情報セキュリティルール

2025/07/01作成

1. 情報セキュリティ基本方針

顧客からお預かりしたデータおよび成果物は、第三者に漏洩・改ざんされることのないよう厳重に管理します。
セキュリティ対策を継続的に見直し、業務の特性に応じて適切な対策を講じます。

2. 情報の取り扱い

顧客情報・ログイン情報・制作データ等は、業務目的以外には一切使用しません。
機密性の高い情報（ID・パスワード等）は、アクセス権限を明確に限定できるGoogleドキュメントや1Passwordで厳格に管理し、作業上第3社へ共有する際には編集・閲覧範囲を明確に設定した上で取り扱います。

3. 使用端末とアクセス管理

業務用PCはウイルス対策ソフトを導入し、OSおよびソフトウェアは常に最新の状態に更新します。
端末にはパスワードロックを設定し、第三者の物理的アクセスを防止します。

4. クラウド・外部サービスの利用

Google Driveなどのクラウドサービスを利用する際は、二要素認証を有効にし、アクセス権限の管理を徹底します。
外部との共有時には必要最小限のアクセス権限（閲覧・編集の範囲）を設定し、誤送信や情報漏洩を防止します。

5. 外部媒体と持ち出し

USBメモリ等の外部記憶媒体は原則使用しません。やむを得ず使用する場合は、暗号化またはパスワード保護を実施します。
業務用データの社外持ち出しは最小限にとどめ、盗難・紛失に備えた対策を講じます。

6. インシデント対応

万が一情報漏洩や不正アクセス等のセキュリティインシデントが発生した場合は、速やかに発注元に報告し、原因調査と再発防止策を講じます。