フジコー株式会社　情報セキュリティ基本ルール

制定日:2024 年 12 月 25 日
フジコー株式会社
代表取締役社長　根岸　誠

1. オフィス編

極秘情報の取り扱い

- 極秘情報は、原則持ち出しは行わない。
- 取引先と個人情報を授受する際は、「機密保持契約書（NDA)」を締結したうえで、都度書面（「授受票」等）での取り交わしを行う。
- 個人情報以外についても取引先と機密性の高い情報の授受を行う際は、必要に応じて「機密保持契約書（NDA)」を締結したうえで、都度書面（「授受票」等）での取り交わしを行う。
- 極秘情報を持ち出しもしくは送付する際は、持ち出す目的や内容を明確にしたうえ、メールやグループウェアなど記録の残る方法で所属長の承認を得る。
  - 持ち出し時：期間、資料名、持ち出し先、理由を記載した内容について、所属長から承認の返信を受ける。
  - 返却時：持ち出し時に宛てた承認の返信に対し、返却した旨を返信する。

クリアスクリーンポリシー

- パスワード付スクリーンセーバーを 5 分以内に起動する。
- 離席する場合は、パスワード付スクリーンセーバーなどを用いてスクリーンロックをかける。
- 長時間（3 時間程度）離席する場合には、PC の電源を落とす。

クリアデスクポリシー

- 机の上に機密情報の入った書類や媒体を放置せず、常に整頓し、机上から情報が漏洩しないように対策をとる。
- 極秘情報の入った書類や媒体は鍵のかかる引き出しやキャビネットに収納する。

パスワードの利用

- パスワードの強度は、以下の通り設定を行う。
  - パスワード文字数：10 文字以上
  - 類推難度：記号英大小数字混在

- 全てのデバイス、ネットワーク、システムにおいて同一のパスワードを設定することを禁止する。
- 機器を紛失した場合は、直ちに社内外のすべてのパスワードの変更を行う。

メール送受信

- メールを送信する際は、送信前に宛先と添付ファイルを再確認する。
- 不特定多数の人に同報メールを送信する際は、BCC に指定する。
- 怪しいメールの添付ファイルやリンクは開かない。
  - Office 製品のマクロ設定は無効または警告にしておく。
  - ウィルス対策ソフトを最新の状態にする。

事務・OA 機器

- コピー機、プリンター等で入出力した文書、FAX 送受信文書（不特定の者宛てを除く）を放置しない。
- FAX 送信時は印刷物の裏紙を使用せず、誤送信を防ぐために宛先を必ず確認する。

その他の留意事項

- 来訪者のワークスペースへの立ち入りは極力制限し、立ち入る場合は従業者が同伴する。
- オフィス内での機密情報に関わる会話は、必要関係者以外への漏えい及び盗聴を防止するよう配慮する。
- 外出や退社時には、ノート PC を鍵のかかる引き出しやキャビネットに収納するかセキュリティワイヤーで固定する。
- 社外へ持ち出す鞄等に入れている情報は常に把握し、不用意に機密性の高い情報が入ったままにならないよう、細心の注意を払う。

2. パソコン＆モバイルデバイス編

PC、モバイル機器、外部記憶装置の利用及び持ち出し（共通）

- 個人で購入した情報通信機器（PC、モバイル機器）・外部記憶装置を原則利用しない。
- 公共機関で移動する場合、情報通信機器・外部記憶装置を入れた鞄等は常に携帯し、網棚等目の届かない場所には置かない。また、鞄等から目を離す場合、鞄の施錠やセキュリティワイヤーにて席へ固定するなどの盗難防止対策を実施する。
- 車両等で移動する場合には、情報通信機器・外部記憶装置を入れた鞄等は必ず一緒に持ち歩く。
- 社外へ鞄等に入れて情報通信機器・外部記憶装置を持ち出す際、それらのパスワードを記録した手帳やメモは同じ鞄に入れない。

- 帰宅時に、飲酒を伴う飲食店等へ立ち寄る際は、情報通信機器・外部記憶装置の社外へ持ち出しは禁止とする。
- 社外への情報通信機器・外部記憶装置を持ち出す際は、格納している極秘情報について記録に残しておく。（例：別媒体へのコピー、リスト一覧等）

情報通信機器（PC、タブレット PC）の持ち出し

- 社外へ持ち出しする PC は、共有 PC・専有 PC にかかわらず暗号化を行う。
- PC を持ち出す際、原則極秘情報（機密性３）は入れない。
- PC を社外へ持ち出す際は、所属長へメールにて申請を行い、持ち出していることが組織に認識できる状態を維持する。
  例）グループウェア等のスケジュール表への記入等
- 持ち出した PC（共有 PC・専有 PC）での個人業務（資料の作成等）は、不特定多数の人がいる場所（公共交通機関※、展示会場、飲食店等）では行わない。
  ※飛行機や新幹線等での長距離の移動を伴う出張で、やむなく PC を使用する場合は、覗き見防止フィルターを利用する。ただし、極秘情報については閲覧、編集してはならない。
- 展示会等、不特定多数の人が集まる会場において、デモ等で PC を立ち上げておく必要のある場合は、原則共有 PC を使用する。やむを得ず専有 PC を使用する場合は、一般情報（機密性１）以外の情報は格納しない。

携帯電話・スマートフォン、iPad のルール

- パスワードによるキーロックをかける
- スマートフォン、iPad は、内臓ディスク／SD カードを暗号化する。
- 各社指定のセキュリティツール、サービスの設定を行う。
- 紛失時は、情報セキュリティ担当者に連絡し、適切な対応を行う。

外部記憶装置のルール

- 外部記憶装置は、暗号化機能付きのものに限定する。
- 所属長は最低でも月に一度、外部記憶装置の持ち出し状況、紛失の有無、保存したデータの削除状況について確認する。
- アンチウィルスソフトの適用有無に関わらず、データの受け渡しを行う際は、事前にウィルススキャンを必ず行い、安全性が確認された外部記憶装置を利用する。
- USB 等でデータを社外へ持ち出す際は、暗号化もしくはパスワードをかける。

情報通信機器・外部記憶装置の再利用及び廃業

- 使用済みの情報通信機器・外部記憶装置は、ディスクの破棄、もしくはデータの消去を行ったうえで廃棄する。

3. 情報資産の分類

情報資産は機密性により、以下のように分類する。

機密情報：業務上の機密事項または会社の不利益となる事項ならびに個人情報を含む情報

機密性	大分類	中分類	小分類	例
極秘 （機密性:3）	個人 情報	取引先	・機微情報を含む個人情報 ・私的な情報を含む個人情報	・自宅の住所録 ・人事考課表 ・クレジットカード情報
		自社	・人事考課情報 ・マイナンバー	
	個人情 報以外	取引先	・機密保持契約(NDA)を締結した顧客情報全般	
		自社	・営業秘密 ・インサイダー情報	
社外秘 （機密性:2）	個人情 報	取引先	・関係者に公開されている個人情報	・座席表 ・組織図
		自社	・社内に公開されている個人情報	
	個人情 報以外	取引先	・契約情報 ・設計情報 ・ユーザ情報	・提案書 ・見積書 ・契約書 ・仕様書 ・打合せ議事録 ・図面 ・顧客リスト ・ユーザ台帳 ・メールリスト
		自社	・社外秘資料全般	・活動方針

一般情報：機密情報以外の情報

機密性	大分類	中分類	小分類	例
一般情報 （機密性:1）	個人 情報	取引先	・一般公開されている個人情報	・名刺
		自社	・一般公開されている個人情報	
	個人情 報以外	取引先	・一般公開されている顧客情報	・カタログ ・パンフレット ・会社案内
		自社	・一般公開されている営業情報	

4. 情報資産の取り扱い

各情報資産は機密性に応じて以下のように取り扱うこと

	極秘(機密性:3)	社外秘(機密性:2)	一般(機密性:1)
ラベル表示	書類: 「極秘」や「Confidential」等を明記する。	制限なし	制限なし
	外部記憶装置:識別できるよう色付きのシール等を貼る		
保管	書類:キャビネット・引出施錠保管／保管期間の設定／クリアデスクの実施	書類:キャビネット・引き出し保管／保管期間の設定／クリアデスクの実施	書類:クリアデスクの実施
	サーバ: フォルダのアクセス制御／サーバーラックによる施錠保管／保管期間の設定／クリアスクリーンの実施		サーバ:サーバーラックによる施錠保管／クリアスクリーンの実施
	PC・外部記憶装置:キャビネット・引出施錠保管、またはセキュリティワイヤーの設置／入退室管理／保管期間の設定／クリアデスクの実施		
紙コピーの配布	原則禁止 やむを得ず配布する場合は、所属長の承認を得、配布先は関係者に限定する。	社内であれば特別な制限なし。 取引先では関係者に限定。	制限なし
電子メール	原則禁止 やむを得ず配布する場合は、所属長の承認を得、下記の事項を遵守する。 送信:本文に機密情報を記載せず、添付ファイルに記載し、パスワードを設定する。パスワードは添付ファイルと別メールにて送付。 受信:パスワード設定を依頼する。	関係者に限定 送信:本文に機密情報を記載せず、添付ファイルに記載し、パスワードを設定する。パスワードは添付ファイルと別メールにて送付。 受信:パスワード設定を依頼する。	制限なし
FAX による伝送	原則禁止 やむを得ず送付する場合は、所属長の承認を得、関係者に限定し、相手先に送受信を確認する。また、印刷物の裏紙は使用しない。	関係者に限定 相手先に送受信を確認する。 印刷物の裏紙は使用しない。	制限なし

電話による会話	関係者に限定	社内であれば特別な制限なし。取引先では関係者に限定。	制限なし
第三者への情報提供	原則禁止（経営者の承認がある場合は除く）	原則禁止（経営者の承認がある場合は除く）	制限なし
社内送付	原則手渡し	制限なし	制限なし
社外送付	原則禁止　やむを得ず送付する場合は、所属長の承認を得、関係者に限定し、履歴が残るよう宅配便にて送付する。	関係者に限定し、開封の痕跡が残るシール・テープ等を使用する。	制限なし
持ち出し	原則持ち出しは行わない やむを得ず持ち出す際は、期間、目的、理由等を明記した上、所属長の承認を得ること。 紛失時のリスクを鑑み、PC 内に保有している極秘情報についてわかるよう、記録を残しておく。 その他、下記事項を遵守する。 ・紛失、盗難にあわぬよう、細心の注意を払う。 ・目の届かない場所に放置せず、常に携帯する。 ・PC は必ず暗号化を行う。 ・外部記憶装置は必ず媒体を暗号化もしくはデータにパスワードを設定する。	持ち出しを行う場合は、下記事項を遵守する。 ・紛失、盗難にあわぬよう、細心の注意を払う。 ・目の届かない場所に放置せず、常に携帯する。 ・PC は必ず暗号化を行う。 ・外部記憶装置は必ず媒体を暗号化もしくはデータにパスワードを設定する。	制限なし
廃棄処分	書類：シュレッダーの徹底、または重要文書処理システムによる溶解処理		制限なし
	PC・サーバ・外部記憶装置：専用ソフトによるデータの完全抹消／廃棄業者から「粉砕／廃棄証明書」を入手／物理的破壊		
裏紙の使用	禁止		制限なし

5.　インシデント発生時の対応手順

インシデント発生時の対応手順を影響度別に以下に示す。

大 ·社外(顧客、取引先)にも影響が及ぶ場合
中 ·会社全体に影響が及ぶ場合
小 ·組織または個人に影響が限定されている場合

インシデントによる影響度：

No	手順	影響度：大	中	小
1	社内報告	所属長·部長·常務·社長へ連絡		
2	社内調査	一次調査の実施 (状況·事実確認、影響範囲、リスクの特定、原因など)		
3	インシデント発生報告書の作成(中間報告)	発生部署より総務へ報告		
4	証拠の保管	情報の調査に必要な証拠として、サーバのデータ、アクセスログ、文書類、通信記録、入退出記録等の現状の保存		
5	対策委員会の設置	インシデントの影響度に応じて、社長が緊急対策員会の		
6	原因追及·対策検討	フジコー全社にて緊急対策委員会※を設置	組織にて対策チームを設置	
7	対策の実施			
8	再発防止策の要否判断·再発防止策の検討			
9	インシデント発生報告書の作成(最終報告)	発生部署より総務へ報告		

※　緊急対策本部における主な対応

- 必要な施策の実施
- 再発防止策の検討及び、適切な是正の実施
- 対外的対応
- 関係者(顧客·関係会社)への対応(個人情報の場合、影響を受ける可能性のある本人への連絡含む)
- 法的対応