事件・事故の報告

■個人情報に係るセキュリティの事象･弱点を発見した場合は、出来る限り
個人情報保護管理者および上長に電話もしくはメールで報告する。

（個人情報に係るセキュリティの事象･弱点の例）

サービスや装置の停止	システムやハードウェアソフトウェアの誤動作	誤送信・誤発送等のミス	社内ルールの不遵守	紛失・き損
改ざん・破壊	ウイルス感染	PC等の動作異常	苦情外部通報	ヒヤリハット

緊急時対応は、速やかな事実の報告が最重要です！

ウイルスへの対応策と感染時の対応

■パターンファイルは自動更新設定にする。

■アンチウイルスソフトは常駐設定にする。

■利用するブラウザに応じて適切なセキュリティ設定を実施する。

※従業員は、貸与されたPCの設定を原則として変更しない。

（有線接続の場合）
ネットワークケーブルを抜く

（無線接続の場合）
Wi-fi接続をオフする

※PCの電源はOFFしない

情報システム管理者に
速やかに事実報告を行う

事件・事故による悪影響

損害賠償責任などの経済的損失

- **顧客や取引先企業から損害賠償を求められる可能性**
  →漏えい件数など、発生した事件･事故の規模によっては多額の損害賠償責任の発生
  →係争案件化することによって長期に渡り「人」「時間」「資金」等がかかる虞
- **事件･事故の公表による株価の下落や顧客離れによる業績不振**

会社のイメージダウン

- **当社の社会的信用の失墜**
- **マイナスイメージを払拭できず同業他社との競争力の低下**

罰則・ペナルティー

- **（本人）故意犯に対する法的罰則の可能性**
- **（本人）就業規程違反による懲戒等処罰の可能性（故意･過失は問わない）**
- **（組織）行政機関からの当社に対する監督責任の追及**

それでも報告が大事！

いますぐ出来る不正アクセスの防止策

■PCのスクリーンセーバは、組織の定めに従い設定する。

※従業員は、許可なく一時的でもPC等の設定をルール外に変更しない。

■離席する場合は、画面ロックし、不正使用の防止に努める。

■プリンター等には印刷物を放置しない。

■ノートPCは、ワイヤーロックを施すか、不使用時の施錠管理を実施する。

物理的媒体の管理

■私物のUSBメモリや外付けHDDは、使用禁止。

■業務でUSBメモリや外部記憶媒体などを使用する場合、
個人情報保護管理者或いは本件に関する決裁権者の承認を得る。

会社資産のUSBメモリ等は、組織で一元管理されています。
使用を希望する場合、従業員は部門責任者等の決裁権者に申請し、承認を得てください。

■社有・私有問わずスマートフォンを記憶媒体として利用すること及び
USBポートを利用したスマートフォン等の充電は禁止する。

社外でのセキュリティ対策①

在宅勤務・場外労働にあたっては、**社内で業務を行うのと同等以上の**
セキュリティ対策を各従業員が責任をもって実施しなければなりません。

ルールを再確認し、各自が実施すべきセキュリティ対策を認識してください。

■持出し前(社内)の注意

①社内から持出す文書（電子ファイル）には、
ファイルにパスワードを設定する等の安全管理策を施す。

・PCを社外に持出す従業員は、必要以上の情報をPCに格納したままにしない。
・不要な情報は適宜PC内から削除する。

②文書（紙/電子）の持出し・持ち帰りは禁止。

社外でのセキュリティ対策②

■持出中(移動中)の注意

①無用な立ち寄りや飲食は避ける。

・情報資産を持ち歩いている場合、飲酒等は特に避け、速やかに帰宅すること。
※あるいは、一旦社内に情報資産を置いてから飲食等に向かう。

②資産は決して手放さず、放置しない。

(考慮すべきリスク)

・会社帰りに同僚と居酒屋に寄り、
帰りのタクシーに置き忘れ**紛失**する。
・網棚に上げたことを忘れて下車してしまい、**紛失**する。
・立ち寄った飲食店で席を外している間に**置き引き**に遭う。
・車中に放置し車上荒らしにあい、**盗難**被害にあう。

③社外でのネットワーク接続時には盗聴等に留意する。

・公衆無線LAN等は、暗号化されていない場合があるため利用を禁止とする。

社外でのセキュリティ対策④

■社外業務中の注意（在宅勤務を含む）

①可能な限り物理的境界を設け、業務中のセキュリティを確保する。

・家族であっても当社の業務情報を見せたり、話題にしない。

・覗き見や不正操作による情報漏えいを防止するため、部屋を分けたり、業務場所に境界を設けて安全を確保する。

②業務の中断や離席の際には画面ロックを行う。

・社内業務時と同様に、離席時には画面をロックする。

③作業場所は整理整頓を行う。

・社内同様にクリアデスク・クリアスクリーンを行い、適正に情報を管理する。

・業務場所を整理整頓し、配線に躓いて情報が滅失する等の事故が発生しないよう留意する。

社外でのセキュリティ対策⑤

■自宅のセキュリティ状況を確認する

在宅勤務を行う場合、最低限行うべきセキュリティ対策を挙げています。
定期的に、業務を始める前にチェックしてください。

□自宅にある全PCのアンチウィルスソフトの更新

アンチウィルスソフトは常駐設定になっているか確認する。

□自宅にある全PCのOS等のパターンファイルの更新

定期的に更新設定を確認し、最新版が適用がされていることを確認する。

□自宅にあるルータ等のサポート期間及びID/PWの確認

メーカーサポートの継続状況を確認する。

□自宅にあるルータ等のファームウェア、ソフトウェアの更新

脆弱性等に対し、アップデートファイルの提供を確認する。

□自宅にある他PCのインストールアプリの安全性の確認

ネットワーク内にファイル共有ソフトをインストールしたPC等はないか確認する。

□自宅での業務書類の印刷禁止

社外での振る舞い

業務上で取扱う、または知り得た情報は会社の資産です。
社外では以下のルールを守りましょう。

■業務外で使用、利用しない。
■不用意に口外したり、話題にしない。

→例え身近な人の情報でも、業務上知りえた情報であれば本人に対しても口外しない。
→業務上の話を、従業者以外との会話でしない。
→従業者同士であっても、社外での業務内容に関する話題は避ける。
→社内、顧客先に関わらず、許可なく書類・データの持出しは行わない。
→業務に関わることや職場のことを、SNSに書き込まない。