安全管理細則（ユーザ用）

株式会社＊＊＊＊＊

制　定　平成２６年　９月　１日　初　版

個人情報保護 管理者	安全管理 責任者

目次

第１章　目的

第１条　目的

本細則は、別途定める「安全対策管理規程」によって、当社の従業者が当社の執務室、作業場及びコンピュータ・システムを利用するに当たり、その遵守事項を定め、安全かつ安心して利用できるよう維持することを目的とする。

第２章　物理的安全対策

第２条　執務室及び作業場の管理者

執務室及び作業場の安全管理は、安全管理責任者が行う。従業者は、安全管理者の指示に従う。

第３条　従業者の責務

当社の従業者は、当社室内において盗難その他の犯罪が発生した時及びそれに類する事実を発見した時は、速やかに部門長または安全管理責任者に急報してその指揮を受けるほか、臨機応変の措置をとる。部門長又は安全管理責任者が不在の場合は、その上位者に報告してその指揮を受ける。

２　発見した事実が、個人情報保護に関するものである場合。別途定める「個人情報保護基本規程（緊急事態への準備）」に従って、個人情報保護管理者に報告する。

第４条　当社出入口の鍵の管理

当社出入口の鍵の管理は、次に定めるとおりとする。

（１）　当社及び各拠点出入口の鍵は、代表取締役によって鍵所有権限があるとして指定された者（以下「鍵所有者」という。）が管理する。

（２）　出社の際に当社及び各拠点出入口の開錠を行った鍵所有者は、室内に異状がないか確認する。

（３）　退出時の施錠は、最後に帰社する鍵所有者が、社内の戸締まりや火気などのチェックを行った後、別途定める「最終退出点検表」に、点検項目の状況、施錠の時間及び氏名を記録する。

（４）　「最終退出点検表」は、安全管理者、又は安全管理者が指名したものが、毎月、前月分について記入漏れや異常などがないか点検する。

第５条 入室資格の付与

当社の従業者は、安全管理責任者が定めた「社員証」を着用して業務に従事する。

２　配送等の出入業者は原則として荷捌きスペースで業務を行い、執務室及び作業場には入室させない。作業の必要上やむをえず入室させる場合は、退出までの間必ず担当社員が同行する。

３　当社の従業者は、自分宛に訪問者があり、執務室または作業場に立ち入るときは、「入退受付票」を本人に記入していただき、身元および用件を確認して入室を許可し、作業場内では「ゲストカード」を着用させる。また、退室をする時には退室時間を「入退受付票」に記録する。なお、「入退受付票」は、総務が１年間保管し、保管期限を過ぎたも

のはシュレッダーなどで裁断する。

第６条 入室資格の特定

作業場への入室資格は、原則として総務部門が指定した「社員証」の交付を受けた者に限る。エレベータやコピー機などの保守点検の為に、保守管理会社の作業要員が執務室に入室する際は、予め当社に届けるものとし、「ゲストカード」を着用していただく。

第７条 入室資格者の確認

各部門の責任者は、当社の従業者が「社員証」を着用している事の確認を適宜行う。

２　当社の従業者は、特に不審と思われる訪問者に対して入室を拒否し、安全管理責任者又は各部門の責任者に連絡するとともに、適切な措置をとる。

第８条 訪問者の入室資格

訪問者の入室資格は、入室に際し、貸与された「ゲストカード」を見やすい部位に着用している者とする。

２　原則として、訪問者が執務室に入室する場合は、社員が同行しなければならない。ただし、当社の代表者から特に指名されたものを除く。

第３章　コンピュータ・システム安全対策

第９条 パソコン及び媒体の管理

当社の従業者は、当社の業務を行う上で、当社のサーバ、プリンタなどのネットワーク資源を利用する場合、以下に留意する。

（１）　原則として、各自に配付されたパソコン、記録媒体及び端末等の機器のみを使用することとし、外部のパソコン、記録媒体及び端末等を、当社ネットワーク及び機器類に接続してはいけない。何らかの必要性があって個人や外部法人所有の機器などを当社ネットワーク内で使用する場合には、システム管理者の許可を得ることとし、システム管理者は、当該機器が安全であることを確かめた上で、「外部機器・媒体持ち込み承認記録」にて使用を承認する。

（２）　発行されたアカウントの貸し借りを行ってはならない。パスワードは定期的（少なくとも６カ月に一度）に変更し、外部に漏れないよう管理すること。

（３）　外部から持ち込んだファイル及びネットワークからダウンロードしたファイルは、必ずウィルスチェックを行うか、自動でウィルス検知を行うことができる PC で利用する。また、毎週１回ディスクのウィルスチェックを行うこと。

（４）　パソコンの取り扱いには、十分注意すること。特にノートブックパソコンや外部記録媒体の持ち運び時は、盗難、破損などに対する注意する。

（５）　ノートブックパソコンやデータを記録した外部記憶媒体を社外に持ち出す場合は、「ノート PC、可搬媒体持ち出し記録」で申請した上で顧客へのプレゼンもしくはコンバートデータの受理の場合に限ることとし、原則としてそのほかの場合に社外に持ち出してはいけない。尚、中に保管された個人情報又は機密情報がある場合は、そのデータを暗号化するかパスワードをかけて、厳重に取り扱うこととし、移動中、

身体から離してはならない。

（11）脆弱あるいは不正行為を行う可能性があるソフトウェア（例：Winny,Share,スパイウェアなど）を使用してはならない。また、それ以外であっても、業務に不要なアプリケーション等のソフトウェアのセットアップ（インストール）を行ってはならない。

（12）電源を入れたまま長時間放置をしないこと。原則は、電源を切断すること。最低でもログオフかパスワード付スクリーンセーバーの起動をしておくこと。ログオフ等を忘れた場合に備え､スクリーンセーバーが 10 分以内に自動起動するよう設定する。

（13）社給の携帯端末を利用する場合、別途定める「携帯端末取扱マニュアル」を遵守する。また、紛失しないよう注意して携帯するものとするが、万が一紛失した際は、速やかに安全管理責任者に届け出ること。

（14）当社社員は、許可無くモデム、ルータ及びリモートアクセス機器などの通信機を接続してはならない。接続する場合は、システム管理者の承認を得た上で行い、システム管理者は、当該危機に対して通信系路上の不正アクセス及び漏洩対策を行うこと。

第４章　データなどの管理

第１０条 データ等の管理

当社の従業者は、情報資産を記録したデータ（紙、電子媒体を含む。以下「データ」という。）が、当社の重要な資産であることを認識し、その取扱及び授受について十分注意する。当社は、データ等の取扱及び授受についてのセキュリティを確保するために、以下を定め、従業者は、それを遵守する。

（１） データの取得・入力

データを取得する際は、可能な限り安全な方法を選択する。また、取得したデータを電子化する際は、誤入力を防ぐために、入力内容のチェックを行うこと。できるだけ入力者以外によるチェックがのぞましい。

（２）データの利用・保管

データは、その重要度に応じて、担当した部門の責任者が鍵のかかる書棚に責任をもって保管、管理する。

顧客から預かったデータは、鍵がかかる書棚や倉庫に保管する。データの保存期間は原則として設定完了後 2 カ月とする。保管する必要がなければ速やかに顧客に返却又は廃棄する。

（３）移送・送信

機密情報が記載された文書等を移送する際は、紛失･盗難などの危険性を避けるような方法で行う。郵便などの場合は、重要度に応じて配達記録郵便や書留郵便などを利用する。社外で本人から取得、または委託先へ持参する等により持ち運びする場合は、機密情報であることを自覚して厳重に取り扱うこととし、移動中絶対に身体から離してはならない。また、受託時の受け渡しには、授受の記録をとり保管する。

（４）廃棄

顧客から預かったデータを顧客の指示で廃棄する際は、シュレッダーで裁断してか

ら廃棄する。

パソコン上のデータを廃棄する場合は、再利用できないよう完全に消去する。

電子媒体を廃棄する場合は、再利用できないよう物理的に破壊する。

規程等の制定及び改廃

本規程の制定及び改廃は、安全管理責任が、個人情報保護管理者の承認を得て行う。

付則

制定：平成２６年　９月　１日　初　版