株式会社新東海旅行

情報セキュリティ管理規程

第１章　総則

（目的）

第１条　この規程は、会社保有情報等の適切な活用・保全・運用に関し、会社取締役・社員全員が職務遂行上遵守すべき基本的事項を規定し、全社的情報セキュリティ管理を実現することにより、経営管理の質的向上を図ることを目的とする。

（適用範囲）

第２条　会社のすべての会社保有情報のセキュリティ管理は、この規程に則って行う。

２　顧客および社員等に関する個人情報については、この規程よりも高度なものを求める部分については、さらに別途定める「個人情報取扱基本規程」に基づくものとする。

（用語定義）

第３条　この規程における用語の定義は次のとおりとする。

（１）会社保有情報とは、電磁化・非電磁化にかかわらず会社が保有するすべての情報をいう。

（２）会社保有情報には、別段の定めのない限り、職務の遂行によって新たに生成または拡充された情報が含まれるものとする。

（３）会社保有情報には、会社の所有する情報だけでなく、他社（者）から正当に入手し、保有する会社保有情報も含むものとする。

２　他社（者）とは、会社および会社取締役、社員以外の個人、法人、団体等をいう。

３　社員とは、会社と雇用関係（契約社員およびパートタイマーを含む。）を有するすべての者をいう。

４ 電磁化情報とは、情報システムによって処理可能な状態にある情報をいう。

５ 非電磁化情報とは電磁化情報以外の情報をいう。

６ 情報管理責任者とは、情報内容の変更、開示等に関する意思決定権および情報管理権限を有する者のことをいい、情報作成者所属グループレベル以上の部門責任者がこの職責に任せられるものとする。

７ 機密とは、第 13 条の規定により機密区分が「極秘」、「厳秘」、「社外秘」に区分されたものをいう。

８ アクセスとは、情報の閲覧を含み、情報を使用すること、および情報利用手段を使用することをいう。

９ アクセス権限とは、アクセスできる権限をいう。

10 アクセス権限者とは、アクセス権限を有する者をいう。

11 情報セキュリティとは、情報を必要とするアクセス権限者のみが正しい内容の情報を正しく利用できるよう、会社保有情報を安全に保護することをいう。

12 情報セキュリティの管理とは情報セキュリティを維持・運営・向上させるため、会社保有情報およびその環境を管理することをいう。

第２章 情報セキュリティ保全の基本的責務

（情報セキュリティ関連義務）

第４条 すべての取締役および社員は、会社保有情報のセキュリティを保全しこれに対する注意義務を負う。

２ すべての取締役および社員は、業務遂行するお客様現場の情報のセキュリティ規定を守らなければいけない。

（情報の不正入手の禁止）

第５条 すべての取締役および社員は、他者に帰属する情報を非合法にまたは社会的批判を招く手段により入手してはならない。また提供を相手方に強要したり、相手方の申し出を受諾したりしてはならない。

２ すべての取締役および社員は、会社保有情報の使用目的が限定されているかどうかを確認する義務を負い、使用目的が限定されている場合は、その目的以外に使用してはならない。

３ すべての取締役および社員は、会社保有情報を許可なく社外に持ち出したり他者に開示したりしてはならない。

４ すべての取締役および社員は、情報取扱に関するすべての法令を遵守しなければならない。なお、本規程よりも厳しい法令はこの規程に優先して従わねばならないものとする。

（業務委託先への業務依頼）

第７条 職務遂行上必要な場合に限り、社外の業務委託先の事前審査の合格を条件に指定し、会社保有情報にかかる業務の一部または全部を委託することができる。ただし、この場合、委託する業務内容は、職務遂行上必要な範囲に厳しく限定するとともに、業務委託先におけるその守秘義務、本「情報セキュリティ管理規定」遵守義務および複製物の取扱い方法を含む、会社保有情報の情報セキュリティを規定した秘密保持契約書を、業務委託先と締結し、これを履行させなければならない。

２ 業務委託先に会社業務を委託した場合、当該業務終了後の会社保有情報およびその複製物の返却・廃棄等の処理結果を文書等により確認しなければならない。

第３章 情報セキュリティの管理体制

（会社の情報セキュリティ統括）

第８条 情報セキュリティ管理を委嘱し、委嘱された取締役（情報セキュリティ管理担当取締役という。）は、会社の情報セキュリティ管理を統括するとともに、その責任を負う。

２ 社長は情報セキュリティの総括責任者として、情報セキュリティ管理担当取締役を兼任する。

（情報セキュリティ管理の徹底）

第９条 情報セキュリティ管理の推進のため、情報セキュリティ管理担当取締役の下、情報セキュリティ管理委員会を置く。

２ 情報セキュリティ管理委員会は、情報セキュリティ管理担当取締役を補佐する。

３ 情報セキュリティ管理委員会は、会社各部門および事業場の情報セキュリティ管理状態を監査し、適切な助言や勧告を行うとともに、情報セキュリティ管理担当取締役に報告する。

（情報セキュリティの管理責任）

第 10 条 部門長は、情報セキュリティ管理総括責任者として、担当する部門における情報セキュリティの管理を総括するとともに、その責任を負う。

（プロジェクト等の情報セキュリティ管理）

第 11 条 複数の部門がプロジェクト等を編成して職務を遂行する場合、そのリーダーは当該プロジェクトに関する情報の情報管理責任者となるとともに、情報セキュリティ管理全般の責任を負い、必要な措置を講じなければならない。

２　お客様現場でのプロジェクトには、会社が指名したチームリーダーは当該プロジェクトに関する情報の情報管理責任者となるとともに、情報セキュリティ管理の責任を負う。

第４章 機密情報の管理

（機密情報）

第 12 条 会社保有情報の中で、許可した者以外に開示したり、目的外に利用された場合、経営資源としての価値を損なう恐れのある情報を機密情報とする。

２ 取引先情報を預かっている場合、取引先が機密情報と指定し、かつ、当社が同意した情報は機密情報として取り扱う。

（機密区分の設定）

第 13 条 会社保有情報は、機密の程度に応じ、「極秘」、「厳密」、「社外密」に区分（以下「機密区分」という。）される。

ただし情報セキュリティ管理総括責任者は、情報セキュリティ管理担当取締役の承認を得た上で、各部門ごとの機密区分を細分化することができる。

（情報管理責任者の役割）

第 14 条 情報セキュリティ管理総括責任者は、情報管理責任者の助言の下、次の各号の事項を実施する。

（１） 機密区分の決定と表示

（２） 機密区分に応じたアクセス権限者と許諾する権限範囲の決定

（３） 他社（者）開示に関する書面による許可

（４） 機密保持契約に基づく会社保有情報である旨の表示

（５） 機密区分に応じた廃棄処理およびその確認

（６） 機密区分に応じた情報の保全

（７） 使用目的を限定する必要がある場合の使用目的の設定

（８） 必要に応じた第１号および第３号に関する有効期限の設定

（９） その他関連事項

（機密情報の保管）

第 15 条 機密情報（秘密情報を記録したＵＳＢメモリやハードディスク等の媒体を含む）は、施錠できる保管庫に保管しなければならない。

２ 機密情報の保管場所は、所在を表示してはならない。

３ 全ての秘密情報（文書・記録媒体等）について、保管場所または作業場所からの持出し、自宅への持ち帰り、電子メール等による送信、郵便より発送、手渡し、宅急便等による配達、オンラインクラウド等への格納することにより持出すことは一切禁止する。

（機密情報の処分）

第 16 条 機密の情報資産を廃棄する場合は、シュレッダーで細断し処分を行う。

２ シュレッダーによる裁断処分が不可能な記録媒体は、焼却、溶解、破壊等その他適適切な方法により処分する。

３ 秘密情報を保管していたコンピュータ・サーバ等のコンピュータ機器類を廃棄する場合、または他者に譲渡等する場合には、内蔵されている記憶装置（例えば、ハードディスク）内に残っている情報が誤って他者に開示されることのないよう、電磁的記録の消去を実施する。

４ 秘密情報を保管していたコンピュータ・サーバ等のコンピュータ機器類を修理する場

合、修理に出す業者を予め選定し、以下の項目を含む秘密保持契約を結んでから、修理を依頼する。

・修理にあたり知りえた情報を第三者に漏洩しないこと

・修理に必要な範囲でのみ情報の複写を行い、修理完了後複写した情報は再読できないように消去すること

（アクセス権限の付与）

第 17 条 情報管理責任者は、アクセス権限を職務遂行上必要な者のみに対し付与し、職務遂行上必要な範囲に限定しなければならない。

２ 情報管理責任者は、アクセス権限付与の要請を受けた場合、前項に基づいて厳正に判断しなければならない。

（会社保有情報へのアクセス）

第 18 条 会社保有情報へのアクセスは、アクセス権限者のみ行うことができる。

２ 会社保有情報へのアクセスは、第 14 条に基づき情報管理責任者が指定した条件のもとに行わなければならない。

３ 秘密情報を記録した媒体（ＵＳＢメモリ、ハードディスク等）はアクセス権者以外の者がアクセスできないようにパスワードによるアクセス制限をかけなければならない。

４ 秘密情報を管理しているサーバや端末パーソナルコンピュータについては、アクセス権者以外の者がアクセスできないようにパスワードによるアクセス制限をかけなければならない。また、パスワードがアクセス権者以外に開示してはいけない。

５ 秘密情報を取り扱うサーバ・ネットワーク機器には windows10 と office 以外のソフトウェアをインストールしない（ウィルス定義ファイルは windows のものを使用する）。

Winny、WinMX、KazaA、Skype、Share 等の P2P ファイル交換ソフト、SoftEther 等の仮想 VPN 構築ソフト、及び VNC（*）等の遠隔操作ソフトウェアをインストールしていけない。

（*）VNC：VNC、WinVNC、RealVNC、UltraVNC、TightVNC、MultiVNC、MetaVNC、TridiaVNC、ChormiVNC、及び記載以外の VNC ソフトも対象に含む。

ウィルス対策について、いつも windows10 のウィルス定義ファイルを最新版に更新し、Microsoft Defender でウィルスを対策する。

OS 脆弱性対策について、Windows Update を自動化し、OS やソフトウェアを常に最新の状態に保つこと。

６ 秘密情報取扱者が異動等により除外された場合、パスワードを変更し、秘密情報を格納したフォルダへのアクセス権を削除する。また、秘密情報取扱い作業場所や保管場所への立入り不可するようにしなければいけない。

（アクセスの記録）

第 19 条 「極秘」に該当する会社保有情報へのアクセスは、記録ログを一定期間残すものとし、有事の際には適時、適切かつ有効に利用される様、常に情報管理委員会により管理されなければならない。

（会社保有情報内容の改変）

第 20 条 会社保有情報内容の改変は、情報管理責任者、および情報管理責任者の許諾を得たか、または権限の委譲を受けた者のみ行うことができる。

（他社（者）所有の情報へのアクセス等の管理）

第 21 条 他社（者）から開示を受けた情報へのアクセス等の管理は、所有権が会社にないことに鑑み、本規程を遵守することに加え、開示にかかる契約書、誓約書等がある場合には、それらに基づき、厳重に行わなければならない。

（立入禁止区域）

第 22 条 情報セキュリティ管理総括責任者は、所轄部門において、アクセス権限者以外の者の立入禁止区域を指定することができる。

２ 立入禁止区域においては、情報セキュリティ管理総括責任者は、アクセス権限者である旨の表示およびアクセスの記録等により管理を徹底しなければならない。

３ 会社保有情報へのアクセスが情報通信ネットワーク、情報システム等によって提供される場合は、所轄の情報セキュリティ管理総括責任者は、アクセス権限者以外の者のアクセス禁止領域を指定することができる。

（会社保有情報の他社（者）への開示等）

第 23 条 会社保有情報の他社（者）への開示は、機密区分に応じて情報管理責任者の許可がなければ行ってはならない。

２ 機密情報の他社（者）への開示に関し、前項許可に加え、その所轄担当取締役、部門長は自らの許可を必要とする情報を指定することができる。

３ 機密情報の特定他社（者）への開示にあたっては、機密保持契約を締結しなければならない。なお、その実行については第 22 条を準用する。

４ 取締役および社員は、退任または雇用の関係がなくなった後も、在職中に知り得た機密情報を他に開示したり不正に使用したりしてはならない。

（電子メールの利用）

第 24 条 取締役および社員は、業務で電子メールを利用する際には、誤送信防止、メールアドレス漏えい防止する対応策を定めなければならない。

２ 社外秘又は極秘の情報資産を送信する場合は、メール本文ではなく添付ファイルに記載し、ファイルを暗号化して送信する。添付ファイル暗号化の方法は、パスワード保護の設定又はパスワード付きの ZIP ファイルにする。パスワードは先方とあらかじめ決めておくか電話で知らせるなど、パスワードが傍受されないよう配慮する。

３ 漏洩の恐れのある Web メールやフリーメールアドレス、個人契約のプロバイダアドレスへのメール送信を禁止する。

４ インターネット上のサービス（ストレージ）の利用を禁止する。

（業務 PC の利用）

第 25 条 秘密情報の取扱い有無にかかわらず、会社支給以外のパソコン等情報機器（個人所有や個人の家族所有を含むパソコン等情報機器、インターネットカフェ等に設置されているパソコン等情報機器）を、業務に利用してはいけない。

２ お客様先で作業する場合、お客様指定以外のパソコン等情報機器を、業務に利用してはいけない。

３ パソコン等情報機器をインターネットへ接続して利用する場合は、以下に定める対策を実施し、外部からの攻撃を防御してはいけない。

・パーソナルファイアウォール導入する。

・モバイル環境からの接続は認禁止する（該当ディバイスを無効化にする）

・ファイル共用機能を停止する

・不要なアカウントの削除、及び有効なアカウントにパスワードを設定する。
パスワードは他人に推測できないように設定し、3 ヶ月 1 回に変更する。

（緊急事態の想定と対応計画）

第 26 条 情報セキュリティに関しては、緊急事態を想定した対応策を定めなければならない。

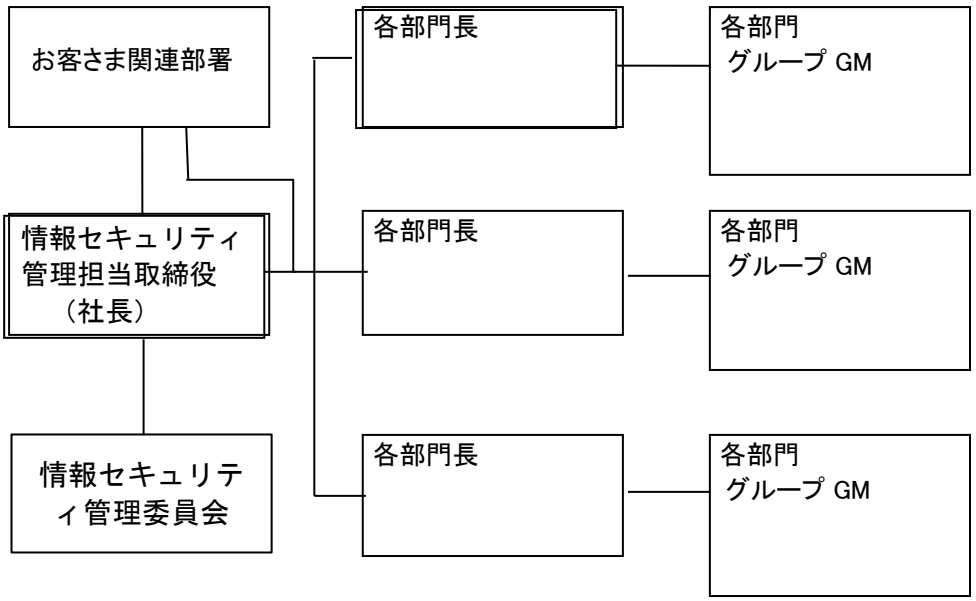
２ 情報セキュリティに関する緊急事態の発生に備え、複数の連絡手段による連絡網を整備するとともに、定期的に訓練を実施しなければならない。

（緊急事態発生時の対応）

第 27 条 情報セキュリティに関する緊急事態が発生した場合は、情報セキュリティ管理担当取締役の指揮のもとに対応する。

２ 緊急事態の発生時には、あらかじめ定めた連絡網により関連部門へ緊急連絡するとともに、協力して解決にあたるもととする。

＜情報セキュリティ緊急対応体制図＞



３ 情報セキュリティに関する緊急事態が発生し、解決したら、必ず原因を究明して、同の事故が再発しように防止策を策定し、直ちに実施しなければならない。

４ 情報セキュリティ事故の対応と関係する情報は、守秘義務の対象であるため、漏えいしていけない。

５ 業務委託時、委託先で情報漏えい事故が発生した場合でも、上記第２号、及び第３号、第４号に従って迅速に対応しなければいけない。

（情報セキュリティ教育）

第 28 条 会社保有情報管理の一環として、全社員に対し情報セキュリティ管理の必要性・重要性への意識を高めるべく啓発し、具体的管理を現場で実践させるために情報セキュリティ管理総括責任者は必要な社員教育を計画し、実行しなければならない。

２ 情報セキュリティ管理総括責任者は、社員に対して、入社時に情報セキュリティに関する誓約内容を中心とした教育を実施する。管理職への昇格時には、情報セキュリティ管理者レベルの情報セキュリティ教育を実施する。異動者、増員時に担当する職種ごとに、専門分野に必要とされる情報セキュリティ教育を定期（１回/年）的に実施する。

３ 情報セキュリティ管理総括責任者は、関連する社外協力業者に対しても必要に応じて前項の施策を講じるものとする。

第５章 情報セキュリティ管理の監査

（情報セキュリティ管理の監査）

第 29 条 情報セキュリティ管理総括責任者は、所轄部門における情報セキュリティ管理実態の精査を行い、その結果を情報セキュリティ管理担当取締役に報告するものとする。

（機密保持契約等にかかる立入検査等）

第 30 条 会社が機密保持契約を締結し、会社保有情報を契約相手方に開示する場合においては、相手方において適切に保全・管理されていることを実地に監査・検査するため、会社は立入検査権を契約文言に規定し、かかる権利を確保しなければならない。

２ 情報セキュリティ管理総括責任者は、前項により必要に応じ立入検査を実施し、結果を部門長に報告する。

３ 第１項記載の同様文言に基づき検査権相手方が有する場合で、相手が立入検査を求めた場合、該当する部門責任者は、関係部門と連携を取り、誠意をもってその検査に応じなければならない。

第６章 罰則

（懲戒）

第 31 条 社員が故意または重大な過失により、この規程に違反し、「社員就業規則」に定める各種懲戒に該当する場合は、同規則により措置される。

２ 取締役については、会社法等に照らして処遇が決定される。