

情報管理要領

＜株式会社泰和工業＞

制定日 : 2022年6月24日

改訂日 :

1. 組織／体制

(1) 情報セキュリティの責任者、担当者と役割は、次のとおりとする。

① 情報セキュリティ責任者 : (役職) 常務取締役 (氏名) 中里 登喜男

※本要領に基づき、社内の情報セキュリティの運用について指導、監督する。

② 情報セキュリティ担当者 : (役職) 総務課長 (氏名) 斎藤 俊彦

※本要領に基づき、社内の情報セキュリティの運用を行う。社内外との問合せ窓口となる。

(2) 情報システムの担当者を配置する。

① 情報システム担当者 : (役職) 総務課長 (氏名) 斎藤 俊彦

※情報システムの導入、運用を行う。社内の問合せ窓口となる。

2. 業務従事者の教育・指導

(1) 業務従事者に対し、情報セキュリティ等に関する教育・指導を継続的に実施する。(最低年1回)

(2) 業務従事者が退職等で業務を離れる際は、次の手続きを行う。

① 誓約書の提出

② 会社が貸与した情報資産の返却

3. 情報システムの対策

(1) 外部からの社内ネットワークへの不正アクセスを防止する。

(2) 電子ファイルは、アクセス権を設定しているファイルサーバ等に格納する。

(3) サーバやPCにウィルス対策ソフトを導入し、パターンファイルの更新を定期的に行う。

(4) 情報システム(Windows、ソフトウェア等)に対して、修正プログラムの適用、Windows update等を行い、脆弱性の解消を行う。

(5) 私物のスマートフォン／携帯電話／タブレット等で、業務の撮影、画像送信を行わない。

(6) PC、外部記憶媒体(SDカード、USBメモリ等)の利用は、会社貸与品のみとし、個人所有のものを使用しない。

(7) 社外等でのUSBメモリ等の利用時には、情報を暗号化する。

4. 機密情報の取扱い

※機密情報：会社にとって重要な秘密情報、開示された場合、損害が生じる情報

(1) 機密情報は、目的外のことに利用しない。

(2) 機密情報の社外持出しは、原則、禁止とする。(特に、自宅への持出しは、絶対に行わない。)

やむを得ず、重要情報を社外に持出す際は、社内ルールに基づき、承認を得る。

承認者：(役職) 常務取締役 (氏名) 中里 登喜男

- (3) お客様から重要情報として指定された機密情報(以下、「重要情報」という。)は、目録(※お客様から提示される様式)で管理する。
- (4) お客様から受領した機密情報の配布(複製・複写)は、お客様との契約条項に基づき行う。なお、配布する際には、いつ、誰が、誰に、どのような方法で配布したか等を記録する。
- (5) 機密情報が記録された紙媒体、外部記憶媒体(USBメモリ、SDカード、CD、DVD等)は、常時、施錠可能な書庫等に保管する。
- (6) お客様から受領した重要情報は、業務上不要になった時点で委託元へ返却、もしくは廃棄・削除する。

5. 再委託先の管理

- (1) 委託元が求める情報セキュリティ要件を再委託先が満たしていることを確認する。
- (2) 再委託先に重要情報を提供する場合、委託元の承認を得る。
- (3) 再委託先へ提供する重要情報は、目録(情報授受の記録)で管理する。
- (4) 重要情報は、業務上不要になった時点で再委託先から返却、もしくは廃棄・削除していることを確認する。

6. 情報セキュリティ事故

- (1) 情報セキュリティ事故の発生時は、委託元に速やかに報告する。
- (2) 委託先内の情報共有、委託元への報告等の連絡網は、次のとおり。
発見者 ⇒ 情報セキュリティ担当者 ⇒ 情報セキュリティ責任者 ⇒ (お客様)
※情報セキュリティ担当者から社内へ共有
- (3) 情報セキュリティ事故の発生時には、再発防止策を検討し、是正処置を行う。また、再発防止策の実施後、有効性評価を行う。

7. 自主点検/監査

- (1) 情報セキュリティの対策状況について、自主点検を行う。(最低年1回)
- (2) 自主点検結果に基づき、継続的改善を行う。

8. その他

本要領は、定期的に見直しの検討を行い、必要に応じ改訂する。

以上