

日進木工株式会社 情報セキュリティ規程

第1条（目的）

本規程は、日進木工株式会社（以下「当社」という。）が保有または管理する情報資産を適切に保護し、情報漏えい、改ざん、滅失、紛失、不正アクセス、サイバー攻撃、業務停止その他のリスクを防止することにより、当社の事業継続、信用維持および取引先・顧客等の権利利益の保護を図ることを目的とする。

第2条（適用範囲）

本規程は、当社の役員、従業員、契約社員、パートタイマー、アルバイト、派遣社員その他当社の業務に従事するすべての者（以下「従業員等」という。）に適用する。
また、業務委託先その他第三者に当社情報資産を取り扱わせる場合は、本規程の趣旨に沿った管理を求めるものとする。

第3条（情報資産の定義）

本規程における情報資産とは、当社の事業活動に関わる有形・無形の情報およびそれを取り扱う設備等をいい、主として次のものを含む。

1. 顧客情報、取引先情報、個人情報
 2. 設計図面、製品仕様書、技術情報、ノウハウ
 3. 見積書、契約書、財務情報、人事情報、社内資料
 4. 電子データ、メール、クラウド上のデータ
 5. パソコン、スマートフォン、タブレット、サーバー、ネットワーク機器
 6. USBメモリ、外付け媒体、紙媒体その他記録媒体
-

第4条（基本原則）

当社は、情報資産について、次の観点を重視し管理する。

1. 機密性：許可された者のみが情報にアクセスできること
 2. 完全性：情報が正確かつ最新の状態に保たれること
 3. 可用性：必要なときに情報を利用できること
-

第5条（管理体制）

1. 当社は、情報セキュリティ責任者を定め、全社的な情報管理を統括させる。
2. 各部門責任者は、自部門の情報資産管理について責任を負う。
3. 情報セキュリティ責任者は、必要に応じて対策の指示、点検、教育、是正措置を行う。

第 6 条（情報資産の分類と管理）

1. 情報資産は、その重要性に応じて「機密情報」「社外秘情報」「社内情報」「公開情報」等に区分し、適切に管理する。
2. 機密情報および個人情報へのアクセスは、業務上必要な者に限定する。
3. 紙媒体の機密情報は施錠保管し、電子情報は適切なアクセス制御を行う。

第 7 条（ID・パスワード等の管理）

従業員等は、システム利用にあたり、次の事項を遵守しなければならない。

1. ID・パスワードを第三者に貸与、共有または開示しないこと
2. 推測されにくいパスワードを設定し、定期的な見直しを行うこと
3. 退席時は画面ロックを行うこと
4. 多要素認証が利用可能な場合は積極的に利用すること

第 8 条（電子メール・インターネット利用）

1. 不審なメール、添付ファイル、URL は開かないこと。
2. 業務に無関係な危険性の高いサイトへのアクセスを行わないこと。
3. 当社名義を用いた不用意な情報発信を行わないこと。
4. 誹謗中傷、違法行為、著作権侵害等につながる利用を禁止する。

第 9 条（端末・ソフトウェア管理）

1. 会社貸与端末は業務目的に限り使用する。
2. 無断でソフトウェア、アプリケーション、クラウドサービスを導入してはならない。
3. OS、ソフトウェア、ウイルス対策ソフトは最新状態を維持する。
4. 私物端末を業務利用する場合は、会社の承認を得た場合に限る。

第 10 条（情報の持出し・外部共有）

1. 顧客情報、機密情報その他重要情報を社外へ持ち出す場合は、事前に上長の承認を得るものとする。
2. 持出し時は、暗号化、パスワード保護、送付先確認等の安全措置を講じる。
3. フリーWi-Fi等、安全性の確認できない通信環境で重要情報を取り扱う際は十分注意する。

第 11 条（個人情報および機密情報の取扱い）

1. 個人情報は、法令および社内ルールに従い、利用目的の範囲内で適切に取得・利

- 用・保管する。
2. 顧客情報、取引先情報、技術情報、営業秘密等を業務目的以外に利用してはならない。
 3. 在職中はもとより、退職後も業務上知り得た秘密情報を漏らしてはならない。
-

第 12 条（バックアップ・事業継続）

1. 重要データについては、必要に応じて定期的なバックアップを実施する。
 2. 災害、事故、サイバー攻撃等の緊急時に備え、重要業務の継続および早期復旧に努める。
-

第 13 条（廃棄・返却）

1. 不要となった書類、記録媒体、機器等は、復元困難な方法により適切に廃棄する。
 2. 退職、異動、契約終了時には、貸与物・情報資産を速やかに返却し、アクセス権限を見直す。
-

第 14 条（委託先管理）

当社が外部委託先に情報資産を取り扱わせる場合は、秘密保持契約その他必要な契約を締結し、適切な管理体制を確認する。

第 15 条（インシデント対応）

1. 情報漏えい、不正アクセス、ウイルス感染、端末紛失、誤送信等の事故またはその疑いがある場合、従業員等は速やかに上長および情報セキュリティ責任者へ報告しなければならない。
 2. 情報セキュリティ責任者は、被害拡大防止、原因調査、復旧対応、再発防止策の実施を行う。
 3. 必要に応じて、関係先、行政機関、専門機関等へ適切に報告・相談する。
-

第 16 条（教育・啓発）

当社は、従業員等に対し、情報セキュリティに関する教育、注意喚起、訓練等を継続的に実施し、意識向上に努める。

第 17 条（監査・見直し）

当社は、本規程の運用状況を必要に応じて確認し、法令改正、社会情勢、技術動向、事故発生状況等を踏まえ、継続的に見直し・改善を行う。

第 18 条（違反時の措置）

従業員等が本規程に違反した場合は、就業規則その他社内規程に基づき、必要な指導、是正措置または懲戒処分の対象となることがある。

制定日：2026 年 4 月 1 日

日進木工株式会社

代表取締役社長 北村卓也