情報セキュリティ・情報管理規定

第 1 章　各自の端末の取り扱い

1 条（端末のログインアカウント）

- パスワードは半角英数字 8 文字以上（小文字、大文字、数字を必ず含める）とする。
- 四半期に 1 度（1,4,7,10 月）の月初めにパスワードを変更すること。
- 全員のパスワードは 1 部プリントして金庫に保管する。（会長管理）
- 各自はパスワードを厳格に管理するよう務める。
- 自動ログインは必ずオフにする。

2 条（セキュリティソフト）

- 会社で支給するソフトをインストールする。
- アップデートは必ず実施する。
- ウイルス検出があった場合は CSR 責任者に報告する。

3 条（OS のアップデート）

- セキュリティアップデートは必ず実施する。
- OS のアップデートについては CSR 責任者に相談して決める。

4 条（ネットモラル）

- ウイルス感染の可能性が高いサイトは閲覧しない（アダルト、海外サイトなど）。
- 疑わしいアプリケーションはインストールしない（Windows＝スキャンに引っかかるものはインストールしない）。
- ダウンロードしたファイルについては必ずチェックする。

- メールに添付されている不審なファイルは開かない（クリックしない）。

5 条（端末の外への持ち出し）

- 共有端末（PC、タブレット、スマホ、カメラ）を持ち出す場合は CSR 担当者に申し出て、所定の手続きを行う。

6 条（SNS、ブログ等の WEB メディアサービス）

- 会社の機密情報に関する書き込みは行わない。
- 取引先との私的交流に関しては機密情報が漏洩しないよう細心の注意を払う。
- SNS 等のアカウントの乗っ取り、なりすましを防ぐためにセキュリティ設定は必ず利用する。

7 条（離席時）

- 端末を画面ロックまたはスリープ状態にする（パスワードを入力しないと再開できない状態にする。）

8 条（退勤時）

- 各自の端末の電源は切る。

9 条（私物端末の取り扱い）

- 私物端末での業務は禁止する。但し、必要と判断される場合は所定の手続きを行い、許可を得ることで可能とする。
- 社内ネットワークはゲスト用のネットワークを利用する。
- 私物端末には社内のデータを移さない。
- 私物端末上で、会社アカウントでのメールソフト、コミュニケーションツールの使用は禁止する。

第 2 章　機密データの取り扱い

---

1 条（機密データ）

- アカウント情報（IDPW など）が記載されている全てのメディア、ファイル、書類。
- 金融関連に関する情報（クレジットカード番号など）が記載されている全てのメディア、ファイル、書類。

- 請求、見積に関する情報が記載されている全てのメディア、ファイル、書類。
- 写真、氏名、住所、電話番号などの個人情報が記載されている全てのメディア、ファイル、書類。
- 契約書。
- 業務上知り得た情報。
- 判断出来ないものに関しては責任者に確認する。

2 条（データの共有）

- 社内で機密データを受け渡しする時は、LANDISK を使用する。
- 社内ネットワーク、ゲスト用を除いた WiFi は社員のみアクセス可とする。
- 社内でチャットツールで機密データの受け渡しをしない。
- クラウドサービスで機密データの受け渡しを原則しない。
- 社内ネットワークが使えない状況（他事務所、出張など）で受け渡しが困難な時は、クラウドサービスのみ利用できる。

3 条（進捗管理ツール）

- 社外の人と共有しているプロジェクトには機密データを置かないよう注意する。
- アカウントは厳重に管理する。
- パスワードは四半期に 1 度、各自の端末のパスワード変更と同じタイミングで変更する。

  （その際、端末と同じパスワードは使用しない。）

4 条（保管・破棄）

- 自身の机周りの整理整頓を常に心がける。
- 機密データを含む全ての物理データは、会社指定の金庫へ保管する。
- 不要になった HDD は物理的に破壊して破棄する。

- 不要になった CD、DVD、書類はシュレッダーで破棄する。
- 破棄を行う際は、会社指定の手続を経て実施する。

  ※手続きは、破棄申請 → CSR 責任者に許可 → 台帳に記録 → 破棄実施。

5 条（アウトソーシング）

- アウトソーシングする場合は、弊社指定の NDA を締結した会社に限る。

  なお、情報セキュリティ指針が存在しているか確認を取る。

第 3 章　入室管理

- 部外者の入退室は、応対した者が氏名、会社名、入室・退室の日時を記録する。（配達業者、工事関係者、会社関係者（外部顧問）は除く）
- 最初入室者と最終退室者は会社所定のノートに時刻と氏名を記録する。
- 最終退室者は、共有ハードディスク、共用 PC の電源を切る。

第 4 章　体制

---

1 条（社内の連絡体制）

- 取引先、または取引が発生する予定のクライアントに対する責任者は藤本部長とする。
- クライアントに影響を及ぼすセキュリティ事故等が発生した場合、藤本部長に報告する。
- 情報セキュリティ担当者は CSR 担当者とする。

2 条（社内のセキュリティ体制の確認）

- 四半期に 1 度（1,4,7,10 月）、社内セキュリティ担当者は役員を含む全社員に対してのセキュリティ教育を実施する。
- 役員を含む全社員は、毎月セキュリティルールが遵守されているかのチェックシートを記入後、提出する。
- チェックシート記入と提出の実施後、遵守されていない項目が発覚した場合、セキュリティ担当者は 1 条 1 項で定める責任者に報告する。

- セキュリティ担当者は責任者により任命する。

第 5 章　セキュリティインシデントが発生した場合

以下の通り対応する。

1： 発見・報告

発見次第、体制に基づき報告を行う。

- 応急処置より前に報告を行い、報告後に応急処置、調査を行う。

2： 応急処置（初動）

セキュリティ担当より方針を決定、応急処置を行う。

- 該当する端末のネットワーク遮断。
- 各アカウントの停止。
- 各サービスログイン停止処理。

3： 調査

原因・被害状況の調査を行う。

- 内部（人的ミス）、外部（盗難など）によるものか。
- 漏洩した情報の種別確認。
- PC 紛失（盗難）の場合は保管場所と使用方法の確認。

4： 報告・事後対応

- 再発防止策を策定する。
- 損害の補償についての措置を講じる。

付則

本規定は 2022 年 11 月 24 日より施行する。