※同封の「解答用紙」へご回答いただき、年末調整書類と一緒に返送してください。

テクノウェイブでは「Pマーク」及び「ISMS」の認証を取得しており、最低年一回の社員教育を制定しております。つきましては、スタッフの皆様におかれましても本テキストによる教育へのご協力をお願いいたします。

Web でも受講できます。
Web で受講いただいた場合は同封の解答用紙の返送は必要ありません。

個人情報保護・セキュリティ教育テキスト

昨今、新聞やテレビ等で「〇〇社から個人情報が漏洩した」という事故が度々報道されています。
平成 28 年度に JIPDEC（一般財団法人日本情報経済社会推進協会）に報告があった個人情報の取扱いにおける事故の報告では、843 の付与事業所より 2,044 件の事故報告があり、前年度より増加しています。
また、事故の原因として**「メール誤送信」（約 2 割）が最も多く、**次いで「紛失」「郵便の宛名違い」となっており、前年度に比べると割合が減少したものの依然これらが多くを占めています。紛失は主にノート PC やモバイル端末。
注目したいのは**「プログラムやシステムの作業ミス」や「不正アクセス・不正ログイン」による事故が 2 倍強に増加**しており、作業手順や ID/PW の管理方法の見直しが一段と求められる結果となっています。

私達一人一人がセキュリティの運用ルールを厳守して、「個人情報及び機密情報を守る」意識を持つことが重要です。

このテキストでは、今一度「個人情報」「セキュリティ」をご理解いただき、個人情報や機密情報の漏洩を防ぐために、改めて皆さんと意識を共有していただくために一読いただき、**同封の「解答用紙」にご解答ください。**

① 個人情報とは

知っているようで、よくわかっていないなんてことはありませんか？

氏名、住所、電話番号、メールアドレス、社員番号、給与明細、健康情報、お客様情報、写真、映像、音声、名刺・・・本人を特定できるものが個人情報です。ID など単独では本人を特定できなくても、他の情報と組み合わせる事で本人が特定できるなら、それも個人情報です。

② 個人情報保護法

個人情報を正しく扱わなければならないという法律があります。

2005 年 4 月から「個人情報の保護に関する法律」が施行されています。この法律は会社等を対象とした法律ですが、事件や事故を起こした人に対して、結果として損害賠償を請求されるということもありえるのです。

③ 就業先企業のルールを守ること

当たり前のことですが、とても大事なことです。

就業先によって運用ルールは異なりますが、仕事をするときは、就業先のルール（社風、服務規程、慣行、その規程）を守らなければなりません。個人情報を含む情報の取扱いについても、就業先のセキュリティルールがありますから、そのルールに従って仕事をしてください。

④ 守秘義務

派遣では特に重要なルールです。

仕事をするうえで知った情報や書類、USBメモリなどの記録媒体を持ち出したり、他人に漏らしてはなりません。話し声にも気を付けましょう。また、就業期間が終了した後も同様です。

- 書類や記録媒体を持ち出さない
- 机を離れるときや、退社するときは、書類などを出したままにしない。パソコンの画面も情報を表示したままにしない。
- 仕事で使った書類や記録媒体などは、もとの場所に戻す。
- 仕事上知った情報を他人に漏らさない。

⑤ 漏洩への注意

「しゃべる情報」も重要な個人情報です。

仕事をする上で知った個人情報や企業情報等の機密情報を社外の人に口外したり、仕事以外の目的に利用してはいけません。特に、酒席での会話や喫煙場所での会話は要注意です。また、公共の場でも同様な注意が必要です。

裏へ続く

⑥ 紛失への注意

「忙しい」、「ずさんな整理」そんなところから、紛失が起こります。

情報漏洩する原因のほとんどが、「うっかりミス」です。
書類や記録媒体を整理しないでいたり、ばらばらのままの書類を持って歩いたり、うっかり立ち話をしているときに置き忘れたり・・・そんなことのないように、普段から注意を怠らないでください。もちろん意図的に紛失するなど、もってのほかです。特に飲みの席及びその帰路では注意が必要です。
入館証・社員証・IDカード等の管理もとても大事で、紛失してしまった場合は派遣先及び就業先に大変な迷惑をかけることとなりますので厳重に管理するとともに、万が一紛失してしまった場合は速やかに就業先の連絡ルールに従い関係各所に報告をしてください。

⑦ 保管・整頓

整理・整頓は仕事の基本です。

就業先で仕事をする時は常に整理・整頓に心掛けましょう。書類その他記録媒体等の保管場所が就業先で決まっているか、就業先の責任者もしくは担当者に確認して下さい。決まっている場合は必ずその保管方法で保管して下さい。
例えば保管庫に保管し施錠してから退社するなどです。

⑧ PC の取扱い

パソコンの取り扱いで被害が拡大します。

就業先の管理規程や運用規程に従い、管理を徹底して下さい。

- 利用しているパソコンから長時間席を外す時は、電源を切る又はログオフし、他人が貴方になりすまして利用できない状態として下さい。
- 就業先からパスワードが与えられた場合、絶対他人に教えてはいけません。
- パソコンから出力した書類は、速やかに回収し長時間放置しないで下さい。
- インターネット接続は、私的な目的に利用してはいけません。また、SNS 等への業務情報の投稿はしないでください。
- 許可されていないソフトウェアを無断でインストールしてはいけません。
- 自分のノートパソコン等を無断で持ち込み、利用してはいけません。業務上やむを得ず持ち込む時は、就業先の責任者もしくは担当者に確認し、承認を得て下さい。
- Winny 等のファイル共有ソフトは情報漏洩の危険性がかなり高いので、職場や自宅に関わらず使用しないで下さい。

⑨ 携帯電話の取扱い

携帯電話にも個人情報が一杯です。

会社から貸与された携帯電話は会社の管理細則に従って取扱って下さい。
私有の携帯電話には許可がない限り、業務に関わる情報を登録しないで下さい。
また、私有の携帯電話を業務で使用する事は原則禁止です。やむを得ず使用したときは、使用後直ちに発信記録・着信記録を消去して下さい。

⑩ 外部との通信について

情報漏洩の一番危険な手段です。

就業先から、業務上メールアドレスが与えられている場合、私的な目的での利用は厳禁です。業務上での使用は、就業先での管理規程や運用規程に従って下さい。

個人情報や企業情報等の機密情報をメールの添付ファイルで送る時は、必ず就業先の責任者あるいは担当者に確認し、判断を仰いで下さい。
FAX を送信する場合、送信前に必ず相手先番号を確認し、誤送信が無い様注意して下さい。
電話で社外あるいは社内から個人情報や機密情報の問合せがあった場合は、自分で判断しないで、必ず就業先の責任者あるいは担当者に判断を仰いで下さい。

重要な情報ではないと思っても、漏らしていけない機密情報である場合があります。

⑪ 廃棄する情報について

捨てたゴミからも情報漏洩します。

個人情報や企業情報等機密情報が記載された書類や記録媒体はそのままゴミ箱に捨ててはいけません。記載された文字などが読めなくなる様処理を行う必要があります。
具体的には、書類はシュレッダーによる裁断や焼却処分となりますが、詳しくは就業先の責任者もしくは担当者に確認し、ルールに従ってください。

以　上