人的管理規程

1.0版

人的管理規程

人的管理規程

１　趣旨

本規程では、役員を含む従業員及び契約相手がその責任を理解し、求められている役割にふさわしいことを確実にすることを目的とする。

２　対象者

当社の情報資産に携わっているすべての者（役員、従業員、契約相手、またはそれを運用、管理し、業務に携わっているすべての者）を対象とする。

３　対象システム

本規程は人的管理に関するものであり、情報システムや情報機器を対象としない。

４　遵守事項

４．１　雇用

４．１．１　雇用前

(A.7.1)

役員、従業員の雇用にあたっては、以下の事項を遵守しなければならない。

（１）経歴等の確認については、関連法令、規則及び倫理に従って行うこと。またこの確認は、事業上の要求事項、アクセスされる情報の分類及び認識されたリスクに応じて行うこと。

（２）応募者の情報は、個人情報保護法に基づき、適切に処置すること。

（３）雇用する場合には、以下の事項について確認を行うこと。

・情報セキュリティに関するその役割を果たすために、必要な力量を備えていること

・組織にとって、その役割を任せられ、信頼できる人物であること

４．１．２　雇用条件

(A.7.1.2)

当社の情報資産に携わっているすべての者は、以下の条件を遵守しなければならない。

（１）従業員及び契約相手との雇用契約書には、情報セキュリティに関する責任及び組織の責任を記載しておくこと。

（２）従業員及び契約相手の契約上の義務ついて、以下の事項を明確にしておくこと。

・秘密保持契約書又は守秘義務契約書への署名、捺印をすること

・扱われる情報資産に対する保護、管理に関する責任を明確にしておくこと

・当社が定める情報セキュリティに関する要求事項に従わない場合にとる処置に

ついて、明確にしておくこと
・雇用期間の終了後についても、この雇用条件に定められた責任が継続することを明確にしておくこと

４．１．３　雇用期間中

(A.7.2)

当社の情報資産に携わっているすべての者は、以下を遵守しなければならない。

（１）組織の確立された方針及び手順に従った情報セキュリティの適用を、従業員及び契約相手に要求すること。

（２）職務に関連する組織の方針及び手順について、適切な意識向上のための教育及び訓練を定期的に受けること。

（３）教育、訓練の内容には、以下の項目を含めること。

・情報セキュリティに関する経営陣のコミットメント
・情報セキュリティに関する規則及び義務を熟知し、これを遵守すること
・情報セキュリティに関する基本的な手順及び規則
・これらに違反した場合の処置

４．１．４　雇用終了及び変更

(A.7.3)

当社の情報資産に携わっているすべての者は、以下を遵守しなければならない。

（１）雇用の終了又は変更後も、秘密保持契約又は守秘義務契約内容が継続することを、十分に認識させること。

４．２　プライバシー及び個人を特定できる情報の保護

(A.18.1.4)

顧客の個人情報（以下「顧客情報」とする）を適切に収集・保管・廃棄における取り扱い時に注意するべき事項をまとめ、発生しうる問題を未然に防ぐことを目的とする。

顧客情報を取り扱うすべてのコンピュータ及び媒体を対象とする。

４．２．１　顧客情報を取り扱う部門の特定

(A.8.1)

役員、従業員は、以下を遵守しなければならない。

（１）情報セキュリティ委員会は、当社内にて顧客情報を取り扱う部門を特定し、その部門長に対して、以下の遵守事項を徹底させなければならない。又、当該従業員に対する顧客情報の取り扱いについて、十分認識させなければならない。(「４．３情報セキュリティ教育」参照)

（２）特定されていない部門においては、顧客情報を取り扱ってはならない。

４．２．２　顧客情報管理責任者の設置

(A.8.1.2)

役員、従業員は、以下を遵守しなければならない。

（１）顧客情報の収集・保管・廃棄を行う部門の部門長は、顧客情報管理責任者を任命し、部門内に保有する顧客情報について、それぞれの責任者を明確にしなければならない。

４．２．３　顧客情報保護方針の公開

(A.18.1.4)

役員、従業員は、以下を遵守しなければならない。

（１）顧客情報管理責任者は、顧客情報を広く一般から収集する場合、当社の Web サイトや広告等に当社の顧客情報保護方針を公開しなければならない。

（２）顧客情報保護方針には、下記に記載される遵守事項の内容および当社への連絡先を明確にしなければならない。

４．２．４　顧客情報の収集

(A.8.1.1)

顧客情報の収集を行う者は、以下の事項を遵守しなければならない。

（１）顧客情報の収集時には、顧客に対して利用目的を明示し、顧客から同意を得なければならない。なお、収集以外の形で得た顧客情報を利用する場合は改めて顧客から同意を得なければならない。

（２）顧客に示した利用目的に必要な情報以外の情報を収集してはならない。

（３）収集した情報を顧客に明示した利用目的以外の利用をしてはならない。

４．２．５　顧客情報の保管

(A.8.1.2)

顧客情報管理責任者は、以下の事項を遵守しなければならない。

（１）顧客情報に対する登録・参照・変更・削除の実施可能な者を明確にし、顧客情報へのアクセス制限を実施しなければならない。

（２）顧客情報を利用する場合、正確な情報を利用しなければならず、そのための保護策を実施しなければならない。

（３）顧客情報のバックアップを実施しなければならない。バックアップした媒体は、顧客情報と同様の管理策を設けなければならない。

（４）顧客から当該顧客の顧客情報に関する開示・訂正・削除の要求があった場合、

これに対応しなければならない。

４．２．６　顧客情報の破棄

(A.8.1.4　A.8.3.2)

顧客情報管理責任者は、以下の事項を遵守しなければならない。

（１）顧客情報を廃棄する場合、第三者の目にさらされないように注意して廃棄しなければならない。

（２）電子媒体等の破棄においては、『システム利用規程』に基づいて実施しなければならない。

４．２．７　顧客からクレーム処理

(A.8.1.2)

顧客情報管理責任者は、以下の事項を遵守しなければならない。

（１）当社の業務において顧客からクレームを受けた場合には、速やかに対応しなければならない。

（２）顧客情報が漏えいしてしまったなど、必要がある場合、情報セキュリティ委員会を開催し、当社の見解を迅速に明確にし、関係者に周知しなければならない。

（３）いかなるクレームでも、第一報を 12 時間以内に情報セキュリティ委員会に報告し、その後の対応状況に関しても適宜連絡しなければならない。

４．３　情報セキュリティ教育

(A.7.2.2)

情報セキュリティ意識の向上のため、情報資産に携わっているすべての者、またはそれを運用、管理し、業務に携わっているすべての者を対象とし、情報セキュリティ教育、訓練に関わる事項を規定する。各自の責任及びその責任を果たす方法について、認識をさせることを目的とする。

４．３．１　教育の計画立案

(A.7.2.2)

教育部門ならびに、各部署の情報セキュリティ責任担当者は、対象者およびタイミング、もしくはその内容について、各教育を計画し、立案しなければならない。また、保護すべき情報及び情報を保護するために実施されている管理策を考慮に入れて、計画する。

（１）一般説明会

教育部門は、年に１回、情報資産に携わるすべての人に対して、情報セキュリティに関する説明会を実施しなければならない。

（2）再教育

教育部門は、情報セキュリティ違反者に対して、セキュリティの再教育を実施し、違反の再発防止に努めなければならない。

（3）新入社員、中間採用者への教育

教育部門は、新入社員、中間採用者に対して、入社時に情報セキュリティ教育を計画しなければならない。

（4）社内異動者への教育

各部署の情報セキュリティ責任担当者は、社内異動者に対して、異動時に、その部署の情報セキュリティに関して教育を計画しなければならない。

（5）契約社員および協力会社への教育

各部署の情報セキュリティ責任担当者は、契約社員および協力会社に対して、部署の情報セキュリティに関して、許可された権限と責務に応じた教育を計画しなければならない。

４．３．２　教育の実施

(A.7.2.2)

教育部門ならびに、各部署の情報セキュリティ責任担当者は、情報資産に携わるすべての人に対し、以下の教育内容について、教育資料を使用し、情報セキュリティ教育を実施しなければならない。

（1）教育内容

・当社の情報セキュリティ方針
・情報セキュリティの問題のもつ意味を理解
・組織や個人の情報セキュリティの重要性
・情報セキュリティ対策
・情報セキュリティ計画
・データ所有者の責任
・モラル教育
・法令、規則等の違反、罰則に関する事項
・禁止行為に関しての教育他
・最新の情報

（2）再教育

教育部門は、情報セキュリティ違反者に対して、情報セキュリティの再教育を実施し、違反の再発防止に努めなければならない。

（3）新入社員、中間採用者への教育

教育部門は、新入社員、中間採用者に対して、入社時に情報セキュリティ教育を実施しなければならない。

（４）社内異動者への教育

各部署の情報セキュリティ責任担当者は、社内異動者に対して、異動時に、その部署の情報セキュリティに関して教育を実施しなければならない。

（５）契約社員および協力会社への教育

各部署のセキュリティ責任担当者は、契約社員および協力会社に対して、部署の情報セキュリティに関して、許可された権限と責務に応じた教育を実施しなければならない。

４．３．３ 訓練の実施

(A.7.2.2)

教育部門ならびに、各部署の情報セキュリティ責任担当者は、情報セキュリティに責任をもつ対象者に対し、定期的に、以下の訓練内容について、訓練資料を使用し、情報セキュリティの訓練を実施しなければならない。

（１）訓練内容

・リスク分析
・情報セキュリティ対策についての導入、管理、運用、利用等
・情報セキュリティ問題の検出、検知、報告、復旧等

４．３．４ 教育、訓練資料

(A.7.2.2)

教育、訓練資料は、適切な教育、訓練を行うため、環境の変化及び、管理策の追加変更等を考慮に入れ、定期的な見直し行う。

教育、訓練資料には、以下のものがある。

・一般説明会教育資料
・再教育資料
・新入社員教育資料
・中間採用者教育資料
・社内異動者教育資料
・協力会社および契約社員教育資料
・情報セキュリティ対策訓練資料
・情報セキュリティ問題訓練資料

４．３．５ 教育実施記録

(A.7.2.2)

教育部門は、教育、訓練の実施状況に関して以下の記録を行わなければならない。

（１）記録項目

・教育の実施日、時間
・教育実施者（部署）
・教育の受講者
・教育の内容

４．３．６ 教育運用実施報告、確認

(A.7.2.2)

教育部門は、情報セキュリティ委員会に教育、訓練の実施状況を報告しなければならない。

情報セキュリティ委員会は、情報セキュリティの教育、訓練が適切に行われているかを把握するため、教育部門から提出される情報セキュリティ教育実施報告書を確認しなければならない。実施されていない場合、教育部門に対して、適切な指導を行わなければならない。

４．４ 懲戒手続

(A.7.2.3)

本規程は､当社の情報セキュリティ違反に対する罰則の適用手順及びそれに関わる遵守事項を規定する。

情報セキュリティ方針および規程類が適用されるすべての人を対象とする｡罰則事項の執行は、情報セキュリティ違反に対する罰則の適用に関わる情報セキュリティ委員会のメンバー、部門長及び人事部門の担当者を対象とする。

４．４．１ 罰則案件の届出

(A.7.2.3)

部門長は罰則に相当すると思われる従業員の情報セキュリティ違反を確認した場合、情報セキュリティ委員会に罰則の適用について審議を求める案件の届出を行わなければならない。なお、部門長の情報セキュリティ違反に関する罰則案件の届け出は情報セキュリティ委員会のメンバーが行うものとする。

４．４．２ 情報セキュリティ委員会での審議及び決定

(A.7.2.3)

情報セキュリティ委員会は届出が行われた罰則案件について審議を行い、罰則の適用と再教育についてその要否と程度または内容を決定しなければならない。また、審議するうえで、以下の事項を考慮する。

（１）違反の内容及び重大さ並びにその業務上の影響
（２）最初の違反か又は繰り返し起こされたものか
（３）違反者は、適切に教育、訓練されていたか

（４）関連する法令、規則又は取引契約内容についての確認
（５）その他、必要と判断される内容

４．４．３ 人事部門での罰則手続き

(A.7.2.3)

人事部門の担当者は情報セキュリティ委員会での決定に基づき、該当者に対する就業規則に従った罰則の決定及び適用に関する手続きの実施をしなければならない。

４．４．４ 再教育

(A.7.2.3)

情報セキュリティ委員会は罰則案件の審議結果で再教育が必要と決定した該当者に対して再教育を実施しなければならない。

５　運用確認事項

人的管理において、以下が行われていることを確認しなければならない。

（１）顧客情報の収集、保管、廃棄、クレーム等に関し、定期的に確認を行わなければならない。また、その状況を記録し保管しなければならない。
（２）教育実施後理解度を測り、理解度の低い者に対し、十分な理解が得られるように再教育等を実施しなければならない。
（３）関連法令、社内規程及び契約上の義務違反等を明確にし、それに対する被害状況等を確認する。その結果をもって、必要な対応策を検討し、実施可能な対応策を行わなければならない。実施が困難な場合は、残存リスクとして従業員が認識しなければならない。
（４）また、これらの事項については、必ず記録を残さなければならない。
（５）関連法規等ついては、定期的に見直し、最新の状態にし、従業員及び必要な契約相手等に知らしめなければならない。

６　除外事項

業務都合等により本規程の遵守事項を守れない状況が発生した場合は、情報セキュリティ委員会に報告し、例外の適用承認を受けなければならない。

７　罰則事項

本規程の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については『４．４懲戒手続』に従う。

８　公開事項

本規程は対象者にのみ公開するものとする。

９　改訂

・本規程は、平成ｘｘ年ｘｘ月ｘｘ日に情報セキュリティ委員会によって承認され、平成ｘｘ年ｘｘ月ｘｘ日より施行する。

・本規程の変更を求める者は、情報セキュリティ委員会に申請しなければならない。情報セキュリティ委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。

・本規程は、定期的（年１回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。