個人情報・機密情報保護研修（理解度確認シート）

1．個人情報とは？

当該情報に含まれる氏名、生年月日その他の記述などによって特定の個人を識別できるもの、または個人識別符号が含まれるものが個人情報に該当します。

«個人情報に該当するもの»

・氏名、住所、電話番号、年齢、生年月日、所属会社名、職位、社員名簿、住所録、緊急連絡網　など。

氏名のみで特定の個人を識別できる場合は「個人情報」となり、また、姓（名字）だけでは誰かを特定できませんが、その姓（名字）に「○□△会社に勤務」「東京都○△区○△町△番地在住」などの情報が加われば、その人が誰であるかを特定できるため、「個人情報」となります。

・DNA、指紋、手指の静脈、運転免許証番号、基礎年金番号、マイナンバー　など。

個人の身体的特徴を変換した符号や公的機関が個人に割り振った番号などが「個人情報」となります。

2．個人情報・機密情報の取扱い原則

就業先では、就業先の個人情報や機密情報に触れる機会があります、就業先の個人情報や機密情報を取り扱う各プロセスにおいて、セキュリティを意識し注意して取扱いをします。

- **取得**するときは、**業務上の必要な範囲内**で取得しなければなりません。
- **利用**するときは、**利用目的の範囲内**で利用する、指定された**目的以外**に利用してはいけません。
  就業先の許可なく、記録媒体等に**複写**、**複製**してはいけません。
  資料やデータを許可なく**第三者に提供**してはいけません
  指示された業務が終了したら、預かった資料やマニュアルは**速やかに返却**します。
- **移送**するときは、紛失、漏洩、誤配等の**危険を最小限**にするようにしなければなりません。
- **保管**するときは、決められた**所定の場所**、**施錠キャビネット等**に保管しなければなりません。
- **廃棄**するときは、就業先の指示に従い、**シュレッダー等**により**適正**に**廃棄**します。

3．注意するポイント

（1）入退出許可証（社員証）、パスワード等の取扱い

①入退出許可証が貸与されたら、**紛失**、**盗難**に注意します。

②他人と**貸し借り**は絶対にしてはいけません。

③就業先システムのアカウント／パスワードは他の者には**開示せず**、適切に管理します。

④万が一紛失等の際は、悪用されないよう、**すぐに責任者に連絡**し、紛失の手続きをします。

（事例）入館証（セキュリティカード）が入ったカバンを電車に置いてきてしまった。駅に届いている可能性があるため、その日は「忘れました」と嘘をついた。次の日、駅に届けられていなかったため、会社で紛失手続きをしたところ、カード使用履歴にて会社に侵入されていたことが発覚・・・。

⚠ 早急に手続きをしないと個人情報や社内秘の情報が盗まれる事件に発展することになりかねません。

（2）就業先構内での取扱い

①コピー・FAX・プリンター機に資料を**放置**してはいけません。

②就業先の書類やデータを自宅に**持ち帰ったり**、クラウド上のデータを個人アカウントへ**転用**してはいけません。

③就業先で**情報セキュリティに関する規程**や**ルール**が定められている場合はそれに従います。

（事例）自宅で仕事をするため職場のデータを USB に保存して無断で持ち出ししていたが、内部監査で書類の作成時刻が勤務時間外になっていることがわかり、事情聴取をされ、持ち出しが発覚・・・。

⚠ データの持ち出しは、USB の紛失やパソコンのウィルス感染など、漏洩の危険にさらす行為になります。

（3）ネットワーク、E メールの取扱い

①メールや FAX を送信する場合は、**宛先**や**送る内容**に間違いがないことを十分確認してから送信します。

②複数名へ一斉にメールをする場合は、必ず宛先 **BCC** を利用します。

③**業務目的以外**でインターネットに接続して WEB サイトを**閲覧**したり、**私用メール**をしてはいけません

④ウィルスの感染となるため心当たりのないメール（添付ファイル）は**不用意に開封**してはいけません。

⑤不特定多数が閲覧できるサイトへ就業先の情報を**掲載**、**投稿**してはいけません。

（Twitter・BLOG・Facebook・電子掲示板など）

（事例）業務中に自身の机上にある食べ物をスマートフォンで撮影し、Twitter に投稿。
しかしその画像には机上にあった社名などが記載された申告書類が写りこんでおり、取引先の情報が流出・・・。

⚠ SNS への不用意な投稿がきっかけで会社の個人情報や機密情報を漏洩させてしまう場合があります。

（4）情報の持ち出し、運搬の取扱い（許可を得て、業務で持ち出しをするとき）

①運搬に適したバックに入れ、**肌身離さない**ようにし、目が届かない場所、電車の網棚、着席時の足元などに置いてはいけません。

②少しの時間でも、**自動車**に**放置**してはいけません。

③貸与されている**携帯電話**、**ノート PC**、**タブレット**等の**紛失**、**盗難**に注意します。

④運転中は**寄り道**や**回り道**をしてはいけません、就業先の情報を持ったまま**飲酒**は**厳禁**です。

⑤飲食店、交通機関、エレベーターなど**公共の場**で、不適切な発言（就業先の情報や中傷）をしてはいけません。

（事例）職場の近くの喫茶店で同僚とランチの最中に、顧客である A 社を中傷するような会話をしていた。
しかし同じ店内にいた A 社の関係者に聞かれていたことにより、後日、その会社から取引停止を告げられた・・・。

⚠ 公共の場では身内や知り合いがいることも考えられます。この発言を今この場でしてしまうと、もしかすると大変なことになってしまうかもという意識を忘れてはいけません。

4．個人情報・機密情報の漏洩による影響

次のことを十分認識し、個人情報等の保護に努めることが必要です。

（1）漏洩した個人情報はどうなる？

情報はインターネット上の闇のマーケットで販売され、勧誘の電話や高値品の紹介などが届くようになるなど軽度な被害から、近年ではオレオレ詐欺、架空請求詐欺、偽装恐喝など巧妙な手口で**悪用される被害**が出ています。

（2）企業への影響

個人情報の流出などによる企業側のダメージは計り知れません。

社会的信用の失墜、**業務停止**、ともすれば**巨額な賠償**にも発展しかねない大きな影響を受けます。

この他にも、顧客対応、漏洩情報の回収、マスコミ対応なども発生し、人手や時間、金銭的に大きな打撃を受けます。

（3）個人への影響

個人情報の取扱いに関するルールを故意に違反したり、または重大な過失により、個人情報を漏洩させた場合は、法律による罰則に加えて、会社の規程により、懲戒解雇を含め**厳しい処分**が行われます。

5．事故発生時の対応

万が一、**紛失や盗難、情報漏洩等**に**気付いた場合**、または**可能性がある場合**でも、自分だけで判断せず、**直ちに**就業先の責任者に報告し判断を仰いでください。

すぐに連絡・相談をすることにより、2 次被害を抑えるアクションに繋げることができます。

当社は、プライバシーマーク認定事業者として、個人情報保護体制を維持・強化しながら、個人情報保護管理の徹底に努めています。
自身を守るためにも正しく理解して頂き、共に個人情報保護に取り組んでください。
※本テキストは、当社 HP 派遣マイランスタッド内で参照できます。