社員・職員に求められる情報セキュリティ

株式会社Purpom Media Lab

ISMS教育教材

doc_id: EDU-MAT-003 ／ version: 1.0
制定日: 2024年4月1日

1. 社員としての責任と義務

当社のISMSに基づき、全社員・職員は情報セキュリティの維持に責任を持ちます。情報セキュリティは特定の担当者だけの問題ではなく、全員が当事者です。

> **社員に求められる基本姿勢**
>
> - 情報セキュリティ方針・社内ルールを理解し遵守する
> - 不審な事象に気づいたらすぐにISMS担当者に報告する
> - 自分が扱う情報資産の価値と重要性を認識する
> - セキュリティより利便性を優先しない

2. 業務端末の取り扱い

PC・スマートフォン

- 業務用PCは私的利用禁止（個人のUSBメモリ・ソフトウェアの使用禁止）

- 離席時は必ず画面ロック（Windows: Win+L、Mac: Ctrl+Cmd+Q）
- OSアップデートは通知があったら速やかに適用する
- 紛失・盗難が発生した場合は直ちにISMS担当者に連絡する

在宅勤務・外出先での利用

- 公共Wi-Fi（カフェ・空港等）での機密情報の取り扱いは避ける
- 画面を他人に見られないよう注意する（のぞき見防止フィルター推奨）
- 業務終了後はPCを安全な場所に保管する

3. メール・コミュニケーションのルール

メール送信時の注意

- 送信前に宛先・添付ファイルを必ず確認する
- 個人情報・機密情報をメールで送る場合はパスワード設定を検討する
- 不審なメールの添付ファイル・リンクは絶対に開かない
- 誤送信した場合はすぐにISMS担当者に報告する

4. 情報の取り扱い分類

分類	例	取り扱い
機密情報	顧客個人情報・契約内容・認証情報	社外持出禁止・暗号化必須
社内限定	社内議事録・売上データ・人事情報	社員間のみ共有可
公開情報	会社ウェブサイト・プレスリリース	制限なし

5. 退職・契約終了時の手続き

- 業務データを個人端末・クラウドに残さない

- 会社から貸与されたPC・機器をすべて返却する
- 業務上知り得た機密情報は退職後も守秘義務が継続する

6. インシデント報告フロー

気づいた社員 → **ISMS担当者（宮田幸輝）に連絡** → 状況確認・初動対応 → 経営者（青木光平）への報告 → 再発防止策の検討

受講確認
本教材の内容を理解し、社員・職員としての情報セキュリティ責任を果たすことを確認しました。