情報セキュリティおよびコンプライアンス管理規程

制定日：2025年10月01日

最終改定日：2026年2月10日（第3版）

第1章 総則

第1条（目的）

本規程は、合同会社AuroraNce（以下「当社」といいます）およびそのクライアントから預かる機密情報を適切に保護し、業務の安全性と信頼性を確保するための遵守事項を定めるものです。

第2条（適用範囲）

本規程は、当社の業務に従事するすべての役員、従業員、および業務委託パートナー（以下「スタッフ」といいます）に適用されます。

第3条（誓約）

スタッフは本規程を熟読し、別途定める「秘密保持誓約書（NDA）」に署名・捺印した上で、これを誠実に遵守する義務を負います。

第2章 アカウントおよびアクセス権限の管理

第4条（パスワード管理ツールの利用義務）

1. 業務におけるすべてのIDおよびパスワードの管理は、原則として当社が指定するパスワード管理ツール（1Password 等）を使用するものとします。
2. Webブラウザ（Chrome、Edge等）の標準機能によるパスワード保存および自動入力を禁止します。各ブラウザの設定において、保存機能を「OFF」にすることを必須とします。
3. パスワード管理ツール自体のマスターパスワードは、第三者に推測されにくい強固なものを設定し、PCの生体認証（指紋・顔認証）等と連携して厳重に管理することとします。

第5条（2段階認証の運用）

2段階認証（ワンタイムパスワード）が必要なアカウントについては、可能な限り前条のパスワード管理ツール内で生成コードを管理し、特定の端末（個人のスマートフォン等）への依存を排除することで、業務の継続性を担保します。

第6条（権限管理とGoogleグループの利用）

1. クライアントよりGoogleスプレッドシート、カレンダー、ドライブ等の共有を受ける際は、原則として個人のメールアドレスではなく、当社が指定する**「管理用グループアドレス」**への権限付与を依頼するものとします。
2. 業務終了または契約終了時は、管理者により速やかに当該グループからの除名処理が行われ、すべてのアクセス権が即時に失効する仕組みを運用します。

第3章 デバイスおよび利用環境のセキュリティ

第7条（使用端末の制限と届出）

業務に使用するPC等の端末（BYOD含む）については、当社が定めるセキュリティ基準を満たした上で、事前に**「端末届出書」**を提出し、許可を得たものに限定します。OSはメーカーのサポート期間内にある最新版（Windows 10/11、macOS 最新3バージョン以内等）の利用を義務付けます。

第**8**条（端末の必須セキュリティ設定）

業務に使用するPCについて、以下の措置を講じることを必須とします。

1. セキュリティソフトの導入: 当社指定の有料セキュリティソフト（Norton 360 等）を導入し、常時有効化すること。
2. ディスクの暗号化: 紛失・盗難時の情報漏洩を防ぐため、OS標準のディスク暗号化機能（WindowsのBitLocker、MacのFileVault）を「有効」に設定すること。
3. ログインロック: 端末起動時および復帰時には、必ずパスワードまたは生体認証を要求する設定とすること。

第**9**条（ブラウザの使い分けと誤操作防止）

複数のクライアント情報を扱う業務特性上、情報の混在（誤送信・誤操作）を防ぐため、クライアントごとにブラウザのプロファイル（ユーザー）を厳格に区分します。また、適切なプロファイルを自動選択するため、ブラウザ選択ツール（BrowserSelector 等）の導入・利用を推奨します。

第**4**章 ネットワークおよび物理的セキュリティ

第**10**条（通信環境の制限）

1. 暗号化されていない公衆Wi-Fi（カフェや施設のフリーWi-Fi等）への直接接続を禁止します。
2. 外出先で業務を行う場合は、以下のいずれかの方法にて通信を行うものとします。
    - スマートフォンのテザリング機能
    - 信頼できるVPN（Virtual Private Network）サービスを経由した接続（※Norton 360付属のセキュアVPN等）

第**11**条（物理的な覗き見防止）

第三者の目に触れる可能性のある場所（カフェ、コワーキングスペース、新幹線等）で業務を行う際は、必ずPC画面に**「プライバシーフィルター（覗き見防止フィルム）」**を装着することとします。また、離席時は時間の長短にかかわらず、必ずPC画面をロックすることを義務付けます。

第**5**章 情報の取り扱いおよび禁止事項

第**12**条（生成**AI**の利用制限）

ChatGPT等の生成AIを利用する際は、入力データがAIの学習に利用されない設定（オプトアウト等）を確認した上で利用するものとします。クライアントの未公開情報、個人名、機密情報（売上データ、独自のノウハウ等）を生成AIに入力することは厳禁とします。

第**13**条（情報の持ち出しおよび目的外利用の禁止）

1. 業務上知り得た情報を、許可なく外部（私用のクラウドストレージ、USBメモリ、個人のメールアドレス等）へ保存・持ち出しすることを禁止します。

2. 契約終了後においても、業務上知り得た秘密情報を第三者に開示・漏洩してはなりません。

第**6**章 監査および事故対応

第**14**条（利用状況の監査）

当社は、セキュリティポリシーの遵守状況を確認するため、必要に応じてスタッフの端末設定やパスワード管理ツールの利用状況等の監査を行う権利を有します。

第**15**条（事故発生時の報告義務）

ウイルス感染、PCの紛失・盗難、情報の誤送信等のセキュリティ事故、またはその恐れが発生した場合は、直ちに当社代表者へ報告する義務を負います。報告を怠った、または隠蔽を図った場合、契約解除を含む厳正な対処を行います。

第**16**条（契約終了時の措置）

スタッフとの契約が終了した場合、当社は直ちに当該スタッフのアカウント（1Password、Google グループ、チャットツール等）を停止・削除します。スタッフは、貸与物および保有する業務データを速やかに返却・破棄するものとします。

以上