○○株式会社
情報セキュリティ基本規程

制 定 日	○年○月○日
施 行 日	○年○月○日
改 訂 日	○年○月○日
決裁機関	○○○○
分　　類	○○○○
版	第○版

第１章　総則

第１条（目的）

この規程は、○○株式会社（以下「会社」という。）が保有する情報資産を、漏えい、改ざん、破壊、不正利用その他の脅威から保護するため、情報セキュリティに関する基本方針、管理体制及び安全管理措置の基本的事項を定め、もって会社の事業の継続と社会的信用の維持を図ることを目的とする。

第２条（定義）

この規程において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

(1) 情報資産　会社が業務上取得し、作成し、又は保有する情報（個人情報、営業秘密、技術情報、経理情報、取引先情報その他一切の情報をいう。）並びに当該情報を記録し、処理し、又は伝送する情報システム、機器、記憶媒体、書類及び設備をいう。

(2) 情報セキュリティ　情報資産の機密性（許可された者だけが情報にアクセスできること）、完全性（情報が正確かつ完全であること）及び可用性（許可された者が必要なときに情報を利用できること）を維持することをいう。

(3) 情報システム　サーバー、ネットワーク機器、パソコン、モバイル端末、ソフトウェア及びクラウドサービスその他の情報処理に用いる機器及びサービスの総体をいう。

(4) 情報セキュリティインシデント　情報資産の漏えい、滅失、毀損、改ざん、不正アクセス、マルウェア感染、サービスの停止その他情報セキュリティを脅かし、又は脅かすおそれのある事象をいう。

(5) 委託先　会社から情報資産の取扱いを伴う業務を受託し、又は会社の情報システムの運用、保守若しくは開発を受託する者（再委託先を含む。）をいう。

(6) 利用者　会社の情報資産を業務上取り扱う全ての者をいう。

第３条（適用範囲）

1　この規程は、会社の役員及び従業員（正社員、契約社員、パートタイマー、嘱託社員その他雇用形態を問わず会社に雇用される者をいう。以下同じ。）に適用する。

2　会社の指揮命令の下で業務に従事する派遣労働者及び会社の施設内で業務に従事する委託先の従業者については、派遣契約又は業務委託契約に定めるところにより、この規程を準用する。

3　この規程は、会社が保有する全ての情報資産に適用し、その保有の形態（電子データ、書類、口頭による伝達等）及び保管の場所（会社の施設内外、クラウドサービス上等）を問わない。

第４条（基本方針）

会社は、情報セキュリティに関する基本方針として、次の各号に掲げる事項を宣言し、

役員及び従業員はこれを遵守しなければならない。

(1) 情報セキュリティに関する法令、国が定める指針及び契約上の義務を遵守すること。

(2) 情報資産を重要度に応じて分類し、分類に応じた安全管理措置を講じること。

(3) 情報セキュリティの管理体制を整備し、責任及び権限を明確にすること。

(4) 情報資産に対するリスクを定期的に評価し、リスクに応じた対策を講じること。

(5) 役員及び従業員に対し情報セキュリティに関する教育を継続的に実施すること。

(6) 情報セキュリティインシデントの発生に備え、迅速に対応する体制を整備すること。

(7) 情報セキュリティの取組みを定期的に監査し、継続的に改善すること。

第 5 条（関連規程との関係）

1　情報セキュリティに関する個別の事項については、この規程に定めるもののほか、次の各号に掲げる規程及びこれらに基づく細則の定めるところによる。

(1) 情報システムの管理に関する事項　情報システム管理規程

(2) パソコン及びモバイル端末の利用に関する事項　パソコン・モバイル端末利用規程

(3) 個人情報の取扱いに関する事項　個人情報取扱規程及び特定個人情報（マイナンバー）等取扱規程

(4) 営業秘密の管理に関する事項　営業秘密等管理規程

(5) 文書の管理に関する事項　文書管理規程

(6) ソーシャルメディアの利用に関する事項　ソーシャルメディア利用規程

(7) 生成 AI の利用に関する事項　生成 AI 利用規程

(8) 施設への入退室及び鍵の管理に関する事項　入退室・鍵管理規程

(9) テレワークにおける情報セキュリティに関する事項　テレワーク勤務規程及びテレワークにおけるセキュリティガイドライン

2　前項各号の規程の定めがこの規程と抵触するときは、この規程の定めが優先する。

第 2 章　情報資産の分類

第 6 条（情報資産の分類）

1　会社は、情報資産を、その漏えい、改ざん又は利用不能が会社、顧客、取引先及び従業員に与える影響の大きさに応じて、次の各号に掲げる区分に分類する。

(1) 極秘　漏えいした場合に会社の存続に関わる重大な損害を与えるおそれのある情報（未公表の経営計画、M&A に関する情報、重要な技術情報等）

(2) 秘　漏えいした場合に会社、顧客、取引先又は従業員に重大な損害を与えるおそれのある情報（個人データ、特定個人情報、営業秘密、顧客との契約情報、人事情報等）

(3) 社外秘　社外への公開を予定しない情報であって、前 2 号に該当しないもの（社内規程、会議資料、業務マニュアル等）

(4) 公開　会社が社外に公開し、又は公開を予定している情報（ウェブサイト掲載情報、公表済みの資料等）

2　情報資産の分類は、当該情報資産を作成し、又は取得した部門の部門情報セキュリティ管理者が、情報セキュリティ責任者の定める基準に従って決定する。

3　個人情報及び営業秘密に該当する情報資産の分類は、個人情報取扱規程及び営業秘密等管理規程に定める区分と整合するように定めなければならない。

第 7 条（分類に応じた取扱い）

1　利用者は、情報資産を、その分類に応じ、次の表に定める基準に従って取り扱わなければならない。

区分	表示	アクセス権限	社外持出し	社外送信	保管	廃棄
極秘	必ず表示	指名された者に限る	情報セキュリティ責任者の承認	原則禁止（暗号化及び責任者の承認を要する）	施錠保管又は暗号化	裁断、溶解又は消去証明
秘	必ず表示	業務上必要な者に限る	部門情報セキュリティ管理者の承認	暗号化	施錠保管又はアクセス制御	裁断、溶解又は復元不能な消去
社外秘	原則表示	従業員	所属長の承認	送信先の確認	施錠又はアクセス制御	裁断又は消去
公開	不要	制限なし	制限なし	制限なし	改ざん防止	通常廃棄

2　情報資産の分類は、その情報資産の重要性の変化に応じて見直すものとし、公表、契約の終了その他の事由により重要性が低下したときは、部門情報セキュリティ管理者が分類を変更することができる。

第 8 条（情報資産台帳）

1　部門情報セキュリティ管理者は、所管する情報資産のうち極秘及び秘に分類されるものについて、情報資産の名称、分類、保管場所、保管媒体、管理責任者、アクセス権を有する者及び保存期間を記載した情報資産台帳を作成し、少なくとも年 1 回その内容を確認して、最新の状態に維持しなければならない。

2　情報資産台帳の様式は、情報セキュリティ責任者が定める。

第 3 章　管理体制

第 9 条（情報セキュリティ責任者）

1　会社は、情報セキュリティに関する最高責任者として、取締役の中から情報セキュリティ責任者を 1 名選任する。
2　情報セキュリティ責任者は、次の各号に掲げる職務を行う。
(1) 情報セキュリティに関する方針、規程及び細則の制定及び改廃に関すること。
(2) 情報セキュリティ委員会の招集及び運営に関すること。
(3) リスクアセスメントの実施及びリスク対応計画の承認に関すること。
(4) 情報セキュリティインシデントの対応の指揮に関すること。
(5) 情報セキュリティに関する教育計画の承認に関すること。
(6) 情報セキュリティ監査の結果に基づく改善の指示に関すること。
(7) その他情報セキュリティの確保に関し必要な事項
3　情報セキュリティ責任者は、個人情報取扱規程に定める個人情報保護管理者及び営業秘密等管理規程に定める営業秘密等管理者を兼ねることができる。

第 10 条（情報セキュリティ委員会）
1　会社は、情報セキュリティに関する事項を審議するため、情報セキュリティ委員会（以下「委員会」という。）を設置する。
2　委員会は、情報セキュリティ責任者を委員長とし、情報システム管理者、各部門の部門情報セキュリティ管理者及び情報セキュリティ責任者が指名する者をもって構成する。
3　委員会は、次の各号に掲げる事項を審議する。
(1) 情報セキュリティに関する規程及び細則の制定及び改廃に関する事項
(2) リスクアセスメントの結果及びリスク対応計画に関する事項
(3) 情報セキュリティインシデントの原因分析及び再発防止策に関する事項
(4) 情報セキュリティに関する教育計画に関する事項
(5) 情報セキュリティ監査の結果及び改善計画に関する事項
(6) その他情報セキュリティ責任者が必要と認める事項
4　委員会は、年〇回定期に開催するほか、情報セキュリティ責任者が必要と認めるときに臨時に開催する。
5　委員会の事務局は、〇〇部に置く。
〈別例：従業員数が少なく委員会を常設しない場合は、本条を「会社は、情報セキュリティに関する事項を審議するため、必要に応じて情報セキュリティ責任者、情報システム管理者及び関係部門の長による会議を開催する。」と定めることができる。〉

第 11 条（部門情報セキュリティ管理者）
　各部門の長は、当該部門における部門情報セキュリティ管理者として、次の各号に掲げる職務を行う。
(1) 所管する情報資産の分類及び情報資産台帳の作成に関すること。
(2) 所属する従業員に対するこの規程の周知及び遵守状況の確認に関すること。
(3) 所管する情報資産に関する情報セキュリティインシデントの一次対応及び情報セキ

ュリティ責任者への報告に関すること。
(4) 所属する従業員の入社、異動及び退職に伴うアクセス権限の付与及び削除の申請に関すること。

第 12 条（情報システム管理者）
1　会社は、情報システムの運用及び技術的安全管理措置を所管する者として、情報システム管理者を置く。
2　情報システム管理者の職務は、情報システム管理規程に定めるところによる。

第 13 条（利用者の責務）
1　利用者は、この規程及び関連規程を遵守し、情報資産を業務上必要な範囲内でのみ利用しなければならない。
2　利用者は、業務上知り得た情報資産の内容を、在職中及び退職後を問わず、正当な理由なく第三者に開示し、漏えいし、又は業務以外の目的に利用してはならない。
3　利用者は、情報セキュリティインシデント又はそのおそれを認知したときは、直ちに所属する部門の部門情報セキュリティ管理者に報告しなければならない。

第 4 章　リスクアセスメント

第 14 条（リスクアセスメントの実施）
1　情報セキュリティ責任者は、少なくとも年 1 回、及び情報システムの大幅な変更、新たな事業の開始、重大な情報セキュリティインシデントの発生その他の必要が生じたときに、情報資産に対するリスクアセスメントを実施しなければならない。
2　リスクアセスメントは、次の各号に掲げる手順により行う。
(1) 情報資産台帳に基づき、評価の対象とする情報資産を特定すること。
(2) 情報資産ごとに、想定される脅威（不正アクセス、マルウェア、内部不正、誤操作、紛失、盗難、災害、委託先の事故等）及び脆弱性を洗い出すこと。
(3) 脅威が顕在化した場合の影響の大きさ及び発生の可能性を評価し、リスクの大きさを決定すること。
(4) リスクの大きさに応じて、リスクへの対応の優先順位を決定すること。

第 15 条（リスク対応）
1　情報セキュリティ責任者は、リスクアセスメントの結果に基づき、リスクごとに、リスクの低減、回避、移転又は受容のいずれかの対応方針を決定し、対応の内容、担当者及び期限を定めたリスク対応計画を作成して、委員会の審議を経なければならない。
2　リスクを受容する場合は、その理由及び受容するリスクの内容を記録しなければならない。
3　情報セキュリティ責任者は、リスク対応計画の実施状況を確認し、委員会に報告しなけ

ればならない。

第 5 章　安全管理措置

第 16 条（組織的安全管理措置）

会社は、組織的安全管理措置として、次の各号に掲げる措置を講じる。

(1) 第 3 章に定める管理体制を整備し、責任及び権限を明確にすること。

(2) 情報資産の取扱いに関する規程及び細則を整備し、当該規程に従った運用を行うこと。

(3) 情報資産の取扱状況を確認するための記録(アクセスログ､持出し記録､廃棄記録等)を整備すること。

(4) 情報セキュリティインシデントに対応する体制及び報告連絡経路を整備すること。

(5) 情報セキュリティの取扱状況を把握し、安全管理措置を定期的に見直すこと。

第 17 条（人的安全管理措置）

1　会社は、人的安全管理措置として、次の各号に掲げる措置を講じる。

(1) 従業員の採用に当たり、秘密保持及びこの規程の遵守に関する誓約書を提出させること。

(2) 従業員に対し、第 24 条に定める教育を実施すること。

(3) 従業員の退職に当たり､情報資産の返却､アクセス権限の削除及び退職後の秘密保持に関する誓約書の提出を確実に行わせること。

(4) 情報資産の取扱いに関する秘密保持義務及び違反時の懲戒に関する事項を就業規則に定めること。

2　会社は､従業員が業務上取り扱う情報資産の重要度に応じて､その者に必要な監督を行わなければならない。

第 18 条（物理的安全管理措置）

会社は、物理的安全管理措置として、次の各号に掲げる措置を講じる。

(1) サーバー等の重要な情報システムを設置する区域及び極秘又は秘の情報資産を取り扱う区域を定め、入退室・鍵管理規程に基づき入退室を管理すること。

(2) 情報資産を記録した機器､記憶媒体及び書類を施錠された保管庫等に保管し､盗難及び紛失を防止すること。

(3) 情報資産を社外に持ち出す場合の手続及び漏えい防止策を定めること。

(4) 情報資産を記録した機器及び記憶媒体を廃棄する場合は、復元できない方法により行い、廃棄の記録を残すこと。

(5) 離席時には机上の書類を片付け､画面をロックすること（クリアデスク及びクリアスクリーン）を徹底すること。

第 19 条（技術的安全管理措置）

1　会社は、技術的安全管理措置として、次の各号に掲げる措置を講じる。

(1) 利用者ごとにアカウントを発行し、識別及び認証を行うとともに、業務上必要な範囲にアクセス権限を限定すること。

(2) ファイアウォール、マルウェア対策ソフトウェアその他の不正アクセス及び不正ソフトウェアから情報システムを保護する仕組みを導入し、常に最新の状態に維持すること。

(3) オペレーティングシステム及びソフトウェアの脆弱性に対する修正プログラムを速やかに適用すること。

(4) 極秘及び秘の情報資産を社外に送信し、又は社外に持ち出す場合は、暗号化その他の漏えい防止措置を講じること。

(5) 情報システムの利用状況及びアクセスの記録を取得し、保存し、定期的に確認すること。

(6) 重要なデータのバックアップを定期的に取得し、復元できることを確認すること。

2　技術的安全管理措置の具体的内容は、情報システム管理規程及びパソコン・モバイル端末利用規程に定める。

第 6 章　インシデント対応

第 20 条（報告）

1　利用者は、情報セキュリティインシデント又はそのおそれを認知したときは、自ら判断して対処することなく、直ちに所属する部門の部門情報セキュリティ管理者及び情報システム管理者に報告しなければならない。

2　部門情報セキュリティ管理者は、前項の報告を受けたときは、直ちに情報セキュリティ責任者に報告しなければならない。

3　利用者は、自らの過失により情報セキュリティインシデントを生じさせた場合であっても、速やかに報告しなければならない。会社は、速やかな報告を行った者に対し、報告したことを理由として不利益な取扱いをしない。

第 21 条（初動対応）

1　情報セキュリティ責任者は、情報セキュリティインシデントの報告を受けたときは、被害の拡大を防止するため、関係者に対し、次の各号に掲げる措置のうち必要なものを直ちに指示しなければならない。

(1) 影響を受けた機器のネットワークからの切断及び電源を切らない状態での保全

(2) 漏えいしたおそれのあるアカウントのパスワードの変更及びアカウントの停止

(3) 影響を受けた情報資産の範囲及び本人の数の特定

(4) 証拠となるログ及び記録の保全

(5) その他被害の拡大を防止するために必要な措置

2　情報セキュリティ責任者は、情報セキュリティインシデントの影響が重大であると認めるときは、代表取締役に報告し、その指示の下に対策本部を設置する。

第 22 条（外部への報告及び公表）

1　会社は、情報セキュリティインシデントが個人データの漏えい等に該当するときは、個人情報取扱規程の定めるところにより、個人情報保護委員会への報告及び本人への通知を行う。

2　会社は、情報セキュリティインシデントが顧客又は取引先の情報資産に影響を及ぼすときは、契約に定めるところにより、速やかに当該顧客又は取引先に報告する。

3　会社は、不正アクセス、ランサムウェアによる被害その他の犯罪行為によると認められる情報セキュリティインシデントについては、警察及び関係機関に届け出るとともに、必要に応じて事実関係及び再発防止策を公表する。

第 23 条（記録及び再発防止）

1　情報セキュリティ責任者は、情報セキュリティインシデントについて、発生の日時、内容、原因、影響の範囲、対応の経過及び再発防止策を記録し、委員会に報告しなければならない。

2　委員会は、前項の報告に基づき原因を分析し、再発防止策を決定するとともに、必要に応じてこの規程及び関連規程の見直しを行う。

3　情報セキュリティインシデントの記録は、〇年間保存する。

第 7 章　教育、委託先管理、監査及び見直し

第 24 条（教育）

1　会社は、役員及び従業員に対し、情報セキュリティに関する教育を次の各号に掲げる区分により実施する。

(1) 入社時教育　入社後〇か月以内に、この規程及び関連規程の内容並びに情報資産の基本的な取扱いについて実施する。

(2) 定期教育　年 1 回以上、情報セキュリティに関する脅威の動向、社内規程の改定内容及び情報セキュリティインシデントの事例について実施する。

(3) 臨時教育　重大な情報セキュリティインシデントの発生、法令の改正又は情報システムの大幅な変更があったときに実施する。

(4) 特定業務教育　情報システム管理者その他情報システムの運用に携わる者に対し、その職務に必要な専門的な教育を実施する。

2　会社は、標的型攻撃メールへの対応訓練その他の実践的な訓練を、年 1 回以上実施するよう努める。

3　従業員は、前 2 項の教育及び訓練を受講しなければならない。やむを得ない事由により受講できなかった者は、別途指定する方法により補習を受けなければならない。

4　情報セキュリティ責任者は、教育及び訓練の実施状況及び受講者を記録し、〇年間保存する。

第 25 条（委託先管理）

1　会社は、情報資産の取扱いを伴う業務を委託する場合は、委託先の情報セキュリティの水準が会社の求める水準を満たすことを、委託先の選定に当たり確認しなければならない。

2　会社は、委託先との契約において、次の各号に掲げる事項を定めなければならない。

(1) 委託先が講じるべき安全管理措置の内容

(2) 秘密保持義務及び目的外利用の禁止

(3) 再委託の制限及び再委託する場合の事前承認手続

(4) 情報セキュリティインシデントが発生した場合の報告義務及び対応

(5) 委託業務の遂行状況について会社が報告を求め、又は監査を行うことができること。

(6) 契約終了時における情報資産の返却又は消去及びその証明

(7) 契約に違反した場合の措置及び損害賠償

3　情報セキュリティ責任者は、極秘又は秘の情報資産の取扱いを委託する委託先について、年 1 回以上、安全管理措置の実施状況を書面又は実地により確認しなければならない。

4　個人データの取扱いを委託する場合の委託先の監督については、前 3 項によるほか、個人情報取扱規程の定めるところによる。

第 26 条（監査）

1　情報セキュリティ責任者は、この規程及び関連規程の遵守状況並びに安全管理措置の有効性について、年 1 回以上、内部監査を実施しなければならない。

2　内部監査は、監査の対象となる部門から独立した者が行うものとし、情報セキュリティ責任者は、必要に応じて外部の専門機関に監査を委託することができる。

3　監査を行う者は、監査の結果を情報セキュリティ責任者及び委員会に報告し、情報セキュリティ責任者は、指摘された事項について改善計画を作成し、改善を指示しなければならない。

第 27 条（見直し）

情報セキュリティ責任者は、リスクアセスメントの結果、情報セキュリティインシデントの発生状況、監査の結果、法令及び指針の改正並びに情報技術の動向を踏まえ、年 1 回以上、この規程及び関連規程並びに安全管理措置を見直し、必要な改定を委員会に諮らなければならない。

第 28 条（違反時の措置）

1　従業員がこの規程に違反したときは、就業規則第〇条の懲戒の規定を適用し、役員がこ

の規程に違反したときは、取締役会において必要な措置を決定する。

2　役員及び従業員がこの規程に違反して会社に損害を与えたときは、会社は、懲戒処分とは別に、当該損害の賠償を請求することができる。

3　派遣労働者又は委託先の従業者がこの規程に違反したときは、会社は、派遣元又は委託先に対し、当該違反の事実を通告し、必要な措置を求める。

第 29 条（細則への委任）

この規程の実施に関し必要な事項は、情報セキュリティ責任者が、委員会の審議を経て細則として定める。

第 30 条（規程の改廃）

この規程の改廃は、情報セキュリティ責任者が委員会の審議を経て起案し、取締役会の決議により行う。

（附則）

1　この規程は、〇年〇月〇日から施行する。

2　この規程は、〇年〇月〇日から改定施行する。

（改定条文：第〇条、第〇条、第〇条）

規程改訂履歴

制定年月日	版	名　　称	起案者	決裁者	行政庁提出 年月日
年　月　日					年　月　日

改訂履歴

改訂年月日	版	改訂箇所・内容・理由等	起案者	決裁者	行政庁提出 年月日
年　月　日					年　月　日
年　月　日					年　月　日
年　月　日					年　月　日
年　月　日					年　月　日
年　月　日					年　月　日
年　月　日					年　月　日
年　月　日					年　月　日
年　月　日					年　月　日
年　月　日					年　月　日
年　月　日					年　月　日
年　月　日					年　月　日
年　月　日					年　月　日
年　月　日					年　月　日
年　月　日					年　月　日
年　月　日					年　月　日
年　月　日					年　月　日
年　月　日					年　月　日
年　月　日					年　月　日