。

コンプライアンス

ストライカーは、すべての従業員と第三者が本ポリシーに従うことを義務付けています。本ポリシーまたは関連の手順について質問があるか、ストライカーのセキュリティプログラムに関して懸念がある場合は、ストライカーの人事担当者、コンプライアンスオフィサー、リーガルカウンセル、または倫理ホットラインまで連絡してください。ストライカーは、ホットラインポリシーに従い、かかる報告の機密性を保持します。