IT-Professor
情報セキュリティポリシー

2021 年 10 月

IT-Professor IT 部

更新履歴

	更新日	更新箇所	更新内容
1	2021/10	初版	

第1章 総則

(目的)

第1条　「IT-Professor情報セキュリティポリシー」(以下本ポリシーと称す)は、IT-Professor(以下IT-Pと称す)およびIT-Pの関連会社各社が保有する情報資産を、さまざまな脅威から保護し、安全で円滑な情報活用の実現に寄与するための原則を規定したものである。
このポリシーにより、情報セキュリティに対する取り組み姿勢を明確にするとともに、全ての従業員等に周知し、情報セキュリティ対策を網羅的かつ継続的に推進する。

(定義)

第2条　本ポリシーで使用する用語を以下のとおり定義する。

1「情報資産」

情報および情報システムの総称とする。
情報は、電子化されたデータ、音声、画像等とし、伝達・保存手段としての媒介・媒体の如何を問わない。
情報システムは、ハードウェア、ソフトウェアおよびネットワーク等で構成し、情報を収集・蓄積・処理・伝達・利用する仕組みとする。

2「従業員」

IT-Pグループ各社と直接雇用契約を締結する社員および派遣契約従事者とする。
また、業務委託先など協働者を含める場合、従業員等と称する。

3「部門長」

各事業部門の長および各管理部門の長とする。また、グループ各社長を含め、部門長等と称する。

(適用範囲)

第3条 本ポリシーの適用範囲を以下のとおりとする。

1　役員および従業員等

2　IT-Pグループ各社

3　IT-Pグループ各社に責任が帰属する情報資産

(原則)

第4条　IT-Pグループは、コンプライアンスマネジメントの一貫としてIT-Pグループ情報管理基本規程および、本ポリシーに基づき継続的に情報セキュリティ活動を実践する。

IT-Pグループの情報資産は、すべて価値ある重要な企業資産として認識する。これはIT-Pグループ共通の基本方針であり、その損傷、消失、悪用、不適切な利用から保護されなければならない。情報資産の保護は、すべての従業員等の責任である。IT-Pの情報資産を利用する者は、情報セキュリティの重要性を十分に認知し、この『情報セキュリティポリシー』遵守しなければならない。

(責任体制の構築)

第5条 IT-Pグループを統括した情報セキュリティ対策の最終責任は、IT担当役員が負う。

以降各章に規定する事項における責任は、事業部門においては関係グループ会社を統括して事業部門長が負い、管理部門においては同様に関係グループ会社を統括して各部長が負う。

IT-Pグループ各社においては、それぞれの社長が責任を負う。

また各章および関係規程に対する責任を明確にするため、必要に応じて役割と権限を定義し、組織毎に付与基準を設定する。

(関係規程の制定)

第6条　本ポリシーは、IT担当役員の責任において制定した。

IT担当役員は、本ポリシーに掲げる原則に従い、実施基準を定める。

IT部長は、日常のセキュリティ活動に必要な手順・手続等を定める。これら情報セキュリティ関係規程は、責任体制を通じ、その内容をすべての従業員等に周知する。

第2章 従業員等の責務

(私的利用の禁止)

第7条　すべての情報資産は、目的外利用および私的利用を禁止する。

(法令、マナーの遵守)

第8条　従業員等は、情報資産の利用にあたって関係法令を遵守するとともに、他人の権利侵害に注意しなければならない。

1 人権の保護

従業員等は、性別・年齢・出身地・国籍・人種・民族・信条・宗教・疾病・障害等による差別を行わないことを理解し、プライバシーの保護などあらゆる人権の保護に努めなければならない。また業務

上知り得た個人の情報について、差別的発言や誹謗中傷などの言論による暴力、電子メール内容を第三者に述べるなどによる秘密の暴露などを禁止する。

2 知的財産権の尊重

従業員等は、著作権・特許権・商標権などの知的財産権の尊重に留意しなければならない。著作物には、文章・写真・音楽・デザイン・プログラムなどが含まれ、権利者に無断で複製や配布などを行うことが禁じられている。またアイディアの盗用や勝手な改ざんについても許されていない。

3 インターネットの利用

インターネットは、全世界のネットワークを相互に接続した通信網であり、管理者が不在で、安全性が保証されていない。そのため、情報の漏洩や改ざん、コンピューターウイルスによる攻撃などの危険性を孕んでいる。
従業員等は、インターネットの危険性を認識したうえで、本ポリシーおよび関係規程に照らして、慎重かつ適切に利用しなければならない。

(ID、パスワード保護)

第9条　従業員等に配布されたID・パスワードは、成りすましによる情報の不正利用・漏洩などを防止するため、本人自身により厳重に管理しなければならない。
また、ID・パスワードの貸借は、いかなる場合においても厳禁とする。

第3章 電子化情報の取扱

(趣旨・目的)

第10条 電子化情報は、生成から利用・保存・廃棄の過程において、その機密性に応じて識別・分類され、適切に管理されなければならない。
特に営業秘密、個人情報、プライバシー情報などの取り扱いは、十分注意しなければならない。また、情報の機密性は、適宜見直されなければならない。

(実行責任)

第11条　部門長等は、自部門において利用する電子化情報を適切に管理する責任を負う。
部門長等は、本条の責任を全うするため、電子化情報取扱責任者を任命することができる。

第4章 アクセス権限管理

(趣旨・目的)

第12条 情報資産に対するアクセス権限は、情報の機密性と重要性に応じて設定されなければならず、また従業員等の業務上の役割に応じ適切に付与されなければならない。
なお、アカウントの発行にあたっては、従業員等としてあらかじめ証明され、本人であることが識別されていなければならない。

(実行責任)
第13条 部門長等は、情報資産に対するアクセス権限設定に係る責任を負う。
また、従業員等への情報資産に対するアクセス権の付与に係る責任を負う。
部門長等は、本条の責任を全うするため、アクセス権限設定責任者を任命することができる。

第5章 物理セキュリティ対策

(趣旨・目的)
第14条 情報資産は破壊や盗難、不正な利用などから物理的に保護され、機密性に応じて適切な対策が講じられなければならない。

(実行責任)
第15条 部門長等は、情報資産の保管や設置場所等に対する安全管理策を講じる責任を負う。

第6章 ネットワーク接続

(趣旨・目的)
第16条 情報資産は、ネットワークを介した非権限者からの不正侵入および情報の盗聴・漏洩・破壊・改ざんなどの脅威から保護され、適切な対策が講じられなければならない。

(実行責任)
第17条 IT部長は、IT-Pグループにおける全てのネットワークを統括する責任を負う。
また、不正なネットワークアクセスや情報の盗聴・漏洩・破壊・改ざんなどにより緊急対応が必要となる場合には、ネットワークの遮断等対策を講じなければならない。
IT部長は本条の責任を全うするために、ネットワーク統括担当者を任命することができる。

第18条 部門長等は、ネットワーク接続が必要となる場合、接続目的および必要な条件を明確にしたうえで、IT部長の指示に従わなければならない。

第7章 ソフトウェアライセンスの保護

(趣旨・目的)

第19条 ソフトウェアは、著作権およびその他の知的財産権に関する法律で保護されており、あらゆる権利侵害から排除された状態で、適切に利用されなければならない。

他者が権利を有するソフトウェアを利用する際には、権利者との間で締結された使用許諾契約等を遵守しなければならない。

(実行責任)

第20条 部門長等は、自部門にて利用するソフトウェアの適切な入手と利用に対する責任を負う。部門長等は、本条の責任を全うするため、ソフトウェア管理責任者を任命することができる。

第8章 コンピューターウイルス対策

(趣旨・目的)

第21条 情報資産は、コンピューターウイルス等の悪意あるソフトウェアから保護され、またIT-Pグループ以外の企業、団体、個人等に対し加害者とならないために、適切な対策が講じられなければならない。

(実行責任)

第22条 IT部長は、IT-Pグループのコンピューターウイルス対策を統括する責任を負う。

また、コンピューターウイルス感染により緊急対応が必要となる場合には、情報資産に対する利用制限を講じなければならない。

IT部長は本条の責任を全うするために、コンピューターウイルス対策統括担当者を任命することができる。

第23条 部門長等は、自部門のコンピューターウイルス対策の責任を負う。

部門長等は、本条の責任を全うするために、コンピューターウイルス対応部門責任者を任命し、自部門におけるコンピューターウイルス対策の適用および体制の整備、情報資産に対する対策の管理に当たらせることができる。

コンピューターウイルス対応部門責任者は、必要に応じて拠点事業所等にコンピューターウイルス対応責任者を配置し、コンピューターウイルス対策に関する適切な管理を行わなければならない。

第9章 外部委託

(趣旨・目的)

第24条　情報資産は、取り扱いを外部に委託する場合においても、本ポリシーおよび関係規程の定めるところにより適切に管理されなければならない。また、機密保持契約が締結されなければならない。

(実行責任)

第25条　部門長等は、外部委託先に対し、本ポリシーおよび関係規程に定める事項を遵守させる責任を負う。

第10章 教育

(趣旨・目的)

第26条　本ポリシーの目的を全うするため、IT-Pグループにおける情報セキュリティ水準の維持と向上に必要な教育・啓発活動は、定期的かつ継続的に実施されなければならない。

(実行責任)

第27条 部門長等は、従業員等に対し、情報セキュリティに関する教育、啓発を行う責任を負う。

第28条　IT部は、IT-Pグループにおける教育・啓発活動を推進するため、情報セキュリティに関するモラル向上と知識習得に必要な情報を提供する。

第11章 監査

第29条　本ポリシーに基づく情報セキュリティ対策の実施状況は、別途定められた規程等に基づき、担当役員が任命した監査権限を有するものによる内部監査の対象となる。

第12章 モニタリング

第30条　IT-Pグループでは、情報資産の不適切な利用、漏洩、盗難、改ざん、破壊等を検知するため、利用状況をモニタリングする。

第13章 罰則

第31条　本ポリシーに違反があったと認められる場合、各社就業規則ならびに関係内規等に基づき処罰の対象となる場合がある。

第14章 改廃

第32条　本ポリシーは、情報セキュリティを取り巻く環境変化に応じて、IT部が見直しを行い、担当役員の承認により改定される。

附則

本ポリシーは、2021年10月1日より適用開始とする。