情報セキュリティポリシー

2020年5月27日 策定
2021年5月28日 改定
株式会社ムジコ・クリエイト

変更履歴

改定日	変更箇所		変更前	変更後(追加)
2021/5/28	1-1	書類・媒体等の取扱いと保管(クリアデスクポリシー)	(1)重要度の高い書類や媒体を机上に放置してはならない。	(1)重要情報が含まれる書類や媒体を机上に放置してはならない。
2021/5/28	1-1	書類・媒体等の取扱いと保管(クリアデスクポリシー)	(2)業務上やむを得ず重要度の高い書類を机上に置く場合は、直接目に触れない状態にする。	(2)業務上やむを得ず重要情報が含まれる書類を机上に置く場合は、直接目に触れない状態にする。
2021/5/28	1-2	画面に表示する情報の管理(クリアスクリーンポリシー)	(1)重要度の高い情報を画面に表示している時に離席する場合は、不正な操作や盗み見を防止するため、画面・キーボードロック等の保護機能を使用しなければならない。	(1)重要情報が含まれる画面を表示している時に離席する場合は、不正な操作や盗み見を防止するため、画面・キーボードロック等の保護機能を使用しなければならない。
2021/5/28	2	重要情報の取扱いに関する標準 (情報の定義)	一般情報 : 公開情報	一般情報 : 限定公開、一般公開
2021/5/28	2	重要情報の取扱いに関する標準 (情報の定義)	追加	※ 具体的な内容については細則「1:情報の種類」を参照
2021/5/28	4	社内ネットワーク利用標準 (標準の名称変更)	社内ネットワーク利用標準	ネットワーク利用標準
2021/5/28	4	社内ネットワーク利用標準 (趣旨)	本標準は、機密保持及び情報資産の保護、有効活用を目的に社内ネットワークの利用管理を行う。	本標準は、機密保持及び情報資産の保護、有効活用を目的にネットワークの利用管理を行う。
2021/5/28	4-2	社内ネットワークへの接続時の注意事項	(2)会社所有の PC は、原則社外ネットワーク(ホテルや自宅の Wi-Fi、テザリングなど)へ接続してはならない。	削除
2021/5/28	4-3	社外ネットワークからのリモートアクセス	4-3 から 4-4 へ項番変更	ー
2021/5/28	4	項目追加	ー	3 社外ネットワークへの接続時の注意事項
2021/5/28	4-3	社外ネットワークへの接続時の注意事項	追加	(1)会社所有の PC を原則社外ネットワークに接続してはならない。

変更日	変更箇所		変更前	変更後(追加)
2021/5/28	4-3	社外ネットワークへの接続時の注意事項	追加	(2)会社所有の PC を業務上やむを得ず社外ネットワークに接続する場合は、安全性　が確保されたネットワークに接続しなければならない。 ※ 具体的な内容については細則「2:社外ネットワーク接続」を参照
2021/5/28	6-1	ウイルス対策ソフトの導入	(1)原則全てのサーバ、PC 及びモバイルデバイスにウイルス対策ソフトウェアを導入する。	(1)原則全てのサーバ、PC にウイルス対策ソフトを導入する。

情報セキュリティポリシー

○目的

当ポリシーは、情報セキュリティ対策の方針と規則を定めるものであり、当社が保有する情報資産を様々な脅威から守り、情報セキュリティ水準を維持・向上させることを目的とする。

○適用範囲

当社にかかわる全ての情報資産（情報や情報システム、及びこれらを保護、使用するのに必要なもの）を対象とする。

○適用者

当社の情報資産を利用する全ての者（役員、社員、契約等により当社の業務を実施する者）を対象とする。

○体制

情報セキュリティ対策の運用体制を確立し、維持及び改善を含めた活動を継続する。

○見直し

業務内容の変化や環境の変化等、必要に応じて情報セキュリティ対策を見直し、継続的な維持・改善に努める。

1　職場環境における情報セキュリティ標準

○趣旨

本標準は、職場環境における情報セキュリティリスクを低減し、情報漏洩等のセキュリティ事故を防止することを目的とする。

○遵守事項

1　書類・媒体等の取扱いと保管（クリアデスクポリシー）

(1)　重要情報が含まれる書類や媒体を机上に放置してはならない。

(2)　業務上やむを得ず重要情報が含まれる書類を机上に置く場合は、直接目に触れない状態にする。

2　画面に表示する情報の管理（クリアスクリーンポリシー）

(1) 重要情報が含まれる画面を表示している時に離席する場合は、不正な操作や盗み見を防止するため、画面・キーボードロック等の保護機能を使用しなければならない。

(2) スクリーンセーバーは必ず有効にし、起動するまでの時間は 10 分以内に設定する。

3　オフィスのゾーニング

(1) 情報漏洩防止の観点で、セキュリティレベル（情報資産の重要度）によってゾーンを明確に分け、セキュリティレベルに応じた対策を取らなければならない。

4　事務・通信機器の取扱い

(1) コピー機、FAX、プリンタ等に書類を放置してはならない。

(2) FAX 送信時には必ず宛先を確認し、誤送信を防止しなければならない。

2　重要情報の取扱いに関する標準

○趣旨

本標準は、社内の重要情報の取り扱い（保存・移動・破棄）において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。

○遵守事項

情報の定義　一般情報 ： 限定公開、一般公開
重要情報 ： 社外秘（個人情報含む）、関係者外秘
※ 具体的な内容については細則「1：情報の種類」を参照

1　重要情報の保存

(1) 権限を有しない者の不必要なアクセスを防ぐため、適切なアクセス権が設定されている場所に保存しなければならない。

2　重要情報の移動

(1) 原則電子メールで送信してはならない。『5-2　電子メールで送受信される情報の保護』を遵守すること。
(2) 原則外部記憶装置（USB メモリ、SD カード等）を使用し、社外に持ち出してはならない。

3　重要情報の破棄

(1) 使用目的が明らかで無い、もしくは使用目的が達成された情報は速やかに破棄しなければならない。
例　DM 用に一時的に保存した顧客情報　等
(2) 紙媒体についてはシュレッダーを利用する等、破棄後に第三者が利用できない措置をとらなければならない。

3　社内 PC における利用標準

○趣旨

本標準は、社内 PC の安全性を確保し、発生しうる問題を未然に防ぐことを目的とする。

○遵守事項

1　PC に導入するソフトウェア
(1) 原則業務に必要のないソフトウェアをインストールしてはならない。
(2) プリンタードライバー以外のソフトウェアは、IT 管理者の許可を得たうえでインストールしなければならない。

2　システム維持
(1) OS 及びインストールしたソフトウェアは、修正プログラム等を適用し、常に最新の状態で使用すること。
(2) PC 利用において異常を感じた場合は速やかに IT 管理者に報告しなければならない。

3　PC の利用の制限
(1) PC の利用者は、与えられたアカウントでログインしなければならない。

4　PC の利用者の変更
(1) PC の利用者は、PC の利用者を無断で変更してはならない。
(2) PC の利用者を変更する場合には、IT 管理者に届け出なければならない。

5　ウイルス対策の徹底
(1) PC の利用者は、PC を利用する上でウイルス対策を徹底しなければならない。
(2)『6 ウイルス対策標準』に規定されている遵守事項を徹底しなければならない。

6　PC に接続する機器の制限
(1) 会社が指定するもの以外の外部記憶装置は原則使用不可とする。
(2) 携帯電話、モバイルデバイスはその方法、目的を問わず接続不可とする。

7　PC及び外部記憶装置の廃棄等

（1）PC及び外部記憶装置を廃棄またはリース返却等する場合にはデータを完全に抹消するか、物理的に破壊しなければならない。

4　ネットワーク利用標準

○趣旨

本標準は、機密保持及び情報資産の保護、有効活用を目的にネットワークの利用管理を行う。

○遵守事項

1　接続機器
(1) 会社が許可していない機器を社内ネットワークに接続してはならない。

2　社内ネットワークへの接続時の注意事項
(1) ネットワーク利用者は、与えられた IP アドレス以外の IP アドレスを使用してはならない。

3　社外ネットワークへの接続時の注意事項
(1) 会社所有の PC を原則社外ネットワークに接続してはならない。
(2) 会社所有の PC を業務上やむを得ず社外ネットワークに接続する場合は、安全性が確保されたネットワークに接続しなければならない。
※ 具体的な内容については細則「2：社外ネットワーク接続」を参照

4　社外ネットワークからのリモートアクセス
(1) 社外ネットワークから社内ネットワークに接続されている機器へのリモートアクセスは原則許可しない。

5　電子メールサービス利用標準

○趣旨

本標準は、電子メールで受け渡される情報の安全性を確保し、電子メール利用にあたって発生しうる問題を未然に防ぐことを目的とする。

○遵守事項

1. 電子メールアカウントの管理について
   (1) 電子メールアカウントを業務目的以外で使用してはならない。
   (2) 電子メールアカウントを不正に利用されたと思われる場合は、『7 セキュリティインシデント報告・対応標準』に基づき対応しなければならない。

2. 電子メールで送受信される情報の保護
   (1) 電子メールの送信にあたっては、送信先のメールアドレスに間違いがないか、確認の上送信しなければならない。
   (2) 当社の事業に関わる情報、顧客、従業員のプライバシーに関わる情報などの重要情報は、原則として電子メールを用いて送信してはならない。

3. 電子メールを介してのウイルス被害の防止
   (1)『6-3　PC における電子メールやインターネット閲覧を介してのウイルス被害の防止』を遵守すること。

6 ウイルス対策標準

○趣旨

本標準は、ウイルスによって引き起こされる情報漏洩やシステム破壊の被害を未然に防ぐことを目的とする。

○遵守事項

1　ウイルス対策ソフトの導入
(1) 原則全てのサーバ、PC にウイルス対策ソフトを導入する。
(2) ウイルス対策ソフトは、会社が選定したソフトを導入し、定期的に見直しを実施する。

2　ウイルス対策ソフトの利用
(1) PCの利用者は、システム管理者が設定したウイルス対策ソフトの設定を変更してはならない。

3　PC における電子メールやインターネット閲覧を介してのウイルス被害の防止
(1) PCの利用者は、送信元不明（特にフリーメール）のメールに添付されたファイルや、実行形式のまま添付されたファイルなど、不審だと疑われるメールの添付ファイルは安易に開いてはならない。また、安易にURLリンクをクリックしてはならない。
(2) 電子メールサービスを利用中に、不審だと疑われるメールを受信したり、ウイルスの発見や、ウイルスと思われる症状を発見した場合は、『7 セキュリティインシデント報告・対応標準』に基づき対応しなければならない。
(3) インターネット閲覧によるウイルス感染を防ぐ為に、PCの利用者は安全ではないと思われるサイトを閲覧してはならない。また、安易にファイルをダウンロードしたりURL リンクをクリックしてはならない。

4　ウイルスに感染した場合、または感染したと疑われる場合
(1) PCの利用者は、ウイルスに感染した場合、または感染したと疑われる場合は、『7 セキュリティインシデント報告・対応標準』に基づき対応しなければならない。
(2) PCの利用者は、有線LAN接続のPCはネットワークケーブルを外し、無線LAN接続のPCは無線LAN機能をOFFにしなければならない。
(3) IT 管理者は情報セキュリティ部門の指示に従い、適切に対処しなければならない。

7 セキュリティインシデント報告・対応標準

○趣旨

本標準は、セキュリティインシデントが発生した場合及びセキュリティインシデントの発生と疑われる場合、適切な連絡経路を通じての報告、定められた手順に従った対応、情報システム環境の復旧がそれぞれ速やかになされることと、発生した事態から問題点や改善点などに対する学習を行い、継続的な再発防止が行われることを目的とする。
当社におけるセキュリティインシデントとは次のような事態を指す。

(1) セキュリティに対する侵害
　例　情報漏洩、ウイルス感染、DoS 攻撃、記録媒体等の紛失 等
(2) システム・ネットワークの故障・損壊
　例 電源異常、自然災害による機器損壊 等
(3) 情報資産への脅威
　例 建物への侵入　等

○遵守事項

経営者の同意・承認の元、未然に防げなかった事態が発生した際に、事態の可及的速やかな収拾と被害や影響範囲を最小にするために、平時の準備と、組織・役割・責任の明確化、伝達方法・事態の評価と対応及び再発防止を含む学習についての取り組みを明確にする。

1　平時の準備
　セキュリティインシデントが発生した場合、あるいは発生が疑われる場合は情報セキュリティ部門に遅滞なく報告がなされ、速やかにセキュリティインシデントの分析、封じ込め、原因の根絶、復旧が可能となるよう、2項以降に示す対応について以下の準備作業を行い、関係者への周知を徹底する。
　(1) 情報セキュリティ部門は、想定するセキュリティインシデントの具体的な対応手順を策定する。
　(2) 情報セキュリティ部門は、策定した対応手順でセキュリティインシデントに対応可能となるよう、定期的に訓練を行い、併せて対応手順に問題がないか確認を行い、対応手順に問題があれば是正する。
　(3) 情報セキュリティ部門は、セキュリティインシデントの検知に必要な情報セキュリティ対策を導入し、情報セキュリティマネジメントを遂行しなければならない。

(4) 情報セキュリティ部門は、各システムの復旧優先度を決定しなければならない。復旧優先度の決定は、対象システムにおいて運用される業務の停止許容時間を観点において行う。(表1参照)

表1

復旧優先度	業務復旧までの許容時間
3	業務が停止することは許されない
2	24 時間以内に復旧しなければならない
1	インシデント発生時は停止してもよい

2　事象の検知、報告

セキュリティインシデント、あるいは発生が疑われる事象を検知したものは、情報セキュリティ部門に遅滞なく報告しなければならない。

3　分析

情報セキュリティ部門は、報告されたセキュリティインシデントに応じ、策定した対応手順に従い、被害の特定、原因の分析を行う。なお、策定した対応手順に該当しないセキュリティインシデントの場合、情報セキュリティ部門は、そのための実行責任者を任命し、対応組織を始動し、被害の特定、原因の分析を行う。

4　封じ込め、根絶、復旧

特定したセキュリティインシデントの原因に基づく対応手順に則り、被害の拡散を防止し、被害箇所の原因の根絶、修復を行い、復旧をする。

5　情報の収集、管理、記録

セキュリティインシデントに関する情報は、実行責任者のもと、以下の情報について一元的に収集、管理、記録する。

- セキュリティインシデントの発生状況及び対応状況に関する情報
- 顧客及び取引先等利害関係者の影響等に関する情報

6　インシデントの再発防止

セキュリティインシデントの対応後、同様のセキュリティインシデントの再発防止、および対応手順の不備等について改善を行う。

(1) セキュリティインシデントへの対応が完了した後、情報セキュリティ部門は、調査結果をもとに再発防止計画を作成しなければならない。再発防止計画作成時には、技術的側面と組織的側面の両方に留意する。

(2) 情報セキュリティ部門は発生したインシデントのうち、以下の要件を満たすものについては、再発防止計画と共に取締役会に報告しなければならない。

- セキュリティ侵害により当社が被害者となる場合
- 顧客や取引先等の社外に対して当社が加害者となる場合

(3) 再発防止計画は、当セキュリティポリシーが適用される全ての者に周知され、適切に実施されなければならない。

(4) 情報セキュリティ部門は、セキュリティインシデントの発生から再発防止計画作成までの一連の管理した記録から、対応手順の不備、または良かった点を整理し、対応手順を改善しなければならない。また、一連の記録を保管、管理しなければならない。