個人情報保護のための内部規定

〔個人情報の管理組織及び管理責任者の設置〕

１．個々の業務遂行における管理者が個人情報の管理責任を負うものとし、統括する管理責任者として会長がこれに当たる。

〔取得に際しての利用目的の通知等〕

２．お客様から個人情報を取得する場合は、利用目的を通知し、お客様の了解を得た上で行うものとする。

〔機密情報・個人データの取扱制限（ 目的外利用、第三者への提供、外部への情報漏洩行為の禁止）〕

３．機密情報・個人データを目的外に利用すること、第三者への提供、外部への情報漏洩を厳に禁止する。また、機密情報・個人データの取扱い（取得・入力・移送・送信・利用・加工・保管・バックアップ・消去・廃棄等）に関する、場所・手段・端末・作業者等は、それぞれの業務遂行に際して正当かつ必要な範囲に限定しなければならない。

〔機密情報・個人データの無断複製禁止〕

４．機密情報・個人データを無断で電磁的方法又は複写機等による複製をしてはならない。

〔機密情報・個人データを含む紙や機器の施錠管理〕

５．機密情報・個人データを含む紙や機器の保管は、施錠できるキャビネット等に収納して施錠して管理することとする。

〔ＰＣ、記録媒体を破棄する場合の再読できない措置〕

６．機密情報・個人データが格納されているＰＣ、記録媒体を破棄する場合は、当該情報及びデータを完全に削除し、再読できない措置を施すこととする。

〔定期的な安全管理措置の見直しと改善〕

７．年に１回以上、安全管理措置の見直しを行い、必要に応じて適切な改善を図るものとする。

〔人的安全管理措置（教育訓練を含む）〕

８．個人情報を取扱う従業者とは秘密保持契約を締結する。

９．秘密保持契約に違反した場合、状況に応じて懲戒処分、減給、損害賠償請求等の措置を行う。個人情報の管理責任者が状況を把握、判断し、会長が処分を決定する。

１０．すべての従業者に対し個人情報保護及び安全管理措置に関する教育を、採用時及び定期的に実施する。

１１．再委託先に対しては、同水準の安全管理措置等を義務付ける。

〔漏洩などの事故があった場合の委託元への報告・連絡体制〕

１２．漏洩などの事故があった場合は、本規程第１条「個人情報の管理組織及び管理責任者の設置」の体制に従って、直ちに委託元へその旨を通知するものとし、その経緯を記載した文書を遅滞なく委託元に提出するものとする。

〔物理的安全管理措置〕

１３．機密情報・個人データを取扱う作業場所や情報システムの部屋における入退室管理機密情報・個人データを取扱う作業場所や情報システムの部屋は、施錠等の措置を講じるものとし、秘密情報等を取扱う権限者以外の者が許可無く立ち入らないように入退室管理を行い、その記録を保管するものとする。

１４．機密情報・個人データを含む媒体、書類、携帯可能なコンピュータなどの机上への放置禁止

機密情報・個人データを含む媒体、書類、携帯可能なコンピュータなどの机上への放置を禁止する。

１５．機密情報・個人データを取扱う機器・装置などの破壊や火災、停電からの保護

機密情報・個人データを取扱う機器・装置などの管理者は、それらの破壊や火災、停電から保護するために適切な管理に務める。

１６．ＰＣの持込み・持出しの原則禁止

特段の理由による責任者の承認がある場合を除き、ＰＣの持込み・持出しを禁止する。

１７．責任者の承認を得て、持込・持出しするＰＣの情報漏洩対策（暗号化等）ＰＣを持込・持出しする場合は、責任者の承認を得て、情報漏洩対策（暗号化等）を充分に施すこととする。

〔技術的安全管理措置〕

１８．機密情報・個人データを取扱う従業者の本人認証

機密情報・個人データを取扱う従業者は本人認証（ＩＤとパスワード等による）を行う仕組みとする。

１９．機密情報・個人データを取扱う従業者個人ごとのＩＤ割り当て

機密情報・個人データを取扱う従業者個人ごとにＩＤ割り当てを行う。

２０．機密情報・個人データを取扱う従業者ＩＤの定期的な見直し

機密情報・個人データを取扱う従業者ＩＤは、定期的な見直しを行うことを義務付ける。

２１．パスワードの管理ルールに基づく運用

パスワードの管理ルール基づく運用を行うこととする。

２２．機密情報・個人データへの必要最少限のアクセス権限付与と認証、記録及び保管

機密情報・個人データにアクセスできる権限者を出来る限り限定するとともに、ＩＤ、パスワードその他の認証手段を用いたアクセス制限を行うものとする。なお、個人情報については、アクセス記録を保管するものとする。

２３．機密情報・個人データの取扱い記録（受渡しの記録、バックアップ、複写の記録等）

機密情報・個人データを取扱ったときは、その受渡し、バックアップ、複写等の記録を行うこととする。

２４．ウィルス対策ソフトウェアの導入とパターン・ファイルの最新版への更新

すべてのＰＣ等にウィルス対策ソフトウェアを導入し、パターン・ファイルの最新版への更新を常時行う。

２５．機密情報・個人データの移送・送信時の暗号化などの対策

機密情報・個人データの移送・送信時は、暗号化などにより不正アクセスを防止する。

２６．機密情報・個人データを取扱う情報システムのアクセスログの採取

機密情報・個人データを取扱う情報システムにあっては、アクセスログを適宜採取し、不正侵入の有無を監視する。

２７．外部ネットワークからの不正侵入防止

外部ネットワークからの不正侵入に対する適切な防御策として、ファイアウオール設置、認証システム導入などの仕組みを講ずるとともに、脆弱性対策として、パッチの適用、バージョンのアップを都度実施するものとする。

〔メール誤送信事故の防止徹底〕

２８．メール誤送信事故防止のため、他者による二重確認、又は自己二重確認機能を用いて、その徹底を図る。

〔本人から求められた場合の個人情報の開示又は訂正〕

２９．個人情報の開示又は訂正（削除を含む。以下同じ。）を本人から求められた場合、個人情報の管理責任者は、速やかにこれの対応措置を講ずること。

〔個人情報の取扱いに関する苦情があった場合の報告・連絡体制〕

３０．個人情報の取扱いに関する苦情があった場合は、本規程第１条「個人情報の管理組織及び管理責任者の設置」の体制に従って報告・連絡するとともに、その是正措置を検討し、結果を遅滞なく関係者に報告するものとする。

なお、上記規則に拘わらず、受託業務にて業務委託先にて作業する場合においては、業務委託先の規則及び指示に従うこととする。