情報セキュリティのルール

		承認
発行日		
最終改訂日		
版数		
廃止日		

○○○株式会社

改訂履歴			
版数	改訂理由	改訂内容	改訂日
1	新規発行	なし	

１．目的

本ルールは、全従業員が利用する。

このルールを守り、セキュリティレベルを維持して個人情報の取り扱いに関するリスクから個人情報を保護することを目的とする。

２．入退室管理

２－１．部外者の入退室管理

（１）部外者（清掃業者、ビル管理会社、コピー保守業者なども含む）がオフィスに入室する際は、受付票を記入して名札を着用する。

（２）オープンスペース以外に部外者を通してはならない。部外者が受付を行わずにオフィスに入って来た際には、オープンスペースへ移動してから対応を行う。

（３）顔なじみの顧客や業者であっても、オフィス内では従業員が同伴する。

２－２．従業員の入退室管理

（１）オフィスを開錠または施錠した従業員は、オフィス開錠・施錠管理表を記入するが警備会社の入退出管理システムがある場合 ID カード管理台帳を作成し定期的に確認を行う。

３．媒体の取り扱い

３－１．電子媒体の取り扱い

（１）私物の電子媒体（USB メモリ、DVD、CD-R 等の電子情報を保存できるもの）を持ち込んではならない。必要な場合は、情報管理者の許可を得る。

（２）電子媒体に個人情報を保存してはならない。ただし、業務上必要な場合には、情報管理者の許可を得た上で利用してもよい。電子媒体に個人情報を保存する場合は、個人情報保存媒体管理表に記入する。

（３）個人情報を保存している電子媒体は、必ず施錠して保管する。

（４）個人情報を保存している電子媒体を廃棄する際は、物理的に破壊する。

３－２．個人情報が記載された紙媒体の取り扱い

（１）不要となった時点で速やかに裁断処理を行う。

（２）裏紙として利用してはならない。

（３）プリンタに出力した場合は、速やかに回収する。

（４）不要にコピーしたり、個人的に保管してはならない。

（５）施錠して保管する。

３－３．授受の記録及び確認

（１）電子媒体及び紙媒体を利用して個人情報の授受、直接の受け渡し、移送等を行う場合は、個人情報授受管理表を記入する。また、移送を行った場合は、受取確認を行う。

４．パソコン及び周辺機器の取り扱い

４－１．パソコン及び周辺機器の持ち出し、持ち込み

（１）無断でパソコンや周辺機器の持ち込みや持ち出しをしてはならない。必要な場合は、情報管理者または社内システム管理者の許可を得る。ただし、個人情報を保存しているパソコンや機器を持ち出す場合は、個人情報保護管理者の許可も得なければならない。

（２）個人情報を保存しているパソコンや機器を持ち出す場合は、データを暗号化するかファイルへのパスワード設定もしくは BIOS パスワード等による閲覧制限を行なわなければならない。採用する手法に関しては、個人情報保護管理者に個人情報の内容を報告した上で、社内システム管理者の指示に従う。

（３）個人保有のパソコンや社外から持ち帰ったパソコンを社内ネットワーク接続する前には必ずシステム管理者の検疫を受ける事。またシステム管理者はその内容を記録保存しなければならない。

４－２．パソコン及び周辺機器利用時の注意事項

（１）無断で以下のことを行ってはならない。必要な場合は、情報管理者の許可を得る。

・パソコンや機器の分解、改造
・設定や配線の変更および機器の増設
・ソフトウェアのインストール

（２）個人情報を保管しているノートパソコンにワイヤーロックを施していない場合は、退社時に施錠保管する。

（３）パソコン内に個人情報を保管してはならない。個人情報の保管は、適切なアクセス権が設定されたサーバの所定フォルダ内に行う。ただし、電子メールのアドレス帳や添付ファイルは例外とし、これらは不要となった段階で速やかに消去すると共に、パソコンへのログイン制限によって保護する。

（４）５分でスクリーンセーバーが起動し、パスワード入力なしでは復帰できない設定とする。また、可能な限り、離席時には手動でパソコンからログオフする。

（５）外出時や帰宅時には、パソコンの電源を切る。

４－３．携帯電話・スマホの取り扱い

（１）社外で携帯電話やスマホを取り扱う際には、紛失しないよう十分注意する。

（２）携帯電話やスマホで、業務に関する個人情報を含むメールを送受信した場合は、用件終了後、速やかに消去する。

（３）携帯電話やスマホを紛失した際は、速やかに情報管理者に連絡する。

５．電子メール、インターネットの利用

（１）電子メール利用時には会社支給のメールアドレスを利用することとし、私用メールアドレスおよびWEBメールの利用は禁止する。

（２）電子メール、インターネットを業務外の目的に利用してはならない。

（３）電子メールの本文に個人情報を記載することは極力控え、宛名等の必要最低限の内容にとどめる。個人情報を記載する必要がある場合は添付ファイルに記載し、添付ファイルの暗号化またはパスワード設定等による保護を行う。

（４）添付ファイルを開く際には信頼できる相手かどうか確認し不審なメールの場合は社内システム管理者に確認してもらうこと。

（５）インターネットからファイルをダウンロードでする場合、事前にシステム管理者へ報告した業務に関するデータのみとする。

６．パスワード管理

（１）パスワードを設定する際は、英数字を交えた 8 文字以上の推測が困難な文字列とする。

（２）パスワードを忘れた際は、システム管理者に申し出て、その指示に従う。

７．整理整頓

（１）部外者が容易に触れることができる場所では、個人情報の保管や放置を行ってはならない。

（２）退社時には机の上を整理整頓し、媒体や書類を放置したまま退社してはならない。

（３）業務中であっても、随時、整理整頓を行い、個人情報の盗難や紛失が発生しないよう注意する。

８．トラブル時の対応

（１）以下の場合には、速やかにシステム管理者に連絡する。また情報管理者および個人情報保護管理者に連絡する。

・個人情報の漏えいや機器の紛失、盗難またはその可能性がある場合

・情報システムの不備など、セキュリティ事件や事故に繋がる可能性に気付いた場合

・ウィルス感染の疑いやパソコンに異常が発生した場合

上記の場合すぐに LAN ケーブルを抜き電源を切ってシステム管理者へ連絡する

９．トラブル時のシステム管理者の対応

（１）前項のトラブル発生時には以下の対応を実行すると共に情報管理者および個人情報保護管理者に連絡する。

・紛失、盗難の場合は機器の遠隔ロックを即時実行する。

・情報システムの不備などの指摘を受けた場合はすぐにインシデント対策を行う

・ウィルス感染の場合は機器を隔離し原因の特定と対策を実装し再発防止のためユーザーへ警告をする