情報セキュリティ基本方針

2019 年 10 月 1 日施行

株式会社 サンキ

情報セキュリティ基本方針

1. 情報セキュリティ基本方針

株式会社サンキは個人情報も含めた情報資産の安全性および信頼性の確保に万全を期し、社会とお客様の信頼に応えるため、情報セキュリティ基本方針を定め、これを実施し推進することを宣言いたします。

(1) 情報資産に対しては、業務上必要な者のみに権限を与え、不正アクセス、紛失、漏えい、改ざん及び破壊などの発生予防に努めるとともに、万一、事故が発生した場合には、再発防止策を含む適切な対策を速やかに講じます。
(2) 情報セキュリティに関する法規制やその他の要求事項を遵守します。
(3) 全社員及び関連するすべての人々に、情報セキュリティの重要性を認識させるとともに、情報資産の適切な利用を行うように周知徹底を図ります。
(4) 当社の経営者は本方針の遵守により、当社およびお客様の情報資産が適切に管理されるよう主導し、継続的な改善を図ります。

2. 全社基本ルール

(1) OS とソフトウェアのアップデート
パソコンの OS は Windows　Update の自動更新を利用して更新する。
Microsoft　Office は自動更新を利用して更新する。
その他のソフトウェアも、可能な限り最新の状態を維持する。

(2) ウイルス対策ソフトの導入
業務で利用する機器には以下のウイルス対策ソフトを導入し、定義ファイルを随時更新する。持ち出し用ノートパソコンは利用時に定義ファイルの更新を確認する。
＊アバスト無料アンチウィルス（定義ファイル更新方法：自動）

(3) パスワードの管理
ログインやファイル暗号化に使うパスワードは、初期パスワードのままで使用したり、名前、電話番号、生年月日は使わない。
パソコンへのログインは現在のパスワードの語尾に 3ki をつけ再設定する。

3. 仕事中のルール

(1) メールの利用

・メールを送信する際は、宛先のアドレス、添付ファイルを間違えていないか確認してから送信する。
・メールの CC,BCC を理解し、BCC で複数相手のアドレスを指定するなどして、意図しないメールアドレスの漏洩に注意する。
・私物 PC でメールを見ることは原則禁止とする。
・心当たりのないメールには十分注意し安易に添付ファイルを開いたり、リンクを参照したりしない。

(2) インターネットの利用

・就業時間内は私的なウェブアクセスは慎む。
・不審なサイトへのアクセス及び社用メールアドレス登録を禁止する。
・業務とは無関係な動画を視聴しない。
・社用 PC から私的なメールサービスや SNS にアクセスしない。

(3) SNS を利用する際には以下を遵守する。

・業務上必要のない限り、業務に関する情報の書き込みを行わない。
・取引先従業者と SNS 上で私的に交流する場合双方の立場をわきまえ、社会人として良識の範囲で交流する。
・セキュリティ設定を行い、アカウントの乗っ取りなりすましに注意する。

(4) データのバックアップ

・データのバックアップは各自 1 か月を標準とし行う。

(5) クリアデスク、クリアスクリーン

・重要書類の入った電子媒体を業務利用時間以外は机上に放置しない。
・離席時には、パソコンの画面をロックしクリアスクリーンを徹底する。(Win+L でスリープモード)
・スリープモード設定は 15 分を標準とし設定する。

(6) 秘密情報の社外への持ち出し

・秘密情報を社外に持ち出すときには、ドライブ全体を暗号化するか、ファイル自身を暗号化する。

・USB メモリなどに保存して持ち出す場合にはドライブ全体を暗号化するかファイル自信を暗号化する。

・USB メモリはパスワード付きのものを使用する。

・電子媒体はケースに入れて USB メモリはタグ、ストラップなどをつけて紛失を防止する。

(7) 秘密情報の保管

・退社時、未使用時は USB メモリ、小型ハードデスク等の電子媒体及び重要書類は机の引き出しや、鍵付きキャビネットに保管し施錠する。

(8) パソコンの操作記録

・社内ネットワークに接続して利用するパソコンは、情報漏洩防止のためにファイルへのアクセス記録やインターネットアクセス記録、パソコンの操作記録を取得するよう設定されている。

(9) 私物機器の利用

・私有の情報機器を業務で利用する場合は、次頁表を参照する

情報機器の種類	遵守事項
パソコン	・個人のパソコンの使用は原則禁止とする ・社内ネットワークへの接続を禁止する ・個人のメールアドレスに秘密情報を添付して送信することを禁止する ・社用メールアドレスで受信した秘密情報の含まれるメールを、個人のメールアドレスに転送することを禁止する
スマートフォン、タブレット端末携帯電話等記憶・通信機能を備えた機器	・社内パソコンへの接続は、原則として禁止する ・秘密情報の保存を禁止する ・個人のメールアドレスに秘密情報を添付して送信することを禁止する ・社用メールアドレスで受信した秘密情報の含まれるメールを、個人のメールアドレスに転送することを禁止する
USB メモリ外付け HDD などの記憶機能を備えた機器	・会社で貸与した機器を利用する ・私有物の利用を禁止する

4. 社員の皆さんへ

(1) 社員の守秘義務

・社員には、守秘義務があります。基本方針を遵守し、情報セキュリティに役立てて情報セキュリティの事故を防ぎましょう。

(2) もし事故が起きてしまったら

・もしもセキュリティ事故が起きてしまったら、すぐに直属の上司に報告し二次災害や事故の影響を最小限に止めましょう。

※ 報告を受けた上司は、緊急連絡体制表の順に報告し指示を受けてください。