



MANAGING YOUR RISK...SMARTER™

テクニカル ポリシー プライバシー

1. 目的と範囲

このポリシーの目的は、ConstructSecure が一般的な Web サイトを運営するにあたって従うべきプライバシーの条件と、ConstructSecure ベンダー事前認定アプリケーションにログインしてそのアプリケーション使用する登録済みクライアントから収集するデータを使用、処理、および保存するにあたって従うべきプライバシーの条件を定義することです。

このポリシーの範囲は、ConstructSecure の公開 Web サイト (www.constructsecure.com) に加え、すべての ConstructSecure ネットワークと IT システム、および CS システムの使用に関連して登録済みクライアントによって提供されるすべてのエンド ユーザー データに適用されます。エンド ユーザー データには、名前、ビジネス用の電子メール、ビジネス用の電話番号が含まれますが、これらに限定されません。CS Inspect モジュールのユーザーは、検査結果に関するアラートを受信するために、ビジネス用の携帯電話番号を提供することもできます。エンド ユーザーのこの個人データは、ユーザーが安全なアカウントをセットアップし、システムからメッセージやアラートを受信できるように、登録済みクライアントが CS アプリケーションを操作および使用する際に必要となります。このポリシーは、アクティブなクライアントアカウントの期間中は完全に有効です。

CS プライバシー ポリシーは、Cookie、データ収集、データ使用、データ処理、データ転送、データ保持および削除、個人データ漏洩の通知、および情報/アカウントの管理または削除について ConstructSecure に連絡する方法に関するポリシーを、明確かつ完全に説明することを目的としています。

2. 訪問者とユーザーの違い

ConstructSecure の Web サイトは公開されており、Web サイトの訪問者が当社のページをナビゲートして当社の製品について学ぶために個人情報を入力する必要はありません。ただし、ConstructSecure は、以下の第 4 項で詳しく説明するように、訪問者のエクスペリエンスを向上させる方法として Cookie を使用します。訪問者が CS サイトを初めて訪問すると、まず、Cookie の使用に関する通知がポップアップ バナーに表示されます。ポップアップ バナーのテキスト内、および当社の Web サイトのすべてのページの下部には、このポリシーへのリンクも表示されます。

このポリシーでは、ConstructSecure システムのユーザーは、CS Safety、CS Financial、CS Tracker、CS Inspect などの CS の 1 つ以上のソフトウェア製品に登録されている個人として定義されています。このポリシーの対象範囲には、CS システムのあらゆる側面を使



MANAGING YOUR RISK...SMARTER™

用するすべてのクライアント エンドユーザーと、ConstructSecure の従業員が含まれます。

CS ユーザーには、CS の Web ベース アプリケーションへの 2 種類のアクセス権のうちの 1 つ (管理または一般) をセットアップできます。2 つのアクセス レベルの唯一の標準的な違いは、管理ユーザーが ConstructSecure によってシステムで最初にセットアップされ、固有のビジネス ニーズに基づいて CS アプリケーションを使用する従業員のリストを内部で管理できるように一般ユーザーを作成する機能を与えられることです。

一般ユーザーがクライアント管理者によって追加された場合、管理者によって提供される識別可能なデータは、一般ユーザーの名前、仕事用の電子メールアドレス、および電話番号のみです。クライアント管理者が一般ユーザー プロファイルを設定アップすると、一意の一般ユーザー プロファイルの正式な作成を開始するためのリンクが記載された自動電子メールが CS システムから一般ユーザーに送信されます。このセットアッププロセスでは、人間と自動プログラムを区別するように設計されたチャレンジレスポンス システム テストである、CAPTCHA (コンピューターと人間を区別する完全に自動化された公開チューリング テスト) を使用します。CAPTCHA は、ほとんどの人間にとっては簡単であるが、現行のボットが実行するにはより困難で時間のかかるタスクの完了を要求することによって、人間とボットを区別します。また、すべてのユーザーは、CS パスワード ポリシーで詳細に説明されている厳密なパスワード システムを設定アップの際に作成し、それを遵守する必要があります。

エンドユーザー アカウントは各ユーザーに固有であり、共有されることはありません。一意のユーザー名とパスワードに基づいて、一般ユーザーは自分が入力した特定のデータにのみアクセスできます。また、エンドユーザーは、各自のクライアント契約書で定義されている CS アプリケーションの特定のモジュール (CS Safety、CS Financial、CS Tracker、CS Inspect など) にのみアクセスできます。

3. 参照文書

このポリシーに関連する具体的な規制およびフレームワークには、以下が含まれますが、これらに限定されません。

- ISO/IEC 27001 規格。A.9.1.1、A.9.1.2、A.9.2.1 ~ A.9.2.6、A.9.3.1、A.9.4.1、A.9.4.3 の各条項。
- 一般データ保護規則 (GDPR)、2018 年 5 月 25 日
- EU-米国およびスイス-米国プライバシー シールド フレームワーク、米国商務省/欧州委員会/スイス政府
- カリフォルニア州消費者プライバシー法 (CCPA)、2020 年 1 月 1 日
- Lei Geral de Proteção de Dados (LGPD)、2020 年 2 月 1 日



MANAGING YOUR RISK...SMARTER™

情報の安全性に対する ConstructSecure の取り組みについて説明した包括的なポリシーは、この CS プライバシー ポリシーと CS 情報セキュリティ ポリシーです。CS 情報ポリシーの目的は、ConstructSecure の情報セキュリティ管理システム (ISMS) の原則と実践についての概要を理解できるようにすることです。CS 情報セキュリティ ポリシーは一般的な情報セキュリティ アプローチを提供する一方で、データの機密性と整合性を確保するために当社が講じる措置について定義した、非常に具体的な以下のテクニカルポリシーによって補足されます。

- CS 利用規定
- CS アクセス制御ポリシー
- CS 変更管理およびセキュア エンジニアリング/開発ポリシー
- CS クリア デスクおよびクリア スクリーン ポリシー
- CS データ バックアップ ポリシー
- CS 文書および情報管理ポリシー
- CS 暗号化ポリシー
- CS インシデント管理ポリシー
- CS 内部および外部監査ポリシー
- CS ロギングおよびモニタリング ポリシー
- CS パスワード ポリシー

また、情報セキュリティとそれを従業員およびクライアントに伝達する方法に関連した組織情報が記載された、以下の社内向け CS マニュアルもあります。

- CS 管理マニュアル
- CS カスタマー/サプライヤー エンゲージメントおよびサポート マニュアル
- CS ディザスタ リカバリおよびビジネス継続性マニュアル
- CS ISMS リスク評価およびリスク処理手法
- CS ISMS リスク評価およびリスク処理レポート
- CS 従業員ハンドブック
- CS システム アーキテクチャ マニュアル

4. Cookie ポリシー

ConstructSecure の Web サイトを適切に機能させるために、Cookie と呼ばれる小さなデータ ファイルが訪問者またはユーザーのデバイスに配置されることがあります。CS の Web サイトが後でブラウザに読み込まれるためのために、訪問者またはユーザーの基本設定 (言語、フォント サイズ、ログイン、その他の表示設定など) を「記憶」できるように、これらの Cookie はデバイス上のテキスト ファイルに保存されます。この一般的な慣行は、お客様の情報のセキュリティと保護を最高水準に保つことに対する



MANAGING YOUR RISK...SMARTER™

ConstructSecure の取り組みを決して過小評価するものではありません。大半の Web サイトがそうであるように、ConstructSecure は Cookie を使用することによって、一貫した効率的なエクスペリエンスを訪問者とユーザーに提供し、登録ユーザーがログイン状態を維持できるようにするなどの重要な機能を実行しています。また、ConstructSecure は、訪問者とユーザーがサイトをどのように操作およびナビゲートしているかを分析し、改善を加える目的でも Cookie を使用することがあります。Cookie 関連の情報は、登録ユーザーのアクションを記憶および記録するためにも使用されません。ここに記載されている以外の目的で Cookie が使用されることはありません。たとえば、ConstructSecure の Web サイトでは、サードパーティの追跡メカニズムが興味・関心に基づく広告で使用するデータを一定の期間にわたって、非提携 Web サイトで収集することを許可していません。また、ConstructSecure は、この特定の Cookie にブラウザがアクセスする必要があることをブラウザに通知する、特別な HttpOnly フラグですべての Cookie にフラグを立てます。この HttpOnly フラグにより、悪意のある JavaScript を使用して Cookie にアクセスしようとする攻撃者の試みを厳重に阻止することができます。

訪問者とユーザーは、各自のブラウザ設定を通じて、任意の Web サイトからの Cookie をブロックできます。設定や Cookie の変更手順はブラウザによって異なります。主要ブラウザで Cookie を無効にする方法の詳細については、それぞれの Web サイトに掲載された手順を参照してください。

- Internet Explorer (<http://support.microsoft.com/gp/cookies/en>)
- Mozilla Firefox (<http://support.mozilla.com/en-US/kb/Cookies>)
- Google Chrome
(<http://www.google.com/support/chrome/bin/answer.py?hl=en&answer=95647>)
- Safari (<http://support.apple.com/kb/PH5042>)
- Opera (<http://www.opera.com/browser/tutorials/security/privacy/>)

Cookie が配置されないようにブラウザの設定を変更することに加えて、デバイスに既に保存されているすべての Cookie を削除することもできます。訪問者またはユーザーがこのオプションを選択した場合は、ConstructSecure サイトにアクセスするたびに基本設定を手動で調整する必要が生じることがあり、一部のサービスと機能がまったく機能しなくなる可能性があります。

訪問者が初めて ConstructSecure の Web サイトにアクセスすると、まず、ConstructSecure が Cookie を使用していることがポップアップ バナーを介して通知されます。

5. データ収集



MANAGING YOUR RISK...SMARTER™

ConstructSecure アプリケーションへの登録の一環として収集されるエンド ユーザー データのうち、個人データまたは個人識別情報 (PII) として分類されるデータには、ユーザーの氏名、ビジネス用の電子メール、およびビジネス用の電話番号が含まれます。

CS Inspect モジュールのユーザーは、検査結果に関するアラートを受信するために、ビジネス用の携帯電話番号を提供することもできます。エンド ユーザーのこの個人データは、ユーザーが安全なアカウントをセットアップし、システムからメッセージやアラートを受信できるように、登録済みクライアントが CS アプリケーションを操作および使用する際に必要となります。

6. データの使用

ConstructSecure の ISMS は、ISO 27001 で定義されている最高情報セキュリティ責任者 (CISO) および GDPR の第 37 条で定義されているデータ保護責任者としての役割を果たす、当社の最高技術責任者によって社内で管理されています。クライアントが当社のサービスとシステムを使用する際、最高技術責任者は、データの使用方法与ユーザーのプライバシーを保護する方法について明確なパラメーターを設定します。これには以下が含まれますが、これらに限定されません。

- CS システムのユーザーについて、ConstructSecure は、クライアント ソフトウェア ライセンスおよびサービス契約書/サブコントラクター参加契約書で定義されている目的でのみデータを処理し、以下の第 7 節で説明するようにすべてのクラウドコンピューティングに Amazon Web Services を利用します。
- ConstructSecure は、契約書およびこのドキュメント内で定義されているとおりに、処理する個人データの機密性を保証します。
- ConstructSecure が第三者とデータを共有したり、第三者の広告プロバイダーを使用したりすることはありません。
- ConstructSecure は、その従業員が完全に精査を受け、CS 管理マニュアルおよび CS 従業員ハンドブックで定義されている適切な個人データ保護トレーニングを受けることを保証します。
- ConstructSecure の従業員は、CS 従業員ハンドブックに記載されている機密保持要件を署名の上承認します。
- データの転送またはダウンロードは、SSL プロトコルを介して行われます。
- データにアクセスする場合、ユーザーは CS パスワード ポリシーで詳しく定義されているユーザー名/パスワードでログインする必要があります。
- データのアップロード中、ファイルは暗号化され、CS 暗号化ポリシーで詳しく定義されているとおりに保存されます。たとえば、暗号化されたファイルごとに独自のキーがあることは要件の 1 つです。
- 保存されたバックアップとログは、CS データ バックアップ ポリシーで詳しく定義されているとおりに暗号化されます。たとえば、ConstructSecure が一時ストレージを使用しないことは要件の 1 つです。



MANAGING YOUR RISK...SMARTER™

7. データ処理

前述したとおり、ConstructSecureは、クライアントソフトウェアライセンスおよびサービス契約書/サブコントラクター参加契約書で定義されている目的でのみ個人データを使用します。また、CS管理マニュアルで詳しく説明されているように、ConstructSecureはクラウドテクノロジーのリーダーであるAmazon Web Servicesと契約を結び、AWSの論理的に分離されたセクションを作成して、CSシステム用の仮想プライベートクラウド(VPC)を作成できるようにしています。AWSはConstructSecureのISMSの範囲外ですが、AWSを選択した理由の1つは、ISO/IEC 27001:2013に基づく独自の認証にあります。つまり、AWSは2010年11月18日に証明書#2013-009を発行しています(その後更新され、最近では2020年3月27日に再発行されました)。

また、AWSとの契約の一環として、当社はAWSのデータ処理補遺(DPA)の当事者となっています。AmazonのDPAは一般データ保護規則(GDPR)、EU-米国およびスイス-米国プライバシーシールドフレームワーク、ならびにカリフォルニア州消費者保護法に完全に準拠し、そのすべての要件を満たしているという点で、このことはデータセキュリティとプライバシーに対する当社の取り組みの重要な要素です。AWSとのDPAは、以下を含むがこれらに限定されない重要なデータセキュリティ要件に関する保証を当社に提供するものです。

- AWSがお客様の指示に従ってのみお客様のデータを処理すること
- AWSがAWSネットワークに対して堅牢な技術的および組織的対策を実施し、それを維持すること
- AWSがセキュリティインシデントに気付いた後、遅滞なくお客様にセキュリティインシデントについて通知すること

8. データ転送

ConstructSecureが第三者とのデータの共有または第三者へのデータの転送を行ったり、第三者の広告プロバイダーを使用したりすることはありません。

ConstructSecureアプリケーションは、SaaSベースのWebホスト型アプリケーションです。前の節で説明したとおり、ConstructSecureはクラウドサービスとしてAmazon Web Servicesと契約しています。その契約の一環として、AWSは米国とヨーロッパ(フランクフルト、ドイツ)の両方でConstructSecureのサーバーを維持し、欧州連合(EU)加盟国(アイスランド、リヒテンシュタイン、ノルウェー、スイスを含む)からのデータがEU加盟国に保持されるようにしています。AWSは、EU-米国プライバシーシールドフレームワークとスイス-米国プライバシーシールドフレームワークの両方に準拠しています。



MANAGING YOUR RISK...SMARTER™

いずれの認定も「有効」として分類されており、次回の認定期限は 2021 年 1 月 16 日に到来します。

9. データの保持と削除

ConstructSecure は、継続的かつ正当な必要性があり、クライアント契約またはサブコントラクター契約の下で作業している場合に限り、すべてのエンド ユーザー データを保持します。特定のユーザー アカウントと個人を特定できる情報は、(クライアントの管理ユーザーまたは ConstructSecure による) アカウントの削除または契約の終了と同時に削除されます。ConstructSecure は、当社のサービスで過失による削除または悪意のある削除から情報を保護するよう努めます。このため、ユーザーが情報を削除してから、アクティブ システムとバックアップ システムからコピーが削除されるまでに遅延が生じる場合があります。

前述したとおり、特定のユーザー アカウントを削除する場合、クライアントの管理ユーザーには、自分が作成したアカウントを CS システムから削除する機能が提供されています。また、クライアント契約またはサブコントラクター契約が終了すると、最高技術責任者は、ログインを無効にし、システムからプロファイルを削除して、アクセスが終了したことを確認することによって、関連するエンド ユーザー アカウントのアクセス権を削除します。

ConstructSecure サブコントラクター参加契約書に詳述されているように、ConstructSecure はサブコントラクターから提出された情報を匿名化して集計する場合があります。また、ConstructSecure はすべての集計情報を所有し、それを任意の目的で使用したり、サブコントラクターに義務を負うことなく第三者に伝達したりする場合があります。集計された情報は匿名情報であり、データ保護法令の対象となる個人データではなくなります。

10. GDPR 要件とプライバシー シールドステートメント

ISO 27001 準拠の情報セキュリティ管理システム (ISMS) を実装することは、ベスト プラクティスであるだけでなく、クライアント、サブコントラクター、およびサードパーティにデータ保護コンプライアンスを実証する上でも不可欠です。また、ConstructSecure は ISO 27001 を実装することにより、2018 年 5 月 25 日に発効した欧州連合の一般データ保護規則 (GDPR) に確実に準拠するための強力なフレームワークを作成しました。

GDPR に準拠するため、ConstructSecure は、欧州連合およびスイスから米国に転送される個人データの収集、使用、および保持に関して米国商務省が定めた、EU-米国プライバシー シールド フレームワークおよびスイス-米国プライバシー シールド フレームワークに準拠しています。



MANAGING YOUR RISK...SMARTER™

ConstructSecure は、米国商務省に対して、プライバシー シールドの原則に準拠していることを証明しています。CS プライバシー ポリシーの条件とプライバシー シールド原則の間に矛盾がある場合は、プライバシー シールド原則が優先するものとします。プライバシー シールド プログラムの詳細および当社の認定を確認するには、<https://www.privacyshield.gov/> をご覧ください。

プライバシー シールド フレームワークと原則の一環として、ConstructSecure は以下を保証します。

- ConstructSecure の自己認証は、連邦取引委員会の調査および執行機関の対象となります。
- ConstructSecure は、第 5 節で前述した限られた個人データを収集し、第 6 節で前述した目的でのみこの情報を使用します。
- ConstructSecure アプリケーションの個々のユーザーは、個人データにアクセスし、個人データの使用/開示を確認、修正、削除、または制限する権利を有します。EU およびスイスのユーザーは、すべてのユーザーと同様に、一意のユーザー名とパスワードを使用して CS システムにいつでも安全にログインし、各自の個人データにアクセスしてそれを確認できます。ConstructSecure アプリケーションのユーザーが個人データの使用/開示を修正、削除、または制限する必要がある場合は、第 13 節に詳しく説明するとおり、ConstructSecure (support@constructsecure.com)に連絡してそれを行うことができます。
- ConstructSecure が第三者とのデータの共有または第三者へのデータの転送を行ったり、第三者の広告プロバイダーを使用したりすることはありません。ただし、ConstructSecure は、原則と矛盾する方法で第三者がデータを処理している場合に、その第三者とデータを共有したり第三者にデータを転送したりした法人 (ConstructSecure を含む) が法的責任を負うことを認めます。
- ConstructSecure は、法的義務と合法的な要求に従い、法執行または国家安全保障の目的で公的機関に個人データを転送する場合があります。
- ConstructSecure は、EU とスイスのユーザー、およびプライバシー シールドの下での個人データの処理方法について質問や苦情があるすべてのユーザーに対し、第 13 節の説明に従って当社に連絡することを奨励しています。ConstructSecure は、質問または苦情を受け取ってから 30 日以内に、可能な限り迅速にお客様の問題を解決するよう務めます。



MANAGING YOUR RISK...SMARTER™

- 当社が十分に対応していない、プライバシーまたはデータ使用に関する未解決の苦情がある場合は、米国に拠点を置く第三者紛争解決プロバイダーである米国仲裁協会 (<https://www.adr.org/TechnologyServices>) にお問い合わせください(無料)。
- お客様が EU または スイス のユーザーであり、上記のいずれの方法でも苦情を解決できない場合は、プライバシー シールド フレームワーク (<https://www.privacyshield.gov/article?id=How-to-Submit-a-Complaint>) に従って拘束力のある仲裁の申立てを行うことができます。

11. カリフォルニアとブラジルの要件

ConstructSecure は、2020 年 1 月 1 日に施行されたカリフォルニア州消費者プライバシー法 (CCPA) にも準拠しています。20 年 2 月 1 日にブラジルで発効した Lei Geral de Proteção de Dados (LGPD)。カリフォルニア州消費者プライバシー法 (CCPA) または LGPD がユーザーの情報に適用される場合、ConstructSecure のデータ慣行に関する情報を受け取る権利を行使したり、情報/アカウントの削除をリクエストしたりするためにユーザーが利用できるプロセスは、このポリシーの第 13 節で説明されています。

ConstructSecure は、ユーザーの個人データを共有、販売、または転送しません。

ConstructSecure は、クライアント ソフトウェア ライセンス、サービス契約書/サブコントラクター参加契約書、およびこのポリシーで定義されているビジネス目的でのみ個人データを使用および処理します。

12. プライバシー ポリシーの変更または個人データの漏洩に関する通知

ConstructSecure は、CS プライバシー ポリシーをいつでも改訂する権利を留保します。このプライバシー通知に大幅な変更が加えられた場合、ConstructSecure はそのような変更の通知を当社の Web サイト (www.constructsecure.com) からリンクされている

「ConstructSecure ブログ」に掲載します。このポリシーの新しいバージョンはすべて、ConstructSecure の Web サイトにすぐに再投稿され、ConstructSecure の Web サイトのすべてのページの下部にある「プライバシー ポリシー」リンクから直接アクセスできます。

さらに、ConstructSecure は、個人データの漏洩が発生した場合にその旨を電子メールで即座に (漏洩を認識してから 72 時間以内に) クライアントに通知します。この通知には、クライアントが必要に応じて管轄の監督当局に漏洩について通知できるようにするために必要な以下の情報が含まれます。

- 漏洩の性質と説明 (影響を受けるユーザーの数を含む)
- 問題の分析と根本原因



MANAGING YOUR RISK...SMARTER™

- 漏洩に対処し、悪影響を軽減するための即時の是正措置
- 同じ性質およびタイプの将来の漏洩を防ぐために提案または実施されたその他の是正措置

13. ConstructSecure への連絡

ConstructSecure の所在地は、450 Bedford Street, Suite 2200, Lexington, Massachusetts, 02420 です。

ユーザーが ConstructSecure のデータ慣行について質問や苦情がある場合、または情報/アカウントの削除をリクエストしたい場合は、最高技術責任者またはコンプライアンス担当副社長に書簡(上記の住所)、電子メール (support@constructsecure.com)、または電話(866-817-2210)で連絡することができます。ConstructSecure の電子メール アドレスへの直接リンクは、当社の公開 Web サイト上、およびユーザーが ConstructSecure システムにログインした後にも表示されます。

ConstructSecure は、ConstructSecure のクライアント契約書またはサブコントラクター契約書に定められているサービス レベル契約 (SLA) に従って問題を直接かつ迅速に解決できるよう、苦情を申し立てた人物に連絡することによって書面による苦情に対応します。。また、EU-米国およびスイス-米国プライバシー シールド フレームワークの原則に従い、第 10 節で詳述されているとおり、ConstructSecure は、米国商務省、米国連邦取引委員会、EU データ保護当局 (DPA)、およびスイス連邦データ保護情報委員会 (FDPIC) を含むがこれらに限定されない適切な独立した担当当局と必要に応じて連携し、ユーザーの満足のいく方法で、ユーザーに費用をかけずに苦情を解決するものとします。

14. ポリシー コンプライアンス a. コンプライアンス基準

このドキュメントの有効性と妥当性を評価するにあたっては、次の基準を考慮する必要があります。

- システムのセキュリティ侵害の件数
- アカウント削除の件数
- データ セキュリティ情報のリクエストの件数と解決時間
- データ セキュリティに関する苦情の件数と解決時間

b. コンプライアンス測定

上記の具体的なコンプライアンス基準は、ConstructSecure によって作成され、CS 情報セキュリティ ポリシーの付録 1 に記載されている、ISMS 包括的コンプライアンス測定表の一部として含まれています。最高技術責任者は、ISMS 包括的コンプライア



MANAGING YOUR RISK...SMARTER™

ンス測定表を使用して四半期ごとのレビューを実行することにより、情報セキュリティ ポリシー全体およびその他すべてのテクニカル ポリシーへの準拠を確認します。四半期レビューの結果は追跡および分析され、年次 ISMS 管理レビュー会議の一部として組み込まれます。

コンプライアンスの測定は、正式な四半期レビューに加えて、定期的なウォークスルー、ビジネス ツール レポート、ポリシー所有者へのフィードバックを含むが、これらに限定されないさまざまな方法で継続的に実施されます。

このポリシーに関連したトレーニングと意識向上の取り組みは、CS 従業員ハンドブックに詳述されているように、ConstructSecure の全般的な従業員トレーニング プログラムの一環として実施されます。

c. 例外事項

ポリシーの例外事項は、ポリシー所有者によって事前に承認されなければなりません。

d. コンプライアンス違反

このポリシーに故意に違反したことが判明した従業員は、解雇を含む懲戒処分の対象となる場合があります。

15. レビューと開発

このポリシーの作成者は所有者とみなされ、変更が指示された場合に必ずポリシーを更新する責任があります。また、このポリシーの年次レビューは、法律、組織のポリシー、契約上の義務に対する関連性のある変更に応じて適切性を維持していることを確認するために、最高技術責任者によって実施されます。

CS 管理マニュアルで指定されているように、ISMS ドキュメントへのすべての変更は、「変更履歴機能」を使用して行う必要があります。これにより、以前のバージョンに対する変更箇所のみが赤いテキストまたは取り消し線付きで表示されるようになります。また、以前のバージョンの ISMS ドキュメントはすべて、CS コンプライアンス担当副社長の個人用ユーザー ドライブに参照用に保存されます。このドキュメントのバージョン管理履歴は、次の表で定義されています。



MANAGING YOUR RISK...SMARTER™

バージョン履歴	日付	作成者	承認者	分類
バージョン 5	6/8/20 (プライバシー シールド)	S. Kirilenko	D. Milinazzo、 K. Sardone	機密
バージョン 4	1/13/20 (CCPA の追加)	S. Kirilenko	D. Milinazzo、 K. Sardone	機密
バージョン 3	5/15/19	S. Kirilenko	D. Milinazzo、 K. Sardone	機密
バージョン 2	5/15/18 (Cookie ポリシー)	S. Kirilenko	D. Milinazzo、 K. Sardone	機密
バージョン 1	5/15/17	S. Kirilenko	D. Milinazzo、 K. Sardone	機密

このポリシーは、最高技術責任者によって毎年レビューされます。