Alludo ベンダー向けセキュリティー要件

目次

はじめに....2
ベンダー向けセキュリティー要件の概要....3
ID およびアクセス管理....3
資産管理....5
IT 運用....6
人的資源のセキュリティー....7
セキュリティーおよびプライバシーに関する研修....7
情報セキュリティーおよびガバナンス....8
ネットワークのセキュリティー....9
暗号技術....10
データのセキュリティー....10
情報コミュニケーション....12
ソフトウェア開発....12
アプリケーションのセキュリティー....13
パッチ管理....13
マルウェアからの保護....13
脆弱性管理....14
ログ記録およびモニタリング....14
インシデント管理....15
物理的および環境的セキュリティー....15
プライバシーおよびデータの保護....16
下請業者への対応....17
事業継続性の管理....17

はじめに

本文書は、Alludo グループ (以下、総称して「Alludo」といいます) の情報セキュリティー、事業継続性、プライバシーの慣行、および Alludo のベンダー各社のセキュリティーおよび事業継続の対策の評価プログラムについて概説するものです。本文書で言及されるプロセス、手順、要件、義務は、総称して「Alludo の標準」といいます。

この**ベンダー向けセキュリティー要件文書**は、Alludo がサービスを提供する際に、商品やサービスを提供するベンダー (以下、「ベンダー」) に対して責任を課し、従うことを求めるセキュリティー、事業継続性、プライバシーに関する事項を通知するものです。ベンダ

ーは、業界のベスト プラクティスと企業のセキュリティー ポリシーに従ってこれらの要件を遵守する必要があります。Alludo は、その原因にかかわらず、データの損失や機器の損傷を含むベンダーが直面する問題について責任を負わないものとします。

本文書と書面による合意との間に矛盾がある場合は、書面による合意の条件が優先されます。また、ベンダーは、国、地域、区域の規制要件に準拠する必要があります。本文書と適用される規制との間に矛盾が生じた場合、ベンダーは、Alludo に通知し、同等のセキュリティー、継続性、またはプライバシー標準を維持するための代替管理を提案する必要があります。

ベンダー向けセキュリティー要件の概要

Alludo には、制限された機密情報を不正なアクセスや不正な開示から保護する責任があります。このため、Alludo は、そのような制限された機密情報が保護され、Alludo によって提供されるサービスが継続的に利用できることを保証する、内部情報セキュリティー、事業継続性、プライバシーの標準として「Alludo の標準」を実施しています。情報セキュリティーとビジネス継続性に関連する社内標準および規制要件を Alludo が遵守できるよう、Alludo は、本文書に概説されている Alludo の標準をベンダーが遵守することを要求します。

同様に、ベンダーが Alludo との契約に基づくベンダーの義務の一部を委任または下請けする、または Alludo に直接または間接的にサービスを提供するために別のベンダーを雇用する場合、ベンダーは、Alludo の標準に準拠した情報保護プログラムおよび計画を実装および管理することを当該ベンダーに要求するものとします。Alludo は、ベンダーが Alludo の標準に関連するコンプライアンス要件を満たせるよう、ベンダーと合理的に協力することに尽力しています。このような Alludo の標準をベンダーに適用する範囲は、当該ベンダーが Alludo に提供するサービスおよび製品の種類によって異なります。

ID およびアクセス管理

ベンダーは、以下を保証するものとします。

1. アクセス管理およびユーザー管理

1.1. 文書化されたアクセス管理ポリシーを導入し、少なくとも 1 年に 1 回見直しを行います。
1.2. ユーザーの役割、権限、アクセス権を定義し、文書化します。
1.3. 関連する承認の記録を含めて、ユーザーのオンボーディングとオフボーディングに関する標準的なプロセスを適用します。

1.4. IT インフラストラクチャのコンポーネントへのアクセスは、最小権限の原則に基づいて許可し、ID 管理ツール (Active Directory、OKTA など) を介して管理します。
1.5. システム、ネットワーク リソース、その他の IT リソースへの個々のアクセスは、一意のユーザー ID と個々のパスワードによって正式に承認し、制御します。
1.6. ユーザー ID の作成/修正および権限の割り当て時には、職務の分離を維持します。

2. パスワードと認証ポリシー

2.1. ユーザーには、最初のサインオン時にパスワードを変更することを要します。
2.2. パスワードの長さ、有効期限、複雑さ、パスワード履歴、試行の失敗、アカウントのロックアウト期間、パスワードの有効期間、初回ログオン時の変更などに関して、業界標準の要件を満たします。
2.3. パスワードのリセットを開始する前は、安全なメカニズムを使用してユーザーのパスワードを配信し、ユーザーの本人確認を行います。
2.4. IdP 認証をサポートしていないシステム、またはスタンドアロンで構築する必要があるシステムは、中央のパスワード ポリシーとアクセス コントロール ポリシーで定義されている設定よりも強力な認証を実施するように設定します。
2.5. すべてのシステムおよびアプリケーションは、承認された ID およびアクセス管理メカニズムを介して安全なログオン手順を使用するよう構成します。
2.6. 不正アクセスを防止するために、システムおよびアプリケーションには、アイドル セッション タイムアウトを設定します。

3. 特権アクセス管理

3.1. リソースへの特権的なアクセス権限は、定義されたユーザーの役割で制限し、権限を与えられた担当者が承認するようにします。
3.2. 特権ユーザー アカウントには、多要素認証が使用されるように設定します。
3.3. 不要になった権限は直ちに取り消します。
3.4. 管理者の認証情報の使用は、トラブルシューティングのような限定された状況に制限し、ユーザーは、最小権限の認証情報で日常業務を行うようにします。
3.5. 重要な IT インフラストラクチャ、システム、ネットワーク デバイス、アプリケーション (リモートアクセス、重要なサーバー、ネットワーク デバイスなど) へのアクセスは、多要素認証により保護します。

4. アクセスの見直しおよび監視

4.1. 定期的にアクセス権の見直しを行い、特定された例外には速やかに対応します。
4.2. すべてのユーザーID (ドメイン、アプリケーション、ネットワーク デバイス、IT システム、ミドルウェア、データベースなどを含む) の調整を年 1 回以下行い、特定された不一致に対しては直ちに修正措置を取ります。

5. サードパーティーおよびベンダーの管理

5.1. ネットワークやシステムへのサードパーティー ベンダーのアクセスは、必要な情報と正式な承認に基づいて厳密に管理します。
5.2. システム、アプリケーション、ネットワーク デバイス、その他の IT インフラ デバイスが本番稼動する前に、ベンダーは、提供するデフォルトの認証情報を変更します。

6. 特別なアクセスに関する考察

6.1. 一般的な ID や共有 ID は、正式に正当性が認められ、上級管理職によって承認されない限り使用せず、これに関して使用状況を追跡し、個人へのアクションを追跡する仕組みを使用します。
6.2. コンソール以外の管理者アクセスはすべて、業界で承認された暗号化アルゴリズムを使用して暗号化し、コンソール以外の管理者アクセスでは安全でないプロトコル (telnet/ftp など) は禁止します。

資産管理

ベンダーは、以下を保証するものとします。

7. 資産管理とインベントリ

7.1. 包括的な資産のインベントリを維持し、資産の所有者の情報、連絡先データ、場所などの重要な詳細を記録します。
7.2. ハードウェア、オペレーティング システム、アプリケーション、データベースを含む情報技術の資産の記録を定期的に更新し、正確性を確保するために見直しを行います。
7.3. 重要な資産の可用性と重要なネットワークおよび情報システムの構成を管理できるよう、資産管理の手順と構成の管理を確立し、維持します。

8. 情報の分類およびラベリング

8.1. 情報分類の方針と、それを裏付ける手順やガイドラインを維持します。すべての資産に、確立された指示に従ってラベル付けを行い、定義された分類レベルに基づいて情報を分類および保護します。

9. 資産の取り扱い

9.1. 資産を適切に取り扱うために、資産管理のガイドラインを維持し、該当するすべての従業員および請負業者に通知します。
9.2. 情報資産を保護し、廃棄すべき資産を特定し、安全委廃棄するための手順を文書化します。
9.3. 雇用、契約、合意の終了または離職時には、割り当てられていた資産が該当する資産管理チームに速やかに返却されるプロセスを確立します。

10. モバイル デバイスおよびリムーバブル メディアの管理

10.1. 業務情報の保存、送信、処理に使用するモバイル デバイス (BYOD を含む) を管理するための方針と手順を実施します。モバイル デバイスに業務情報やリソースへのアクセスを許可する前に、十分な保護対策を取ります。

10.2. リムーバブル大容量記憶装置を使用する場合は、データの安全性を確保するために暗号化します。

11. ソフトウェアのコンプライアンス

11.1. ライセンスが取得されていないソフトウェアや承認されていないソフトウェアの使用は、禁止します。違反行為を特定し、それに対応するために必要な措置を講じるためのプロセスを整備します。

IT 運用

ベンダーは、以下を保証するものとします。

12. 重要なシステムの運用

12.1. 以下を含む重要なネットワークと情報システムを運用するための手順を確立し、維持します。

12.1.1. IT 資産へのアクセスに関する正式な承認プロセス

12.1.2. すべてのテクノロジー (VPN、Windows ログオンなど) に対する堅牢な認証メカニズム

12.1.3. 定期的な特権の見直し

12.1.4. 事業継続性の要件に基づく重要技術のネットワークの場所の特定

13. 変更管理

13.1. IT システム、アプリケーション、データベース、ネットワーク コンポーネントに対して、包括的な変更管理プロセスを実施し、以下を保証します。

13.1.1. すべての変更に関するログ、確認、テスト、および正式な承認

13.1.2. 混乱を招く可能性のある修正のロールバック計画

14. その他

14.1. 秘密情報および機密情報を扱うシステムやネットワーク コンポーネントは、ファイルの整合性監視チェックの対象とします。

14.2. すべてのシステムおよびネットワーク コンポーネントは、正確な時刻に同期させるために認可されたネットワーク タイム プロトコル (NTP) ソースを使用するよう設定します。

14.3. すべての重要なシステム、アプリケーション、ネットワーク機器、およびエンドユーザーのマシンに対して、定期的な事前予防のメンテナンス プロセスを確立します。

14.4. ファイアウォールとルーターのルール一式には、定期的または業界標準に従って見直しを実施し、不要または未承認のルールは速やかに削除します。
14.5. IT 環境全体を通じて、情報とソフトウェアの完全性を維持するための統制を実施します。

人的資源のセキュリティー

ベンダーは、以下を保証するものとします。

15. 身元調査

15.1. 身元調査の実施に関する方針と手順を確立し、維持します。
15.2. 従業員および請負業者の業務開始前に、その職務と責任に基づき、法的に許される範囲で、適切な身元調査を実施します。

16. 人事異動管理

16.1. 新しい従業員に関連する方針と手順を教育することを含め、従業員またはその役割と責任の変更を管理するプロセスを導入します。
16.2. 人事異動に伴い、アクセス権、バッジ、機器、その他のリソースが不要または許可されなくなった場合は、速やかに取り消します。

17. ポリシーの実施

17.1. セキュリティー ポリシーに違反した従業員に対する明確な懲戒プロセスを実施し、維持します。
17.2. 適切な契約措置により、セキュリティー ポリシー違反に対する責任を確保します。これには、従業員の雇用契約やサードパーティー請負業者に対するサービス契約に関連する条項を組み込むことも含まれます。

セキュリティーおよびプライバシーに関する研修

ベンダーは、以下を保証するものとします。

18. セキュリティーとプライバシーに関する研修をすべての従業員と請負業者に義務付けます。すべての研修を雇用時に行い、その後は 1 年または何年かに 1 回行います。
19. IT セキュリティーに重大な責任を持つ従業員および請負業者は、セキュリティーに関する特定の役割と職務に合わせた特別な研修を毎年受けるものとします。
20. 経営関係者が従業員や請負業者の研修の進捗状況を監視および追跡できるツールやシステムにアクセスできるようにします。
21. 組織の研修と意識向上プログラムは、定期的に見直し、更新します。このプロセスでは、進化するビジネス要件、法規制の変更、過去のセキュリティー インシデントから学んだ教訓を考慮に入れます。

情報セキュリティーおよびガバナンス

ベンダーは、以下を保証するものとします。

22. セキュリティーのフレームワークとガバナンス

22.1. ベンダーは、情報およびサイバーのセキュリティー ガバナンスのために、認識されたセキュリティー標準フレームワーク (NIST CSF、RMF、800-53、ISO 27001、CIS など) を導入します。このフレームワークには、以下が含まれている必要があります。

22.1.1. 情報およびサイバーのセキュリティーに関する包括的な方針および手順。毎年の見直し、正式な承認、組織全体への周知

22.1.2. ビジネス目標に沿った明確な情報セキュリティー戦略

22.1.3. 情報およびサイバー セキュリティーのリスクに特化した強固なガバナンスおよびリスク管理のプロセス

22.1.4. 情報およびサイバー セキュリティーに関する法的および規制上の要件を満たすためのコンプライアンスの仕組み

22.2. 認識されたセキュリティー フレームワークに準拠していない場合、ベンダーは、その環境が監査を受けたことを証明する報告書を提出します。

22.2.1. 特定された問題の改善計画 (予定期間を含む) には、ベンダーと Alludo の間での相互の合意を確保します。

23. リーダーシップと組織の構造

23.1. 情報セキュリティーとサイバー セキュリティーに関する適切な役割と責任を定義し、組織全体で実施します。

24. リスク管理と評価

24.1. 以下に対応する上級管理職によって承認された正式なリスク管理のフレームワークを導入します。

24.1.1. 内部および外部の脅威の特定

24.1.2. 対象範囲の情報/データの機密性の評価

24.1.3. 潜在的なビジネスへの影響の評価

24.1.4. 脅威、脆弱性、対応するリスクの評価

24.1.4.1. 特定されたすべてのリスクと脅威には優先順位が付与し、それに応じてリスクを軽減するためのタイムリーな行動を取ります。

24.1.4.2. 組織の主要な事業目的に支障をきたす事象を特定するためのプロセス及び／又はツールを導入します。

24.1.4.3. ベンダーは、提供するサービスに影響を与える可能性のある重大なリスクを修正または軽減できない場合、直ちに Alludo に通知します。

25. コンプライアンスおよびパフォーマンスの監視

25.1. 組織に適用されるすべての法的、規制的、および契約上の要件を特定、記録、追跡するためのプロセスを整備します。
25.2. 法律、規制、契約上の義務が遵守されていることを確認するため、定期的な評価を実施します。このような評価の記録を維持し、特定されたギャップは大幅に遅延することなく改善させます。
25.3. 方針、手順、ガイドラインは最低年 1 回の見直しを実施し、法律、規制、契約上の要件に従って更新します。
25.4. IT、情報セキュリティー、データ プライバシーなどの重要な機能の主な業績評価指標を定義し、正式に文書化し、定期的に評価を実施し、上級管理職に報告します。

ネットワークのセキュリティー

ベンダーは、以下を保証するものとします。

26. ネットワーク設計およびセキュリティー アーキテクチャ

26.1. ベンダーのネットワークには、「多層防御」の原則を採用し、ネットワークのセグメンテーションなどの適切なコントロールを組み込むことで、情報やサイバーセキュリティーの侵害を最小限に抑えます。
26.2. 効果的なアイデンティティ管理と堅牢なオペレーティング システム構成を特徴とする、強力なアーキテクチャ設計を実装します。
26.3. ネットワークの設計と実装は、有効性とセキュリティーを継続的に確保するため、毎年見直しを実施します。
26.4. ネットワーク構成は、適用されるすべての法的および規制要件に準拠させます。

27. アクセス制御と認証

27.1. 外部ネットワーク接続は、確立前に文書化し、ファイアウォールを経由し、検証し、承認を受けます。
27.2. ワイヤレス ネットワーク アクセスには、認証、認可、セグメンテーション、暗号化を実施します。不正な無線アクセス ポイントや不正な接続を検出し、対応するためのシステムを整備します。
27.3. ベンダーのネットワークへのリモート アクセスは、多要素認証による安全な手段で承認を行い、実施します。
27.4. ベンダーのネットワークへの不正アクセスを防止または最小化するためのコントロールを実施します。

28. 安全な管理と運営

28.1. 管理ワークステーションおよびネットワーク デバイス間の管理関連のすべてのネットワーク トラフィックには、業界標準の暗号化と認証プロトコルを使用します。

28.2. コンソール管理者以外のアクセスは、業界で承認された暗号化されたチャネルを通じてのみ行います。
28.3. ゲスト アカウントは無効化または削除します。デフォルトのパスワードおよびベンダーが提供するパスワードはネットワーク デバイスが本番環境に導入される前にすべて変更されるようにします。

29. ネットワーク ハードニングおよび脅威対策

29.1. 攻撃対象領域を減少させるため、未使用のサービス、アプリケーション、ポートは無効化します。
29.2. 重要なネットワーク セグメントには、侵入検知および/または防止対策を導入します。
29.3. 重要なシステムは、サービス拒否 (DoS) や分散型サービス拒否 (DDoS) 攻撃から保護します。

暗号技術

ベンダーは、以下を保証するものとします。

30. 関連するすべての法律、規制、およびビジネス要件へのコンプライアンスを確保するために、包括的な暗号化ポリシーおよびそれをサポートする手順を導入します。このポリシーは、適用される法律および基準に従って安全な暗号化を保証する業界のベストプラクティスに従います。

31. 暗号化の標準および実装

31.1. 業界で承認された安全な暗号化アルゴリズムおよびキーの強度のみを許可し、すべてのシステムとプロセスにわたって適切なデータ保護を保証します。
31.2. 機密情報を保護し、機密データへのアクセスを制限するため、暗号化ソリューションを導入します。
31.3. パスワードの保管と送信にはすべて暗号化を実施し、ユーザー認証情報の機密性を常に維持します。
31.4. 転送中の Alludo データは、暗号化します (最低でも TLS 1.2、またはそれより新しい標準)。
31.5. Alludo の静止データは暗号化します (最低でも AES 256 ビット、またはそれより新しい標準)。

データのセキュリティー

ベンダーは、以下を保証するものとします。

32. リカバリ

32.1. **データのバックアップとリカバリ**
32.1.1. Alludo のデータを定期的にバックアップします。
32.1.2. Alludo のデータのバックアップは、1 年間保持します。
32.1.3. Alludo のデータのバックアップは、暗号化を実施します。
32.2. 災害リカバリ
32.2.1. 災害リカバリの計画は、毎年テストを実施します。

33. バックアップの方針および手順
33.1. バックアップの方針および手順を明確に文書化します。
33.2. バックアップの復元プロセスは、文書化し、決められた頻度でテストします。
33.3. バックアップの復元テストの証拠を維持します。
33.4. 重要なデータのバックアップ ファイルのコピーは、安全に保管します。

34. バックアップの監視
34.1. 失敗したバックアップのログ (もしあれば) は、バックアップ管理者が監視します。
34.2. バックアップに失敗した場合、是正措置を実施し、文書化します。

35. データの場所
35.1. ベンダーは、データが保存される国で適用されるすべてのデータ保護法およびプライバシー法の遵守を確保する責任を負います。
35.2. ベンダーは、国境を越えてデータを転送する際の制限 (GDPR など) を遵守します。
35.3. ベンダーは、データが保存される国の法律および基準に従って、データを保護するための適切な技術的および組織的なセキュリティー対策を実施します。
35.4. Alludo は、合意されたセキュリティー対策および現地の規制の遵守を確認するために、ベンダーのデータ取り扱い慣行を監査する権利を留保します。

36. データの削除
36.1. データを契約終了時に安全に削除するための手順を定め、現地のデータ保持法を遵守します。

37. フルディスク暗号化
37.1. ワークステーションおよびサーバーには、フルディスク暗号化を設定します。

38. データの分類
38.1. データ分類の方針を文書化します。
38.2. データは、その重要性と機密性に基づいて分類します。
38.3. データの機微性に応じたセキュリティー管理を特定し、実施します。

情報コミュニケーション

ベンダーは、以下を保証するものとします。

39. Web のセキュリティー

39.1. Web コンテンツ フィルタリング ソフトウェアを導入し、悪意のあるコンテンツをホストする Web サイトへのアクセスをブロックします。

39.2. すべての Web ベースのシステムとアプリケーションは、安全で認証されたメカニズムを介してアクセスされるようにします。

39.3. アプリケーションや Web ポータルのクライアント サーバー間の通信は、暗号化されたチャネルで行います。

40. 電子メールのセキュリティー

40.1. 電子メール システムの悪用を防ぐため、セキュリティー管理を行います。

40.2. すべての電子メール通信は、暗号化された経路で送信します。

40.3. 電子メール ゲートウェイには、以下を確保します。

40.3.1. フィッシング対策のフィルター

40.3.2. 電子メールのセキュリティープロトコル (DMARC、DKIM、SPF など) を有効にします。

40.3.3. その他の電子メールを介した脅威を防ぐために必要な設定

ソフトウェア開発

ベンダーは、以下を保証するものとします。

41. ソフトウェア開発ライフサイクル

41.1. ソフトウェアおよびシステム開発のフレームワークを確立します。

41.2. システムやアプリケーションは、セキュアソフトウェア開発のベストプラクティス (OWASP など) に従って開発します。

41.3. ソフトウェア コードに関しては、以下を確保します。

41.3.1. 不正な改変からの保護

41.3.2. 安全な保管

41.3.3. 品質保証プロセスの対象とすること

41.4. コードの見直しの実施

42. テストおよび展開

42.1. アプリケーションには、本番環境に展開する前に、徹底したセキュリティーと機能のテストを行います。

42.2. 本番環境と非本番環境は適切に分離します。

42.3. 本番と非本番開発間における職務の分離を維持します。

42.4. 本番データはテスト環境に使用しません。

アプリケーションのセキュリティー

ベンダーは、以下を保証するものとします。

43. アプリケーションのセキュリティー

43.1. アプリケーションのセキュリティー評価は、新規に開発されるすべてのアプリケーションと、重要な変更が加えられる既存のアプリケーションに対して実施し、既知のセキュリティー脆弱性を特定します。

43.2. CVSS スコアが 4 を超える特定されたセキュリティー脆弱性はすべて、アプリケーションを本番環境に展開する前に改善します。

43.3. コードの見直しプロセスを実施し、セキュリティー脆弱性をもたらす可能性のあるコードを特定し、修正します。

44. ウェブ アプリケーションの保護

44.1. 一般向けの Web アプリケーションは、堅牢な Web アプリケーション ファイアウォールによって保護し、外部からの脅威を防ぎます。

パッチ管理

ベンダーは、以下を保証するものとします。

45. 最新のセキュリティー パッチを、パッチによって対処される脆弱性の重要性に基づいて、システム、ネットワーク、アプリケーション、データベースなどに適時に適用します。専有権を有するシステムには、各 OEM から直接パッチを入手します。

46. 本番システムにパッチを展開する前にすべてのパッチをテストし、パッチを適用したサービスの正常な動作は、パッチの適用後に検証します。

47. システムがパッチを適用できない場合、適切な緩和策を講じ、そのような緩和策の有効性を定期的に評価し、対応する証拠を維持します。

マルウェアからの保護

ベンダーは、以下を保証するものとします。

48. すべての IT システムは、サービスの中断やセキュリティー侵害を防ぐために、受信データをリアルタイムで検査するマルウェア保護ソリューションによって継続的に保護します。さらに、適切なユーザー意識向上の手順を実施します。マルウェア対策システムは、ウイルス、スパイウェア、ワーム、不正なモバイル コード、キーロガー、ボットネット、トロイの木馬など、さまざまな脅威を検出しますが、これらに限定されるものではありません。

49. マルウェア シグネチャは定期的に更新し、システムに常に最新の脅威定義を適用します。

50. マルウェア保護ソフトウェアは、スケジュール スキャンとオンデマンド スキャンの両方を実行し、特定された悪意のあるファイルやソフトウェアを隔離または削除するよう構成します。
51. エンド ユーザーには、マルウェア対策を無効にする権限や能力は許可しません。

脆弱性管理

ベンダーは、以下を保証するものとします。

52. 脆弱性管理プロセス

52.1. 包括的な脆弱性管理のための方針、プロセス、手順を確立します。
52.2. 内部および外部ソースからの脆弱性を受け取り、分析、対応するプロセスを実施します。

53. 脆弱性の評価と修復

53.1. 災害リカバリ サイトを含む、ベンダーの IT インフラおよびアプリケーションの脆弱性を四半期ごとに評価します。
53.2. CVSS スコアが 4 以上の特定された脆弱性を定められた期限内に修復します。

54. 侵入テスト

54.1. ベンダーの IT インフラストラクチャおよび Alludo サービスに使用されるアプリケーションに対する独立した侵入テストを毎年実施します。
54.2. このテストは、悪用可能な脆弱性を特定し、サイバー攻撃によるセキュリティー侵害を防止することを目的とします。
54.3. Alludo は、合理的な要求に応じて、関連する侵入/脆弱性テスト レポートへのアクセスを許可しています。

ログ記録およびモニタリング

ベンダーは、以下を保証するものとします。

55. アプリケーションを含む重要なシステムは、主要なイベント (特権アクセスやユーザー活動を含む) をログに記録し、最低 1 年間または適用される規制要件に従って保存するように設定します。
56. 主なイベントのログ (適切なもの) には、最低限、以下のものが含まれます。

56.1. システムのスタートアップとシャットダウン
56.2. 重要なサービスやプロセスの開始と停止のステータス
56.3. コンフィギュレーション パラメータの変更。例えば、システム ブート コンフィギュレーションの変更
56.4. 成功したログインと失敗したログインの試行
56.5. ユーザー アカウントの作成、変更、削除

56.6. アクセスされたシステム/リソース
56.7. 誰がどこからリソースにアクセスしたかの特定と場所
56.8. 日付およびタイム スタンプ

57. 監査ログを複数のソースとセンサーから収集し、関連付け、そのようなイベントの再構築を可能にするために改ざん防止し、安全に保存します。

58. ログ イベント (できればリアルタイム) を監視するプロセスを確立し、不正な活動や攻撃対象を検出し、重要なイベントのログを見直します。

インシデント管理

ベンダーは、以下を保証するものとします。

59. 情報セキュリティーとプライバシーに関するインシデントへの迅速かつ効果的で組織的な対応を確保するために、役割とプロセスを明確に定義します。

60. 従業員および請負業者は、何がセキュリティー インシデントであるかを認識し、インシデントの可能性がある場合、またはインシデントが確認された場合、どこでどのように報告すべきかを学ぶための研修を受けます。

61. インシデントの分析と対応を担当する職員は、その分野の資格を有し、効果的なインシデント対応の実践について定期的な研修を受けます。

62. 報告されたすべてのインシデントのリポジトリを維持し、インシデントの影響を軽減するために取られた措置や、イベントから学んだ教訓を詳しく記録します。

63. Alludo は、組織が影響を受けるセキュリティー インシデントを発見すれば直ちに、または遅くとも 24 時間以内に通知します。

物理的および環境的セキュリティー

ベンダーは、以下を保証するものとします。

64. 業界標準に沿った物理的セキュリティーと環境管理のための方針および手順を実施します。

65. IT システム、アプリケーション、人員を収容する重要施設 (データセンター、運用サイトなど) は、事故、攻撃、不正アクセスから保護します。

66. 電子入退室管理、本人確認、警備員、訪問者管理年中無休の CCTV 監視など、不正侵入を防ぐためのセキュリティー対策を整えます。

67. CCTV の映像は、最低 30 日間、または法的規制により義務付けられている場合はそれ以上保存します。

68. 施設へのアクセスは、特定の目的のために許可された職員に制限し、定期的に見直します。

69. 来訪者は、エスコートされるようにし、入退室時間は記録され、常に来訪者 ID を着用します。アクセスカードまたは鍵は出発時に回収します。

70. 重要な施設は、無停電電源装置 (UPS) や発電機を使用して電力損失から保護し、継続的な操業を保証します。

71. UPS、発電機、煙探知機、消火システム、入退室管理システムなど、重要な機器には定期的なメンテナンスを行い、記録を残します。

72. 施設は耐火材料で建設し、火災警報器、煙探知器、温度センサー、浸水センサー、消火器を備え、自然災害から保護します。

73. ハード コピーとソフト コピーの両方の形式のデータの安全な廃棄メカニズムを定義し、紙媒体にはクロスカット シュレッダーを使用し、電子媒体にはサニタイズ、デガウス、破壊などの方法を使用します。

74. クリア デスク ポリシーにより、ポストイットや文書、リムーバブル メディアの安全な取り扱いを保証します。

75. 物理的および環境的管理は、少なくとも年 1 回、その有効性を評価します。

プライバシーおよびデータの保護

ベンダーまたはそのサブ プロセッサーが Alludo または Alludo の顧客のために個人データを処理する場合、ベンダーは以下のことを保証するものとします。

76. データ プライバシーのコンプライアンスおよびガバナンス

76.1. 適用されるすべてのデータ保護法を遵守します。

76.2. プライバシー マネジメントの枠組みを構築します。

76.3. プライバシー ポリシー、声明、通知、手続き (毎年の見直し) を実施します。

76.4. プライバシー ガバナンスのプロセスおよびリスク管理のプロセスを実施します。

76.5. 法規要件を遵守します。

76.6. Alludo の個人データの処理活動に関する最新の記録を維持します。

76.7. データ プライバシーに関する適切な役割と責任を定義し、実施します。

76.8. 上級データ プライバシー オフィサー (または同等者) を任命します。

76.9. データ プライバシー専門部署を設置します。

76.10. データ プライバシー コンプライアンス活動を調整する委員会を設置します。

77. データ保護およびセキュリティー対策

77.1. 業界標準のセーフガード (ISO/IEC 27001:2013、SOC2 など) を導入し、以下を実施します。

Alludo の情報を保護します。

77.2. 機微な個人データに対する追加的な保護措置を適用します (暗号化、仮名化など)。

77.3. 以下のようにアクセス コントロールを実施します。

77.4. アクセスは、知る必要のある最小限の特権ベースで制限します。
77.5. 終了時または役割の変更時にアクセス権を速やかに削除します。
77.6. 定期的にアクセス権の見直しを実施します。
77.7. 個人データを処理するすべての人員による機密保持の約束を確保します。

78. データ主体の権利の管理

78.1. データ主体の権利義務の履行において Alludo を支援します。
78.2. データ主体の要求を受けてから 2 日以内に Alludo に通知します。
78.3. 法的な要請がない限り、Alludo の指示にのみ従います。

79. インシデント レスポンス

79.1. Alludo のデータに関わる個人情報漏洩については、24 時間以内に Alludo に通知します。

下請業者への対応

ベンダーは、以下を保証するものとします。

80. ベンダーは、Alludo データの取り扱い、処理、または保存に関わるすべてのサブ プロセッサーについて、第三者によるリスク アセスメントを毎年実施します。これらの評価には、サブ プロセッ サーのセキュリティー管理、データ保護対策、関連規制の遵守、および全体的なリスク態勢の評価が含まれます。ベンダーは、要求に応じてこれらの評価の文書を提供し、特定されたリスクに速やかに対処し、サブ プロセッサーへの変更または重大な発見を適時に伝えます。当社は、評価結果を確認し、必要に応じて追加のセキュリティー対策を要求する権利を留保します。

事業継続性の管理

ベンダーは、以下を保証するものとします。

81. 事業継続性管理 (BCM) の方針を策定し、詳細な計画と手順を添付します。これらの文書は、組織の事業継続性目標を概説し、毎年見直しおよび承認を実施します。
82. 既存の事業継続性戦略の有効性を評価するために、BCM テストのフレームワークを開発し、実施します。
83. ビジネス インパクト分析 (BIA) は、少なくとも年 1 回、または重要な組織変更の後に実施します。
84. パンデミック対策に関する具体的な規定を含む危機管理計画を策定します。この計画で、従業員、訪問者、環境、資産の保護、重要な事業運営の維持に重点を置き、緊急事態への適切な対応を保証します。
85. 事業継続性管理システム (BCMS) は毎年有効性テストを実施し、各テストの詳細な記録を保管します。

<文書の終わり>