文書番号	
制定日	
改訂日	
改訂版数	1

個人情報保護
基本規程

承　認	作　成

株式会社〇〇〇〇〇
東京都〇〇区〇〇
電話　03-0000-0000

個人情報保護基本規程	文書番号	
	改訂版数	1

目次

0. 目的 . . . 1
1. 適用範囲 . . . 1
2. 適用基準 . . . 1
A. 3 管理目的及び管理策 . . . 3
A. 3. 1 一般 . . . 3
A. 3. 2 個人情報保護方針 . . . 3
A. 3. 2. 1 内部向け個人情報保護方針 . . . 3
A. 3. 2. 2 外部向け個人情報保護方針 . . . 3
A. 3. 3 計画 . . . 4
A. 3. 3. 1 個人情報の特定 . . . 4
A. 3. 3. 2 法令、国が定める指針その他の規範 . . . 4
A. 3. 3. 3 リスクアセスメント及びリスク対策 . . . 5
A. 3. 3. 4 資源、役割、責任及び権限 . . . 6
A. 3. 3. 5 内部規程 . . . 8
A. 3. 3. 6 計画策定 . . . 9
A. 3. 3. 7 緊急事態への準備 . . . 9
A. 3. 4 実施及び運用 . . . 11
A.3. 4. 1 運用手順 . . . 11
A. 3. 4. 2 取得・利用及び提供に関する原則 . . . 11
A. 3. 4. 2. 1 利用目的の特定 . . . 11
A. 3. 4. 2. 2 適正な取得 . . . 11
A. 3. 4. 2. 3 要配慮個人情報 . . . 12
A. 3. 4. 2. 4 個人情報を取得した場合の措置 . . . 12
A. 3. 4. 2. 5 A. 3. 4. 2. 4のうち本人から直接書面によって取得する場合の措置 13
A. 3. 4. 2. 6 利用に関する措置 . . . 14
A. 3. 4. 2. 7 本人に連絡又は接触する場合の措置 . . . 14
A. 3. 4. 2. 8 個人データの提供に関する措置 . . . 15
A. 3. 4. 3 適正管理 . . . 18
A. 3. 4. 3. 1 正確性の確保 . . . 18
A. 3. 4. 3. 2 安全管理措置 . . . 18
A. 3. 4. 3. 3 従業者の監督 . . . 18
A. 3. 4. 3. 4 委託先の監督 . . . 19
A. 3. 4. 4 個人情報に関する本人の権利 . . . 20
A. 3. 4. 4. 1 個人情報に関する権利 . . . 20
A. 3. 4. 4. 2 開示等の請求等に応じる手続 . . . 20
A. 3. 4. 4. 3 保有個人データに関する周知など . . . 21

A. 3. 4. 4. 4 保有個人データの利用目的の通知 21
A. 3. 4. 4. 5 保有個人データの開示 22
A. 3. 4. 4. 6 保有個人データの訂正、追加又は削除 22
A. 3. 4. 4. 7 保有個人データの利用又は提供の拒否権 23
A. 3. 4. 5 認識 23
A. 3. 5 文書化した情報 24
A. 3. 5. 1 文書化した情報の範囲 24
A. 3. 5. 2 文書化した情報の管理(記録は除く):文書管理 25
A. 3. 5. 3 文書化した情報のうち記録の管理 25
A. 3. 6 苦情及び相談への対応 26
A. 3. 7 パフォーマンス評価 27
A. 3. 7. 1 運用の確認 27
A. 3. 7. 2 内部監査 27
A. 3. 7. 3 マネジメントレビュー 28
A. 3. 8 是正処置 29
改訂歴表 30

個人情報保護基本規程	文書番号	
	改訂版数	1

0. 目的

本規程は、株式会社〇〇〇〇〇(以下、当社という)の個人情報保護に関する取組み及び考え方ならびに遵守すべき事項を JIS Q 15001(個人情報保護マネジメントシステム-要求事項)に基づき規定したものです。

本規程は、当社の個人情報保護に関する管理レベルの維持・向上、本人への安心感の提供と満足度の向上を図ることを目的とします。

1. 適用範囲

(1) 当社の個人情報保護マネジメントシステムは、当社の事業の従事する全ての従業者(役員、監査役、正社員、派遣社員、契約社員、嘱託社員、パート社員、アルバイト社員等)を対象とします。

(2) 当社の個人情報保護マネジメントシステムは、当社の事業の用に供する全ての個人情報に適用します。

2. 適用基準

当個人情報保護基本規程は、当社における個人情報保護を規定する最高位の文書であって、以下の基準の要求事項を適用し作成しました。

当個人情報保護基本規程および関連文書は、基準が改訂された場合、あるいはより信頼性を高めるために、必要な場合に改訂します。

適用基準

JISQ15001:2017(個人情報保護マネジメントシステム—要求事項)

プライバシーマーク付与適格性審査基準(プライバシーマーク推進センター)

3. 用語及び定義

(1)「個人情報保護基本規定」で使用する用語は、以下の基準に準拠します。

JISQ15001:2017(3 用語及び定義)

(2)主な用語の定義

個人情報 (個人情報保護法の定義)	生存する個人に関する情報であって、以下のいずれかに該当するもの。 ・当該情報に含まれる氏名、生年月日その他の記述等によって特定の個人を識別できるもの(他の情報と容易に照合することができ、それによって特定の個人を識別することができることとなるものを含む)。 ・個人識別符号が含まれるもの。
個人番号	番号法の規定により、住民票コードを変換して得られる番号であって、当該住民票コードが記載された住民票に係る者を識別するために指定されるものをいう。
特定個人情報	個人番号をその内容に含む個人情報をいう。
本人	個人情報によって識別される特定の個人。
組織	責任及び権限を持つトップマネジメントが存在し、自らの目的を達成するため、責任、権限及び相互関係を伴う独自の機能をもつ、個人又は人々の集まり。
個人情報保護管理者	トップマネジメントによって組織内部に属する者の中から指名された者であって、個人情報保護マネジメントシステムの計画及び運用に関する責任及び権限をもつ者。
個人情報保護監査責任者	トップマネジメントによって組織内部に属する者の中から指名された者であって、公平かつ客観的な立場にあり、監査の実施及び報告を行う責任及び権限をもつ者。
従業者	個人情報取扱事業者の組織内にあって直接間接に組織の指揮監督を受けて組織の業務に従事している者などをいい、雇用関係にある従業員(正社員、契約社員、嘱託社員、パート社員、アルバイト社員など)だけでなく、雇用関係にない従事者(取締役、執行役、理事、監査役、監事、派遣社員など)も含まれる。
個人情報保護リスク	個人情報の取扱いの各局面(個人情報の取得・入力、移送・通信、利用・加工、保管・バックアップ、消去・廃棄に至る個人情報の取扱いの一連の流れ)における、個人情報の漏えい、滅失又はき損、関連する法令、国が定める指針その他の規範に対する違反、想定される経済的不利益及び社会的な信用の失墜、本人の権利利益の侵害など、好ましくない影響。
個人情報保護マネジメントシステム(PMS)	事業者が、自らの事業の用に供する個人情報について、その有用性に配慮しつつ、個人の権利利益を保護するための方針、体制、計画、実施、点検及び見直しを含むマネジメントシステム。
個人番号関係事務	番号法に規定される個人番号の利用範囲(税・社会保障及び災害対策)に関して、行われる他人の個人番号を必要な限度で利用して行う事務。
個人番号関係事務実施者	個人番号関係事務を処理する者及び個人番号関係事務の全部又は一部の委託をうけた者。
要配慮個人情報	本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の

	不利益が生じないように、その取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報。
匿名加工情報	特定の個人を識別することができないように個人情報を加工して得られる個人に関する情報であって、当該個人情報を復元することができ ないようにしたもの。
適合	要求事項を満たしていること。
不適合	要求事項を満たしていないこと。

A. 3 管理目的及び管理策

A. 3. 1 一般

当社は、JISQ15001 の個人情報保護マネジメントシステム要求事項、「附属書 A 管理目的及び管理策」に基づく個人情報保護マネジメントシステムを確立し、実施し、維持し、かつ、改善します。

当社の個人情報保護マネジメントシステムに関して、この個人情報保護基本規程の A. 3. 2から A. 3. 8に記載します。

A. 3. 2から A. 3. 8の管理策は、トップマネジメントによって権限を与えられた者の承認を得た上で規定すると共に実行いたします。

A. 3. 2 個人情報保護方針

A. 3. 2. 1 内部向け個人情報保護方針

トップマネジメントは、内部向け個人情報保護方針を策定し、文書化します。

内部向け個人情報保護方針は次の事項を満たす内容とします。

a）事業の内容及び規模を考慮して適切な個人情報の取得，利用及び提供に関すること[特定された利用目的の達成に必要な範囲を超えた個人情報の取扱い(以下、“目的外利用”という)を行わないこと及びそのための措置を講じることも含みます。

b）個人情報に関する法令及び国が定める指針及びその他の規範を遵守すること。

c）個人情報の漏えい、滅失又はき損の防止、及び是正に関すること。

d）苦情及び相談への対応に関すること。

e）個人情報保護マネジメントシステムの継続的改善に関すること。

f）トップマネジメントの氏名。

内部向け個人情報保護方針は、イントラネットに掲示すると共に、個人情報保護教育を通して周知徹底を図ります。

また、内部向け個人情報保護方針は当社ホームページに掲載して、利害関係者に公開します。その際は、ホームページのトップページより参照できるようにします。

A. 3. 2. 2 外部向け個人情報保護方針

トップマネジメントは、外部向け個人情報保護方針を策定し、文書化します。

外部向け個人情報保護方針は、A. 3. 2. 1で策定した内部向け個人情報保護方針の内容に加え、次の事項を満たす内容とします。

a） 制定年月日及び最終改正年月日

b) 外部向け個人情報保護方針の内容についての問合わせ先

外部向け個人情報保護方針は当社ホームページに掲載して、一般公開します。その際は、ホームページのトップページより参照できるようにします。

A. 3. 3 計画

A. 3. 3. 1 個人情報の特定

当社の事業の用に供する全ての個人情報を、以下の手順に従って特定します。

(1)部門の責任者が「個人情報管理台帳」を作成し、対象となる個人情報を特定します。「個人情報管理台帳は」個人情報保護管理者が承認します。

(2)「個人情報管理台帳」は、以下の内容を含めて作成します。

①個人情報の名称(項目)
②個人番号の有無
③利用目的
④保管場所
⑤保管方法
⑥アクセス権を有する者
⑦利用期限
⑧保管期限

(3)「個人情報管理台帳」の見直しと修正は、年1回(4月)、適宜に部門の責任者が行い、個人情報保護管理者が承認し、最新の状態を維持します。

(4)その他、新規の種類の個人情報の取り扱いが発生した場合などには、個人情報を特定し、「個人情報管理台帳」を更新します。

関連帳票:02.個人情報管理台帳

A. 3. 3. 2 法令、国が定める指針その他の規範

個人情報の取り扱いに関する法令、国が定める指針その他の規範を、以下の手順に従って、特定します。

1. 法令、国が定める指針その他の規範の特定

(1)個人情報保護管理者は、個人情報の取り扱いに関する法令、国が定める指針その他の規範を特定し「個人情報の取扱いに関する法令、指針及び規範の一覧表」に登録し、承認します。

(2)一覧表には、公布年月日、最終改正日、ホームページURL等を記載し、参照と改訂状況が明確になるようにします。

2. 法令、国が定める指針その他の規範の見直し

(1)個人情報保護管理者は、年1回(4月)に、特定した法令、国が定める指針その他の規範に関する最新情報をインターネットなどで確認し、改訂の有無を確認します。

（2）改訂が当社に関係する場合には、「個人情報の取扱いに関する法令、指針及び規範の一覧表」を修正し、承認します。

3．法令、国が定める指針その他の規範の参照

「個人情報の取扱いに関する法令、指針及び規範の一覧表」は、社内イントラネットに掲載し、いつでも閲覧できるようにします。

関連帳票：27. 個人情報の取扱いに関する法令、指針及び規範の一覧表

A．3．3．3 リスクアセスメント及びリスク対策

A．3．3．1によって特定した個人情報について、目的外利用を行わない為に、必要な対策を講じる手順を確立し、かつ、維持します。

個人情報保護管理者は、A．3．3．1によって特定した個人情報について、その取扱いの各局面（取得・入力、移送・送信、利用・加工、保管・バックアップ、消去・廃棄）における個人情報保護リスク（個人情報の漏えい、滅失又はき損、関連する法令、国が定める指針その他の規範に対する違反、想定される経済的な不利益及び社会的な信用の失墜、本人への影響などのおそれ）を特定し、分析し、必要な対策を講じるための手順を策定し、実施します。

1．個人情報保護リスクの洗い出しと分析、対応策の検討

（1）「個人情報管理台帳」に登録された個人情報について、取扱い方法や保管方法などが同じ個人情報を分類します。

（2）分類ごと及びライフサイクルごとに個人情報保護リスクを特定します。

（3）特定された個人情報保護リスクに対してリスク分析を行います。

（4）個人情報保護リスクが想定される項目については、そのリスクに応じた対策を検討し、社長の承認を得た上で実施します。

また、実施する対策は、関連する規程などに反映させます。

（5）費用や技術的な理由等で、十分な対策が行えない個人情報保護リスクについては、残留リスクとして把握し、社長の承認を得ます。

（6）リスク分析の結果は、「リスク分析表」に記載します。

2．個人情報保護リスクの特定と分析、対応策の見直し

（1）リスク分析表の定期的な見直しを、年1回（4月）、適宜に行います。

（2）定期的な見直し以外に、次のような場合は随時見直しを行います。

（a）個人情報の特定漏れに気付き、「個人情報管理台帳」に登録したとき。

（b）新しい種類の個人情報の取り扱いが発生し、「個人情報管理台帳」に登録したとき。

（c）個人情報のライフサイクルや取り扱い方法等に変化があったとき。

（d）事業内容や組織、事業所等の変化に伴い、個人情報のライフサイクル、取扱い方法或いは個人情報保護リスク等に変化があったとき。

関連帳票：03.リスク分析表