個人情報管理　基本規程

Ver.20170401

制定日：2017 年 4 月 1 日

株式会社ネクストページ

承認(社長)	審査(個人情報管理責任者)	作成

目　　次

改訂履歴

年月日	改訂内容
平成 29 年 4 月 1 日	制定初版

Ⅰ　総則

１．目的

本規程は、当社としての個人情報保護の実現ための、コンプライアンス・プログラムを規定することを目的とする。本文書から他の規程・文書を参照し、これらもコンプライアンス・プログラムを実現する文書の一部とする。
コンプライアンス・プログラムの目的は、個人情報保護の方針の作成、方針に基づく計画、計画にもとづく実施、監査、見直しをスパイラル的に継続することによって、当社の個人情報に関する管理能力を高めていくことである。

２．適用範囲

（１）　対象組織：全社（当社に勤務する社員、準社員、契約社員、派遣社員、パートおよびアルバイトを含む）／全業務

（２）　対象となる個人情報：全部もしくは一部を電子計算機などの自動処理システムによって処理している、又は自動処理による処理を行うことを目的して書面などによって処理している個人情報だけでなく、何らかの規則により索引付けされた個人情報であれば、媒体に関係なく含む。具体的には、「個人情報管理台帳兼保管一覧」に定めた個人情報とする。

３．引用規格

個人情報保護に関するコンプライアンス・プログラムの要求事項（JIS Q 15001）：2006

Ⅱ．用語の定義

本規程では、原則としてJIS Q 15001で規定された用語を用いるものとする。ただし、当社として別の用語を用いる場合には、以下の対応表に定義するものとする。

当社の用語	JISQ15001での用語	定　義
コンプライアンス・プログラム	コンプライアンス・プログラム	当社が自ら保有する個人情報を保護するための、方針、組織、計画、実施、監査及び見直しを含むマネジメントシステム
個人情報	個人情報	個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述、又は個人別に付けられた番号、記号その他の符号、画像若しくは音声によって当該個人を識別できるもの（当該情報だけでは識別できないが、他の情報と容易に照合することができ、それによって当該個人を識別できるものを含む)。
情報主体	情報主体	一定の情報によって識別される、又は識別され得る個人。
当社	事業者	事業を営む法人、その他の団体又は個人。当コンプライアンス・プログラムの適用範囲。
経営者・社長	事業者の代表者	事業者の代表者。当社の代表取締役社長。
従業員	従業員	社員だけでなく、契約社員、派遣社員、パート、アルバイト、嘱託等を含む。
個人情報管理責任者	管理者	当社の内部において代表者によって指名された、コンプラインアンス・プログラムの実施及び運用に関する、独立した責任と権限を持つ者。
内部監査責任者	監査責任者	当社の代表者によって指名された、公平、かつ客観的な立場で、監査の実施及び報告を行う権限を持つ者。
受領者	受領者	個人情報の提供を受ける法人、その他の団体または個人。
情報主体の同意	情報主体の同意	情報主体が、収集、利用又は提供に関する情報を与えられた上で、自己に関する個人情報の収集、利用又は提供について承諾する意思表示。情報主体が子供の場合は、保護者の同意も得るべきである。
収集目的	収集目的	個人情報の利用及び提供の範囲で、情報主体の同意の対象となるもの。
利用	利用	当社が当社内で個人情報を処理すること。
提供	提供	当社が、当社外のものに自ら保有する個人情報を利用可能にすること。
預託	預託	当社が、当社外のものに情報処理を委託するなどのために、自ら保有する個人情報を預けること。

Ⅲ. コンプライアンス・プログラム要求事項

当社は JIS Q 15001 に準拠したコンプライアンス・プログラムを以下のとおり定め、これを遵守する。

4.1　　一般要求事項（目的）

当社は、JIS Q 15001 に準拠したコンプライアンス･プログラム（ＣＰ）を策定し、実施し、維持し、及び改善する。その内容は、この 4・全体で規定する。

4.2　　個人情報保護方針

経営者は、次の事項を含む個人情報保護方針を定めるとともに、これを実行し維持する。経営者は、この方針を文書化し、役員及び従業員に周知させるとともに一般の人が入手可能な措置を講ずる。

a) 事業の内容及び規模を考慮した適切な個人情報の収集、利用及び提供に関すること。

b) 個人情報への不正アクセス、個人情報の紛失、破壊、改ざん及び漏えいなどの予防並びに是正に関すること。

c) 個人情報に関する法令及びその他の規範を遵守すること。

d) コンプライアンス･プログラムの継続的改善に関すること。

当社の個人情報保護方針は以下とおりとする。

個人情報保護方針

１．個人情報の利用目的を特定し、公正かつ適正に取得、利用および委託・提供を行います
２．個人情報への不正アクセス、個人情報の紛失・破壊・改ざん・漏洩等を予防するため、これらのリスクに対して合理的な安全対策を講じるとともに、これらの問題が発生した場合は遅滞なく是正措置を講じます
３．個人情報の保護に関する法令その他の規範を遵守し、個人情報の保護に努めます
４．個人情報保護に関する社内規程を定め、体制を構築・維持するとともに、その継続的な改善に努めます
５．当社の保有する個人情報について、本人から開示・訂正・利用停止等の求めや、苦情・問い合わせがあった場合には、適正に対応します
６．顧客企業から個人情報を取扱う業務を受託する場合には、受託した業務範囲内で個人情報を取り扱います

平成 29 年 4 月 1 日
株式会社ネクストページ
代表取締役　寺澤　晃

当社における個人情報の利用業務について
当社は顧客企業から次のような受託業務において個人情報を取り扱います

- 名簿の印刷、発送
- ダイレクトメールの印刷、発送
- ホームページの運営、会員管理
- 名刺の印刷、発送
- IT コンサルティング業務
- その他個人情報の加工、印刷、発送に関わる業務

個人情報保護方針の外部伝達
ａ）本方針は全社員に周知徹底させるとともに、当社ホームページ上に公表する。

4.3 計画

4.3.1 個人情報の特定

当社は、自ら保有するすべての個人情報を特定するための手順を確立し、維持する。当社は、特定した個人情報に関するリスク(個人情報への不正アクセス、個人情報の紛失、破壊、改ざん及び漏えい）を認識する。

関連規程：個人情報管理　実施細則

4.3.2 法令及びその他の規範

当社は、個人情報に関する法令及びその他の規範を特定し、参照できる手順を確立し、維持する。

関連規程：個人情報管理　実施細則

4.3.3 内部規程

当社は、個人情報を保護するための内部規程を策定し、維持する。内部規程には、次の事項を含まなければならない。

a) 当社の各部門及び階層における個人情報を保護するための権限及び責任の規定。

関連規程：個人情報管理　実施細則

b) 個人情報の収集、利用、提供及び管理の規定。

関連規程：個人情報管理　実施細則／安全対策細則

c) 情報主体からの個人情報に関する開示、訂正及び削除の規定。

関連規程：個人情報管理　実施細則

d) 個人情報保護に関する教育の規定。

関連規程：個人情報管理　実施細則

e) 個人情報保護に関する監査の規定。

関連規程：内部監査細則

f) 内部規程の違反に関する罰則の規定。

本規程に反したものは、就業規則第 38 条、パートタイマー就業規則第 15 条にもとづいて懲戒する。

関連規程：就業規則／パートタイマー就業規則

当社は、事業の内容に応じて、コンプライアンス･プログラムが確実に適用されるように内部規程を改定する。

4.3.4 計画書

当社は、内部規程を遵守するために必要な教育、監査などの計画を立案し、文書化し、かつ、維持する。

関連規程：個人情報管理　実施細則

関連規程：内部監査細則

4.4 実施及び運用

4.4.1 体制及び責任

当社はコンプライアンス･プログラムを効果的に実施するために役割、責任及び権限を定め、文書化し、かつ、個人情報に関連のある業務にかかわる役員及び従業員に周知する。経営者は、コンプライアンス･プログラムの実施及び管理に不可欠な資源を用意する。経営者は、この規格の内容を理解し実践する能力のある管理者を当社の内部から指名し、コンプライアンス･プログラムの実施及び運用に関する責任及び権限を他の責任にかかわりなく与え、業務を行わせる。

関連規程：個人情報管理　実施細則

4.4.2 個人情報の収集に関する措置

関連規程：個人情報管理　実施細則

4.4.2.1 収集の原則

個人情報の収集は、収集目的を明確に定め、その目的の達成に必要な限度において行わなければならない。

4.4.2.2 収集方法の制限

個人情報の収集は、適法、かつ、公正な手段によって行わなければならない。

4.4.2.3 特定の機微な個人情報の収集の禁止

次に示す内容を含む個人情報の収集、利用又は提供は行ってはならない。ただし、これらの収集、利用又は提供について、明示的な情報主体の同意、法令に特別の規定がある場合、及び司法手続上必要不可欠である場合は、この限りではない。

a) 思想、信条及び宗教に関する事項

b) 人種、民族、門地、本籍地（所在都道府県に関する情報を除く。）、身体・精神障害、犯罪歴、その他の社会的差別の原因となる事項。

c) 勤労者の団結権、団体交渉及びその他団体行動の行為に関する事項。

d) 集団示唆行為への参加、請願権の行使、及びその他の政治的権利の行使に関する事項。
e) 保健医療及び性生活。

4.4.2.4 情報主体から直接収集する場合の措置

情報主体から直接に個人情報を収集する場合には、情報主体に対して、少なくとも、次に示す事項又はそれと同等以上の内容の事項を書面若しくはこれに代わる方法によって通知し、情報主体の同意を得る。

a) 当社の内部の個人情報に関する管理者又はその代理人の氏名若しくは職名、及び所属並びに連絡先。
b) 収集目的
c) 個人情報の提供を行うことが予定される場合には、その目的、当該情報の受領者又は受領者の組織の種類、属性及び個人情報の取扱いに関する契約の有無。
d) 個人情報の預託を行うことが予定される場合には、その旨。
e) 情報主体が個人情報を与えることの任意性及び当該情報を与えなかった場合に情報主体に生じる結果。
f) 個人情報の開示を求める権利、及び開示の結果、当該情報が誤っている場合に訂正又は削除を要求する権利の存在、並びに当該権利を行使するための具体的な方法。

4.4.2.5 情報主体以外から間接的に収集する場合の措置

情報主体以外から間接的に個人情報を収集する場合には、情報主体に対して、少なくとも、4.4.2.4 の a)～d)及び f)に示す事項を書面又はこれに代わる方法によって通知し、情報主体の同意を得なければならない。ただし、次に示すいずれかに該当する場合は、この限りでない。

a) 情報主体からの個人情報の収集時に、あらかじめ自己への情報の提供を予定している旨 4.4.2.4 の c)に従い情報主体の同意を得ている提供者から収集を行う場合。
b) 情報処理を委託するなどのために個人情報を預託される場合。
c) 情報主体の保護に値する利益が侵害されるおそれのない収集を行う場合。ただし、c）による収集は当社にはない。

4.4.3 個人情報の利用及び提供に関する措置

関連規程：個人情報管理　実施細則

4.4.3.1 利用及び提供の原則

個人情報の利用及び提供は、情報主体が同意を与えた収集目的の範囲内で行わなければならない。なお、次に示すいずれかに該当する場合は、情報主体の同意を必要としない。

a) 法令の規定による場合。

b) 情報主体及び、又は公衆の生命、健康、財産などの重大な利益を保護するために必要な場合。

4.4.3.2 収集目的の範囲外の利用及び提供の場合の措置

情報主体が同意を与えた収集目的の範囲外で個人情報の利用及び提供を行う場合は、少なくとも、4.4.2.4 の a)～d)及び f)に示す事項を書面又はこれに代わる方法によって情報主体に通知し、事前の情報主体の同意の下に行う。

4.4.4 個人情報の適正管理義務

4.4.4.1 個人情報の正確性の確保

個人情報は、収集目的に応じ必要な範囲内において、正確、かつ、最新の状態で管理する。

関連規程：個人情報管理　実施細則

4.4.4.2 個人情報の利用の安全性の確保

個人情報に関するリスク（個人情報への不正アクセス、個人情報の紛失、破壊、改ざん及び漏えいなど）に対して、合理的な安全対策を講ずる。

関連規程：個人情報管理　実施細則／安全対策細則

4.4.4.3 個人情報の委託処理に関する措置

当社が、情報処理を委託するなどのために個人情報を預託する場合は、十分な個人情報の保護水準を満たしている者を選定する基準を確立しなければならない。また、契約によって、次に示す内容を規定し、その保護水準を担保する。

a) 個人情報に関する秘密保持。

b) 再委託に関する事項について。

c) 事故時の責任分担。

d) 契約終了時の個人情報の返却及び消去。

当該契約書などの書面又はこれに代わる記録を、個人情報の保有期間にわたって保存する。

関連規程：個人情報管理　実施細則

4.4.5 個人情報に関する情報主体の権利

関連規程：個人情報管理　実施細則

4.4.5.1 個人情報に関する権利

情報主体から自己の情報について開示を求められた場合は、合理的な期間内にこれに応じなければならない。また、開示の結果、誤った情報があり、訂正又は削除を求められた場合は、合理的な期間内にこれに応じるとともに、訂正又は削除を行った場合は、可能な範囲内で当該個人情報の受領者に対して通知を行う。

4.4.5.2 個人情報の利用又は提供の拒否権

当社が保有している個人情報について、情報主体から自己の情報についての利用又は第三者への提供を拒まれた場合には、これに応ずる。

4.4.6 教育

当社は、役員及び従業員に、適切な教育を行わなければならない。当社は、関連する各部門及び階層においてその従業員に、次の事項を自覚させる手順を確立し維持しなければならない。

a) コンプライアンス･プログラムに適合することの重要性及び利点。

b) コンプライアンス･プログラムに適合するための役割及び責任。

c) コンプライアンス･プログラムに違反した際に予想される結果。

4.4.7 苦情及び相談

当社は、個人情報及びコンプライアンス･プログラムに関して、情報主体からの苦情及び相談を受け付けて対応する。

関連規程：個人情報管理　実施細則

4.4.8 コンプライアンス･プログラム文書

当社は、コンプライアンス･プログラムの基本となる要素を本規程に記述するとともに、「附則：コンプライアンス・プログラム文書体系」に文書体系の概要を記述する。

4.4.9 文書管理

当社は、この規程が要求するすべての文書を管理する。

関連規程：個人情報管理　実施細則

4.5 監査

当社は、当社のコンプライアンス･プログラムが、JISQ１５００１の規格要求事項を満たしていることおよびその運用状況を確認するために、定期的に監査する。内部監査責任者は、

監査を指揮し、監査報告書を作成し、経営者に報告する。当社は、監査報告書を管理し、保管する。

関連規程：内部監査細則

4.6 事業者の代表者による見直し

経営者は、監査報告書及びその他の経営環境などに照らして、適切な個人情報の保護を維持するために、定期的にコンプライアンス･プログラムを見直す。

関連規程：個人情報管理　実施細則

附則：コンプライアンス・プログラム文書体系概要図

個人情報管理　実施細則

Ver.20190401

制定日：平成 29 年 4 月 1 日

株式会社ネクストページ

承認(社長)	審査(個人情報管理責任者)	作成

目　　次

改訂履歴表

年月日	改訂内容
平成 29 年 4 月 1 日	制定初版

Ⅰ　総則

１．目的

本細則は、「個人情報管理基本規程」を受け、当社としての個人情報保護の実現のための実務的ルールを規定することを目的とする。必要に応じて、本細則から他の細則・文書を参照し、これらもコンプライアンス･プログラムを実現する文書の一部とする。

２．適用範囲

（１）　対象組織：全社（当社に勤務する社員、準社員、契約社員、派遣社員、パートおよびアルバイトを含む）／全業務

（２）　対象となる個人情報：全部もしくは一部を電子計算機などの自動処理システムによって処理している、又は自動処理による処理を行うことを目的して書面などによって処理している個人情報だけでなく、何らかの規則により索引付けされた個人情報であれば、媒体に関係なく含む。具体的には、「個人情報管理台帳兼保管一覧」に定めた個人情報とする。

３．用語の定義

（１）　従業員

当社に勤務する社員、準社員、契約社員、派遣社員、パートおよびアルバイトを含む。

Ⅱ　体制および責任

１．体制

（１）　当社における個人情報保護に関する最高責任者は、代表取締役社長とする。

（２）　代表取締役社長は、個人情報管理責任者および内部監査責任者を以下の通り任命する。

個人情報管理責任者は、可能な限り取締役とし、内部監査責任者と兼務してはならない。

（３）　個人情報管理責任者は、部門毎にコンプライアンス･プログラムの部門個人情報管理者を指名する。

（４）　詳細については、「個人情報保護のための体制図」に定める。

２．責任および権限

（１）　経営者（代表取締役社長）の責任および権限

① 個人情報保護方針を設定し従業員へ周知徹底する。

② 個人情報の保護に関するコンプライアンス事項を全従業員に周知徹底する。

③ JISQ15001 の規格内容を理解し実践する能力を持つ管理者（個人情報管理責任者）を社内から任命し、コンプライアンス･プログラムの実施及び運用に関する責任および権限を他の責任にかわりなく付与する。

④ 内部監査責任者を社内から任命し、監査を実施する上で必要な責任および権限を付与する。

⑤ コンプライアンス･プログラムの実施及び管理に不可欠な資源を提供する。

⑥ コンプライアンス･プログラム文書の最終承認をおこなう。

⑦ 個人情報保護の状況およびマネジメントシステムの見直しを、本細則に基づき実施する。

（２）　個人情報管理責任者の責任および権限

個人情報管理責任者は、以下の事項を実施する上で独立した責任および権限をもつ。

① コンプライアンス･プログラムの実施および運用に関する事項。

② 個人情報保護に関する文書の審査、発行、配付。

③ 経営者によるコンプライアンス･プログラムの見直しのために必要な、情報の収集および報告。

④ 新規に個人情報を収集する際の承認

⑤ リスク分析結果の承認

⑥ 安全対策の実行管理

（３） 内部監査責任者の責任および権限

内部監査責任者は、以下の事項を実施する責任および権限をもつ。

① 内部監査の計画。

② 内部監査の指揮・監督。

③ 監査報告書の作成。

④ 内部監査結果の経営者及び個人情報管理責任者への報告。

（４） 内部監査人の責任および権限

内部監査人は、内部監査責任者の指揮・監督のもと、以下の事項を実施する責任および権限をもつ。

① 内部監査の実施。

② 内部監査結果の内部監査責任者への報告。

③ 監査報告書の作成の補助。

（５） 部門個人情報管理者の責任および権限

① 自部門における個人情報の適切な管理。

② 自部門における個人情報に関する教育。

③ 「個人情報預かり・返却・廃棄証」の承認。

④ 自部門におけるリスク分析および対策の実行管理。

（６） 個人情報に関する問合せ窓口担当者の責任および権限

① 苦情および相談の受付。

② 苦情および相談への対応。

③ 苦情および必要に応じて相談内容の記録。

（７） 従業員共通の責任および権限

従業員は以下の事項に関する責任および権限をもつ。

① 個人情報保護方針の理解。

② 個人情報の収集・利用・管理等、個人情報の取扱いに際し、コンプライアンス・プログラムおよび準拠法令を遵守する。

③ 個人情報管理責任者および部門個人情報管理者の指示に基づいた業務の遂行。

④ コンプライアンス・プログラムに関する教育の受講。

Ⅲ　個人情報の特定およびリスク管理

１．個人情報の特定（個人情報管理台帳兼保管一覧の取扱い）

（１） 既存の個人情報の洗い出し

以下の手順により、社内における個人情報を洗い出す。

① 部門個人情報管理者は、社内を巡回し、文書や、ファイルサーバ内を確認する。

② 部門個人情報管理者は各部門代表者にインタビューを行い、確認洩れの有無と社内の各人が所有している個人情報の有無について、確認する。

③ 部門個人情報管理者は、確認された情報を、「個人情報管理台帳兼保管一覧」に記載し、個人情報管理責任者に承認を得る。

④ 洗い出された「個人情報管理台帳兼保管一覧」に記載漏れがないか否かを確認するために、内部監査時に確認する。

（２）新たに収集する個人情報の特定（新規事業の立上げ時、業務内容の変更時など）

① 業務担当者は、「個人情報管理台帳兼保管一覧」に記載のない個人情報を新たに収集する場合、「新規直接収集申請書」または「新規預託受付申請書」を個人情報管理責任者に提出する。

ａ）「新規直接収集申請書」

これまで当社では扱っていなかった種類の個人情報を、直接本人より収集するときに使用するもの。

ｂ）「新規預託受付申請書」

これまで当社では扱っていなかった種類の個人情報の預託を受ける機会が発生したときに使用するもの。（例えば：○○名簿印刷業務新規受注の場合）

② 個人報管理責任者は、「新規直接収集申請書」または「新規預託受付申請書」の内容を精査し、承認する。「新規直接収集申請書」または「新規預託受付申請書」の内容が当社コンプライアンス･プログラムに反するものである場合、承認せず、個人情報管理責任者が申請者に適切な指導を行う。

③ 承認された個人情報は、個人情報管理責任者が「個人情報管理台帳兼保管一覧」に記載する。

２．リスク分析および安全対策

以下の手順により、リスク分析を実施する。

（１） 個人情報管理責任者は、部門個人情報管理者に「個人情報管理台帳兼保管一覧」をもとに、リスク分析を命じる。リスク分析は、以下のいずれかの手法を用いる。

① チェックリスト方式
② プロセス方式
③ 上記①および②の組み合わせ

（２） リスク分析の実施と対策の決定

部門個人情報管理者は、以下①～③の手順に従って、リスク分析を実施、対策を立案し、個人情報管理責任者の承認を得る。

① 書類及び記憶媒体（FD、CD－R、ＤＶＤ、ＨＤ等）の場合
「プロセス分析表兼リスク対策一覧」により、リスク分析を行い、対策を決定する。

② ネットワーク・サーバー・ホームページの場合
「リスクチェックリスト（ネットーワーク・サーバー編)」および「リスクチェックリスト（ホームページ編)」により、リスク分析を行い、対策を決定する。

③ ①および②に加えて、主要な個人情報を取り扱う業務の場合
「プロセス分析表兼リスク対策一覧」により、個人情報を取り扱う業務の流れと個人情報のライフサイクル（収集、利用、提供、保管、廃棄、削除）に従って、リスク分析を行い、対策を決定する。決定後、残存リスクを認識し、「プロセス分析表兼リスク対策一覧」に記載する。

（３） 安全対策の規定

個人情報管理責任者は、上記リスク分析の結果、必要となった安全対策を「プロセス分析表兼リスク対策一覧」にまとめる。また、必要に応じて、安全対策を「本細則」または「安全対策細則」に規定する。

３．個人情報管理台帳兼保管一覧の管理

（１） 部門個人情報管理者は、常に自部門内における個人情報の所在を、インタビュー等により確認し、「個人情報管理台帳兼保管一覧」の正確性を維持する。その際、取扱い方法または管理者の変更など、「個人情報管理台帳兼保管一覧」の記載事項の変更が必要となった場合には、速やかに「個人情報管理台帳兼保管一覧」を改訂し、個人情報管理責任者の承認を得る。

（２） 新規事業の開始または業務の大幅な変更により、「個人情報管理台帳兼保管一覧」に記載されていない個人情報を新たに収集する場合には、（１）の手順ではなく、“１．（２）個人情報を新たに収集する場合”の手順により、申請および承認を得る。

（３） 部門個人情報管理者が「個人情報管理台帳兼保管一覧」に記載済みの個人情

報の改訂を希望する際は、“２．リスク分析および安全対策”の手順に従って再度リスク分析を行い、「個人情報管理台帳兼保管一覧」を更新し、個人情報管理責任者の承認を得る。

（４）「個人情報管理台帳兼保管一覧」は個人情報管理責任者および部門個人情報管理者のみ閲覧できるものとする。ただし個人情報管理責任者または部門個人情報管理者が許可した者は、この限りではない。

Ⅳ　個人情報の収集・利用・提供および管理

１．各部門における個人情報の収集・利用・提供および管理

（１）　目的

当社内での顧客情報および消費者情報の収集・利用・提供および管理を適切に行なうことを目的とする。

（２）　適用範囲

顧客情報および消費者情報が含まれる全ての業務に適用する。なお、本条項における情報とは、「個人情報管理台帳兼保管一覧」に記載された、紙または電子媒体に記録された個人情報である。

（３）　適用部門

各該当部門(営業、製作、印刷･製本部門、IT コンサルティング部門)

（４）　個人情報の取扱い

①　引合い入手時に行う作業

a）引合いがあった場合、営業担当者は顧客へのインタビュー等を通じて個人情報の取扱いを含む案件か否かを確認する。

b）個人情報を含む物件であった場合は、受注･作業指示票等にその旨を記載し、関連部門（製作部門、印刷製本部門、IT コンサルティング部門）へ伝達する。

②　受注後に行う作業

a）営業担当者は、個人情報を取り扱うプロジェクトの受注後、以下の内容を含む「契約書」（基本契約書または案件ごとの覚書等）を締結する。

・　　・個人情報に関する秘密保持

・再委託に関する事項

・事故時の責任分担

・契約終了時の個人情報の返却及び消去に関する事項

b）　但し顧客から上記内容を含む契約書の締結を求められた場合はそれに従う。

③　顧客情報等を直接収集する場合

展示会等のマーケティング活動において顧客情報を直接収集する場合、以下ａ）

～g）の内容について、収集を行う際のパンフレット等の文書へ記載するか、またはホームページなどの他の手段で伝達し、お客様の同意を得ること。

なお、ホームページの収集フォームを用いて個人情報を収集する場合には、ＳＳＬ等通信の暗号化を行い収集すること。

a） 当社の個人情報管理責任者または代理人の氏名もしくは職名、および所属ならびに連絡先
b） 収集する目的
c） 収集する情報を提供することがある場合には、提供先(受領者)または提供者(受領者)の組織の種類、属性
d） 収集する情報を預託（外部委託）することがある場合には、その旨
e） 本人が個人情報を与えることが任意であること、当社に情報を与えなかった場合の、本人に与える影響（当社からの商品情報が届かないなど）
f） 本人に個人情報の開示を求める権利がある旨、および個人情報に間違いがあった場合に訂正や削除を求める権利がある旨
g） 開示や訂正・削除を求める場合の方法および連絡先(連絡先が a と同じ場合は省略できる)

④ 顧客情報等を間接的に収集する場合

官公庁や委託元から、顧客情報を間接的に収集する場合には、上記ａ）～ｃ）およびｆ）～ｇ）を実行しなければならない。ただし、以下の場合は除く。

a） 名簿業者等の収集業者がすでに上記③の行為を実施している場合
b） 当社が個人情報を預託される場合。

⑤ 公開された情報から個人情報を収集する場合

公開された情報から個人情報を収集する場合、公開された目的の範囲内で収集目的を定めて収集する。

⑥ 個人情報を含む書類・媒体等の受取り

a） 営業担当者が直接、個人情報を預かる場合には、以下の項目を含む「個人情報預り・返却・廃棄証」の 3 枚綴り全てに預かり担当者が捺印をし、「個人情報預り証(黄)」をお客様に提出する。

- 個人情報の項目
- 個人情報の件数（概数）
- 預託目的
- 預託期間
- 授受方法および返却または廃棄の指定

・ 特記すべき安全対策
・ その他取扱い上の注意事項（必要に応じて）

b） 手元に残った「個人情報預り・返却・廃棄証(控)」と「個人情報返却・廃棄証」は、作業指示書(1)に付け製作担当者へ回覧するとともに、確実に個人情報を渡すこと。

⑦ 受託後の個人情報の取扱い

a) データの保管

データは保管フォルダを定めて保管し、アクセス権限を制限し、作業に必要な者のみアクセス可能とする。詳細は、「安全対策細則」に規定する。

b) 紙媒体(版下、フィルム、刷版、校正紙、印刷物、製本、ヤレ紙)および電子媒体の保管

紙媒体および電子媒体については、施錠可能なキャビネットまたは引き出しを保管場所として定め、作業時以外には指定場所に収納し、施錠する。もしくは当該作業期間中、執務室の外部入口を施錠する。詳細は、「安全対策細則」に規定する。

c) データ入力の正確性の確保

データ入力を伴う業務の場合、プロジェクト責任者は、必要に応じて、データの入力確認の手順を定め、これを実施する。

d) 製作・開発環境へのアクセス制限

社内において、個人情報を使用するシステム開発等を行う場合、各種システムのアクセスを必要最低限にとどめなければならない。詳細は、「安全対策細則」に規定する。

e) お客様先での製作・開発

お客様先で作業を行う場合には、以下のことを徹底する。

・ 不要な情報は入手しないこと
・ 離席する場合は、PC の画面を閉じる、資料は机上からしまう等、情報漏洩に留意すること。

⑧ 書類および媒体等の返却

a） 営業担当者は、書類・媒体等を返却する必要がある場合には、「個人情報預り・返却・廃棄証」に定めた方法で返却し、お客様より受領した旨の確認印を「個人情報預り・返却・廃棄証(控)」と「個人情報返却・廃棄証」にいただき「個人情報返却・廃棄証」をお客様に提出する。返却方法としては、手渡しを原則とするが、場所等の問題でやむを得ない場合は、部門個人情報管理者に承諾を得る。

b) 返却確認の記録された「個人情報預り・返却・廃棄証(控)」は当社で5年間保存する。

⑨ データの削除・廃棄

プロジェクト終了後、預託を受けた個人情報は、データを完全削除し、完了後削除担当者は「個人情報預り・返却・廃棄証(控)」と「個人情報返却・廃棄証」に捺印する。営業担当者はそのうち「個人情報返却・廃棄証」をお客様に提出する。お客様から特に要請がない限り、バックアップデータも保存しない。

⑩ 個人情報を含んだ業務の外部委託

外部委託を行う場合には、「Ⅴ　個人情報の外部委託（預託）管理　3　個人情報の預託時の確認」に定める手順に従う。

２．従業員情報の取扱い

（1）　目的

当社内で所有する従業員情報の適正な取扱いについて定める。

（2）　適用範囲

個人情報が含まれる以下の業務に適用する。

① 採用
② 入社手続き
③ 人事管理
④ 法律等に基づく手続き
⑤ その他当社が必要とする業務

（3）　適用部門

総務経理部

（4）　対象となる従業員情報

「個人情報管理台帳兼保管一覧」に示す総務経理部管理の個人情報

（5）　従業員情報の利用者

従業員情報の利用者は以下に定める者とする。

①総務経理部所属の社員
②業務上の必要性があり、個人情報管理責任者または総務経理部門個人情報管理

者の許可を得た者

（６）　従業員情報の収集

人事担当者は、従業員情報を収集する場合、以下の事項を本人に伝達し、合意をとること。

① 収集者の名称（部署名等）
② 利用者の名称（収集者と同一の場合、省略することができる。また、開示を伴う業務委託をする場合には、委託を行う旨も通知する。）
③ 収集目的（法の要請に基づいて収集、利用する場合または記入用紙の見出し等で目的が明らかであり、当該目的以外には使用しない場合は省略できる。）
④ 情報の提出が必須か任意かの区別、および情報を提供しない場合の結果（当該情報が提出されないことにより目的が達せられない場合、情報の提出は「必須」とし、提出しない場合の結果についての通知を省略することができる。）
⑤ 当該従業員情報に関する、収集者の権限
⑥ 従業員情報に関する質問・相談・苦情申し出のための連絡窓口（情報収集者と同一の場合、省略できる。）
⑦ 機微な情報を収集する場合にはその旨
⑧ その他、従業員情報の取扱いに関する実務についての必要事項

（７）　従業員情報の利用

① 従業員情報の利用は、業務に必要な範囲内とし、外部への提供に関しても必要最小限とする。
② 従業員情報の利用者は、作業中、利用を認められていない者に露呈しないよう、注意を払う。また、作業終了後は、ただちに所定の保管場所に返却する。

（８）　従業員情報の更新

人事担当者は、従業員情報および従業員データベースを、その利用目的の必要な範囲内で、最新のものにする。

（９）　従業員情報の廃棄

① 「個人情報管理台帳兼保管一覧」に定められた保管期間を超えた従業員情報は、人事部担当者が速やかに廃棄する。
   a) 紙等の媒体については、シュレッダーまたは所定の文書廃棄箱を利用する。
   b) 電子媒体については、物理的に破壊し、内部の情報が読み出しできないようにする。

（１０）　採用時手続

① 新卒もしくは中途採用など、新入社員を採用する際には、（6）①～⑧の内容を採用広告もしくはホームページ等で明確にする。なお、ホームページの収集フォームを用いて採用する個人情報を収集する場合には、ＳＳＬ等通信の暗号化を行い収集する。

② 送付された履歴書等の応募書類については、鍵付きのキャビネットに保存するなどして、不正に持ち出されないようにする。

③ 履歴書等の応募書類の取扱いについて、採用者はそのまま保存し、不採用者については、シュレッダーを用いるなどして確実に廃棄する。

④ 採用が決定した従業員について、人事部長は「知的財産の帰属および業務上の機密保持に関する誓約書」の提出を求める。これは、社員のみならず、派遣社員、契約社員、アルバイトも対象とする。

⑤ 個人情報管理責任者は、入社時教育において、当社コンプライアンス・プログラムについての説明を行う。その際、コンプライアンス・プログラムに反したものは、懲戒の対象になることを説明する。

⑥ 採用手続に関して、個人情報の収集方法、収集項目および収集目的の変更がある場合、総務経理部門個人情報管理者は「新規直接収集申請書」を起票し、個人情報管理責任者へ提出し、承認を得る。

（１１）　従業員情報の開示請求への対応

① 従業員から、自らの情報について、開示および訂正の求めがあった場合、人事部門の個人情報管理者は、「Ⅵ　個人情報の開示請求および関連業務」にしたがって、本人確認を行い開示する。

② 以下の情報は本人からの求めがあっても、原則、開示は不可とする。

a) 業績評価

b) 人事考課

（１２）　従業員からの苦情対応

「Ⅶ　個人情報の問合せ窓口」に定めた手順にしたがって対応を行う。

３．その他社内における留意事項

（１）　目的

当社内で所有する個人情報の適正な取扱いについて定める。

（２）　適用範囲

個人情報が含まれる以下の業務に適用する。

① 社内および倉庫内での管理
② ＦＡＸの利用時
③ 社内便の利用時
④ 個人情報の廃棄方法
⑤ その他留意事項

（3） 適用部門

全社

（4） 対象となる個人情報

「個人情報管理台帳兼保管一覧」に示す個人情報

（5） 媒体等の社内での管理

① 個人情報を含む紙媒体および記録媒体を社内で長期間（プロジェクト終了期間以上）にわたって保管する場合、「個人情報管理台帳兼保管一覧」に記載し、管理する。「個人情報管理台帳兼保管一覧」は、個人情報管理者が管理する。
② 社内で長期間保管している媒体等を他部門に渡す場合、「個人情報処理一覧」に日付、受渡者および提供部門名を記録する。
③ キャビネット等に保管されている個人情報を廃棄・返却する場合には、「個人情報処理一覧」に、処理日、処理担当者および廃棄方法等を記録し、「個人情報管理台帳兼保管一覧」から削除する。

（6） 倉庫内での管理

① 部門個人情報管理者は、倉庫に個人情報を含む物品を保管する場合、「個人情報管理台帳兼保管一覧」に、保管している物品を記載し、管理する。
② 倉庫内に保管されている個人情報を廃棄・返却する場合、「個人情報処理一覧」に、処理日、処理担当者および廃棄方法等を記録し、「個人情報管理台帳兼保管一覧」から削除する。

（7） ＦＡＸの利用

ＦＡＸを利用して個人情報を送信する場合、送信者は送信先の受取人に、事前に連絡の上で送信し、事後直ちに受取人本人が受領したことを確認する。

（8） 社内便の利用

社内便は「業務委託に関する機密保持契約」を結んだ指定業者によって運営する。

（９）　個人情報を含む物品の廃棄

① 個人情報を含む紙媒体を廃棄する場合、シュレッダーなどによる裁断処理または所定の文書廃棄箱を利用する。

② ①を行わない場合は、廃棄業者を利用し廃棄証明を受ける。

③ 個人情報を含む電子媒体を廃棄する場合、物理的に破壊し、内部の情報が読み出しできないようにする。

④ 個人情報を含むPC、サーバー等を廃棄する場合、必要に応じて外部者の委託業者等を活用し、データを完全に削除すること。

（１０）　その他留意事項

① 個人情報を含む紙媒体および記録媒体を用いて作業を行った場合、帰宅時には机の上に放置せず、指定のキャビネットに収納し、鍵をかけること。

② 作業中、離席する際は、ファイルは閉じ、パスワード付きのスクリーンセーバーを設定するなど、個人情報が露呈しないようにする。

③ コピー、FAX等で個人情報が含まれる作業の場合には、極力、作業完了まで一貫して行う。（仕掛中に、他の作業のために放置しない）

Ⅴ　個人情報の外部委託（預託）管理

１．外部委託先の選定および契約

（１）個人情報の処理など、業務の一部または全てを外部委託するために、新規に外注先を選定する場合には、個人情報管理責任者は、以下の基準Ａまたは基準Ｂを満たしているか否かを「外部委託先評価チェックリスト」で評価する。

① 基準Ａ

a）プライバシーマーク認証取得事業者であること

② 基準Ｂ

a） 知りうる範囲で、過去２年以内に情報漏洩の事故を起こしていないこと。

b） 個人情報保護の重要性を認識し、社内で徹底を図っていること。具体的には以下の内容等を備えた「外部委託先評価チェックリスト」の項目を満たしていること。

- 個人情報保護方針を定めている。
- 個人情報保護に関する教育を行っている。
- 個人情報保護のために管理策を設定、実施している。

c） 個人情報保護に関する契約を締結することができること。

（２）評価終了後、取引可と判断された場合には、以下の内容を含んだ「業務委託に関する機密保持契約書」（基本契約書または案件ごとの覚書等）を締結する。

① 個人情報に関する秘密保持
② 再委託に関する事項
③ 事故時の責任分担
④ 契約終了時の個人情報の返却及び消去に関する事項
⑤ 二者監査の受け入れ許可に関する事項（必要に応じて）

（３）「業務委託に関する機密保持契約書」は、個人情報を外部委託先が保有している期間以上、保持する。

２．外部委託先の定期評価

個人情報管理責任者は、年１回 8 月に、「外部委託先評価チェックリスト」を用いて、外注先を評価する。評価基準を満たしていない場合、部門個人情報管理者と協議の上、取引継続の可否を決定する。

３．個人情報の預託時の確認

（１）外部委託先に個人情報を預託する場合、「預託時チェックリスト」を用いて、以下の事項を確認の上、個人情報を預託する。

① 預託目的
② 預託する個人情報の件数（概数）
③ 預託期間
④ 授受方法および返却または廃棄の指定
⑤ 外部再委託の可否
⑥ 特記すべき安全対策
⑦ その他取扱い上の注意事項

Ⅵ　個人情報の開示請求および関連業務

１．問い合わせおよび開示請求への対応手順

（１）開示請求対応の原則

①　原則として、本人からの開示請求であり、かつ適正な理由があると判断された場合のみ開示に応じる。だだし、本人からの請求であっても以下のa)～ｃ）に該当する場合には、個人情報管理責任者の判断により、開示しないことがある。

a)　本人または第三者の生命、身体、財産その他の権利利益を害するおそれがある場合

b)　当社の業務の適正な実施に著しい支障を及ぼすおそれがある場合

c)　他の法令に違反することとなる場合

②　上記①に関わらず、以下に示す情報については、原則、非開示とする。

a)　入社時試験結果

b)　業務評価結果

c)　お客様より預託されている個人情報

（２）本人確認および対応の手順

①本人確認の実施手順

ａ）ＦＡＸ文書や電話にて、開示請求があった場合は、本人確認を実施する。確認の内容は以下とする。

・本人の名前を確認する。

・住所、電話番号を話していただき、当社の登録情報と照合する。

ｂ）一致した場合には、問い合わせや請求の内容にしたがった開示を行う。

ｃ）一致しない場合には、身分証明書など提示、他の属性（生年月日等）など、更なる手段で本人確認を行う。

②不審者への対応

不審な問い合わせ、開示請求を受け付けた場合には、速やかに個人情報管理責任者へ連絡し、指示を仰ぐ。

③開示の方法

開示方法は、書面によるものとするが、開示請求を行った者が同意している場合には、同意された方法でも可とする。

④個人情報の利用または提供の拒否権

開示の結果、誤った情報などがあり、本人から訂正・削除の依頼を受けた場合には、速やかにこれに対応する。また、第三者への提供の拒否を受けた場合にも、速やかにこれに対応する。

Ⅶ　個人情報の問合せ窓口と対応手順

１．個人情報の問合せ窓口の設置

当社は個人情報に関する苦情及び相談に対応するために、「個人情報の問合せ窓口」を設置する。窓口については、「個人情報保護のための体制図」に定める。

２．ホームページ上への明示

「個人情報の問合せ窓口」についてＨＰ上に明示する。

３．問合せ・苦情の対応手順

（１）電話／ＦＡＸ／メールのいずれかの方法で個人情報に関する苦情及び相談を受けた者は、速やかに「個人情報の問合せ窓口」に取り次ぐ。

（２）窓口担当は対応し、必要に応じて個人情報管理責任者に連絡し、指示を仰ぐ。

（３）窓口担当は、苦情および問合せ内容については、「個人情報・問合せ記録表」に記録する。

Ⅷ　法令およびその他の規範の遵守

１．法規制登録簿の作成

個人情報管理責任者はコンプライアンス事項に継続的に注意を払い、「法規制登録簿」にしたがって法令案の改正等の有無を随時確認する。加えて、年に 4 度 1 月、4 月、 7 月、10 月に包括的な確認を行う。改正等があった場合、コンプライアンス･プログラムの修正の要否を判断し、必要に応じて変更を実施する。

２．法令等の参照

各部署では端末を用いて法令及びその他の規範を参照する。

Ⅸ　教育

１．年間教育計画の策定

（１）個人情報管理責任者は、以下の内容を教育するため、「年度教育・内部監査計画書」を策定し、経営者の承認を受ける。

① 当社のコンプライアンス･プログラムに従うことの重要性と利点
② 当社のコンプライアンス･プログラムに従うことの役割及び責任
③ 当社のコンプライアンス･プログラムに違反した際に予想される結果

なお、これらの講習には教育テキストを用い、それを保管すること。

（２）受講対象には、役員、社員、契約社員、派遣社員を含め、最低年 1 回は教育を受講するよう計画する。

２．教育の実施

（１）役員、社員、契約社員、派遣社員への教育は、個人情報管理責任者もしくは、部門個人情報管理者が実施する。なお、教育は外部の専門家に委託することもできる。

（２）新入社員等に対しては、入社の都度、個人情報管理責任者または部門個人情報管理者が教育を実施する。これには、契約社員、派遣社員、パート、アルバイトの非常勤者も含むこととする。

（３）教育の実績は、その実施者が、以下の項目を含む「教育実施記録」に記録する。

① 名称
② 日時
③ 講師
④ 受講対象
⑤ 使用テキスト
⑥ 教育の概要

（４） 教育の効果については、理解度テスト、内部監査等によって確認する。

X　経営者による見直し

１．見直しの手順

経営者は個人情報を適切に保護しつづけるために、以下の手順によりコンプライアンス・プログラムの見直しを実施する。

（１）参照情報

② 「内部監査報告書」

③ 安全対策の実施状況

④ 「個人情報・問合せ記録表」（無い場合もある）

⑤ 「個人情報事故報告書」（無い場合もある）

⑥ 外部環境の変化

⑦ 法令・ガイドライン等の変更

⑧ その他提案　など

（２）実施時期

毎年６月に実施する。

ただし、経営者の判断により、追加で臨時実施しても良い。

（３）結果の記録

① 見直しの結果については、「コンプライアンス･プログラム見直し指示書」に記録する。

② 指示内容は、個人情報管理責任者および部門個人情報管理者を通じて、関連従業員に徹底する。

XI　文書・記録の管理

１．文書管理の手順

個人情報保護に関する文書を管理するための手順を以下のとおり規定する。

（１）　必要な文書、並びにこれらの作成および承認の責任および権限を、「管理文書・様式・記録一覧表」に規定する。なお、当該権者が不在の場合、審査、承認は上位者または権限を委譲された者が行うことができる。

（２）　文書の最新版の状態を、「管理文書・様式・記録一覧表」で明確にする。

（３）　文書の最新版は個人情報管理責任者が管理し、電子掲示板にて、全社で閲覧可能にする。

（４）　電子データは、最新版の発行に際し旧版のデータを削除する。廃止文書を保管する場合には、旧版をサーバ上に残さず別の媒体に保存するなど、間違って使用しないように識別する。

２．記録管理の手順

個人情報保護に関する記録を管理するための手順を以下のとおり規定する。

（１）　個人情報保護の管理に必要な記録は「管理文書・様式・記録一覧表」に明確にする。

（２）　記録は、見出しなどで識別する。

（３）　担当者は、記録が検索しやすいように、また、紛失、損傷又は汚れないように保管する。

（４）　電子媒体で保管する場合には、権限者以外は削除・訂正が不可能な状態で保管し、バックアップを取る。

（５）　保管期限を過ぎたものについては、各部門個人情報管理者が、廃棄等適切に処理をする。

別紙　「法規制登録簿」

名　称	参照元	入　手　方　法
個人情報保護法	総務省　電子政府	http://law.e-gov.go.jp/cgi-bin/idxsearch.cgi
JIS　Q　15001 個人情報に関するコンプライアンスプログラム要求事項	日本規格協会	
不正アクセス禁止法	総務省　電子政府	http://law.e-gov.go.jp/cgi-bin/idxsearch.cgi
不正競争防止法	総務省　電子政府	http://law.e-gov.go.jp/cgi-bin/idxsearch.cgi
労働基準法	総務省　電子政府	http://law.e-gov.go.jp/cgi-bin/idxsearch.cgi
個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン	経済産業省	http://www.meti.go.jp/policy/it_policy/privacy/041012_hontai.pdf
雇用管理に関する個人情報の適正な取扱を確保するために事業者が講ずべき措置に関する指針	厚生労働省	http://www.mhlw.go.jp/topics/2004/07/tp0701-1.html
印刷産業における個人情報保護に関するガイドライン	日本印刷産業連合会	http://www.jfpi.or.jp/
プライバシーマーク制度における監査ガイドライン	日本情報処理開発協会	http://privacymark.jp/ref/pmaugl.html
千葉県個人情報保護条例	千葉県公式ＨＰ	http://www.pref.chiba.jp/reiki/mokuji_bunya.html
習志野市個人情報保護条例	習志野市公式ＨＰ	http://www.city.narashino.chiba.jp/siyakusyo/kikaku/joho/pdf/kaiseijourei.pdf
ISMS 認証基準	日本情報処理開発協会	http://www.jipdec.jp/
コンピュータ不正アクセス対策基準	経済産業省公式ＨＰ	http://www.meti.go.jp/policy/netsecurity/UAaccessCMG.htm
コンピュータウイルス対策基準	経済産業省公式ＨＰ	http://www.meti.go.jp/policy/netsecurity/CvirusCMG.htm

安全対策細則

Ver.20170401

制定日：2017 年 4 月 1 日

株式会社ネクストページ

承認(社長)	審査(個人情報管理責任者)	作成

目　　次

改訂履歴

年月日	改訂内容
平成 29 年 4 月 1 日	制定初版

Ⅰ　総則

１．　目的

（１）本細則は、当社における個人情報の収集、利用、提供および管理における個人情報に関するリスク（個人情報への不正アクセス、個人情報の紛失、破壊、改ざんおよび漏えい）を低減し、個人情報を確実に保護するための安全対策活動を規定するものである。

２．適用範囲

（１）　対象組織：全社（当社に勤務する社員、準社員、契約社員、派遣社員、パートおよびアルバイトを含む）／全業務

（２）　対象となる個人情報：全部もしくは一部を電子計算機などの自動処理システムによって処理している、又は自動処理による処理を行うことを目的して書面などによって処理している個人情報だけでなく、何らかの規則により索引付けされた個人情報であれば、媒体に関係なく含む。具体的には、「個人情報管理台帳兼保管一覧」に定めた個人情報とする。

３．用語の定義

（１）　従業員

当社に勤務する社員、準社員、契約社員、派遣社員、パートおよびアルバイトを含む。

（２）　来館者

当社本社、支社および営業所等に出入りする当社従業員以外の者。お客様、協力会社等。

（３）　社屋

当社本社、支社および営業所

（４）　事務所

営業部、総務経理部、工務部製作課の執務室

（５）　工場

工務部印刷製本課の執務室

（６）　共用部

トイレ・給湯部

（７）　情報システム管理者

本細則を実施するにあたり、情報システムに関する安全対策を実施する責任者。

（８）　部門個人情報管理者

各部門の個人情報の適切な取扱い、利用および管理について責任を持つ者。個人情報管理責任者より、業務の遂行に必要な権限を付与される。

Ⅱ．物理的アクセス管理

１．一般フロアへの入退室管理

（１）社屋への入退室の制限

① 事務所への出入りは、当社役員、「社員証」を携帯した従業員、「ご来訪者証」を貸与された来館者、および当社社員の同伴による案内がある者のみに限定する。

（２）社員証の携帯および管理

① 「社員証」の管理は、総務経理部が行う。

② 総務経理部は、当社従業員に、社員証№の付与された「社員証」を貸与し、「社員証管理台帳」に記録する。社員証を付与する際、氏名、生年月日、所属部署等を確認し、受け取り手が本人であることを確実にする。

③ 当社従業員は、事務所等での勤務中、所属部署および氏名を識別できる「社員証」を目に見える位置に携帯しなければならない。

④ 紛失等により、「社員証」の再発行の依頼があった場合には、総務経理部は上記②の手続きを行う。

a) その際、従業員本人であることを確認するとともに、紛失状況等の詳細を確認し、二重貸与にならないことを確実にする。

b)紛失等した社員証は無効とし、「社員証管理台帳」にその旨を記入する。

⑤ 従業員の退職または契約打ち切り等の場合には、社員証の返却を求め、「社員証管理台帳」に返却日および理由を記入する。

⑥ 従業員間の社員証の貸与および社員証№の共有はしてはならない。

（３）ご来訪者証の貸与及び管理

① 「ご来訪者証」の管理は、総務経理部が行う。

② 来館者があった場合、対応従業員は来館者に対し、社名、氏名、訪問先、訪問目的、時刻を「来訪者記録表」への記入するよう依頼する。ただし、滞在時間が短く、滞在範囲が限定されており、かつ滞在時間中つねに当社社員が同伴する場合は、省略できる。

③ 総務経理部は、記入内容を確認した上で、来館者に「ご来訪者証」を貸与する。

④ 来館者は、当社内での滞在時間中、貸与された「ご来訪者証」を目に見える位置に携帯しなければならない。

⑤ 務経理部は、来館者が事務所等を退出する際には、「ご来訪者証」の返却確認を行ない、返却日時を「来訪者記録表」に記録する。

⑥ 総務経理部は、毎月末、「ご来訪者証」の現物と「来訪者記録表」を照合する。現物の過不足等を発見した場合には、直ちに当該ご来訪者証を特定し、該当する部門個人情報管理者に、ご来訪者証の捜索を依頼すると共に、業務上の問題が発生していないことを確認する。

a）問題が発生していた場合、個人情報管理責任者に直ちに報告し、指示を受ける。

b）ご来訪者証が見つからなかった場合、個人情報管理責任者の判断により、当該ご来訪者証を無効とし、「来訪者記録表」にその旨記入する。

（4）不審者の識別および対応

① 「社員証」、「ご来訪者証」のいずれも携帯しておらず、当社社員の同伴もない者を見つけた場合には、当社従業員から必ず声をかけ、身元、訪問先、目的を確認する。

a）確認できた場合、総務経理部にて「ご来訪者証」の発行手続きを求める。

b）確認できなかった場合、氏名および連絡先を確認した上で、退出を求める。

（5）施錠の管理

① 社屋への出入口の鍵鍵およびセキュリティシステムICキーの管理は総務経理部が行なう。

② 社屋への通常の出入は、正面玄関から行なう。その他の出入口は掃除・物品の搬入その他必要時のみ開錠することとし、平常時は施錠する。

③ 総務経理部は必要のある社員に正面玄関の鍵およびセキュリティシステムICキーを貸与し、「社員証管理台帳」にICキーのキーナンバーを記録する。紛失・再発行・返却等の手続きは、社員証の手続きと同様とする。

④ 各部最後に退出するものは、退社時チェックリストの自部門の項目を確認し、チェックをして退社する。

⑤ 最終退出者は、退社時チェックリストの自部門および共用部の項目を確認し、チェックをし、セキュリティシステムを稼動させ、正面玄関を施錠して退社する。社屋に残留者がいる場合、アラーム設置のドア・窓が閉められていない場合は、セキュリティシステムにより警告されるので、確認、解決してから退出する。ただし、対応に危険のある場合は、警備会社に連絡し指示に従う。

（6）深夜・早朝・休日の入退室

① 深夜・早朝・休日は、警備会社の監視時間となるので、この時間に社屋へ立ち入る際、または深夜業となり退出できない場合は、警備会社へ連絡しなければならない。

② 深夜・早朝・休日に小人数で業務にあたる時は、正面玄関を内側から施錠する。

２．キャビネットの管理

（１）　個人情報の媒体の保管

①　個人情報が記録された紙およびCD－R等の情報記録媒体は、原則、施錠が可能なキャビネットに保管する。

（２）　キャビネットの鍵の管理

①　キャビネットの鍵は、総務経理部が管理する。

②　従業員がキャビネットに管理された物品を利用する場合には、総務担当立会いのもと解錠する。

Ⅲ　論理的アクセス／ネットワーク管理

１．アクセス権限の管理

意図しない情報漏洩および誤操作による情報の破損等、トラブルを未然防止するため、アクセス権限について以下のとおり規定する。

（１）アクセス権限の管理者

①　情報システムに関するアクセス権限の付与、抹消および変更は、情報システム管理者が「アクセス権限管理台帳」により管理する。

（２）アクセス権限の申請および付与

① アクセス権限の申請は、各部門責任者から、情報システム管理者に「アクセス権限申請書」を提出することで行う。その際、各部門責任者は、アクセス権限の利用についても責任を持つ。

② 情報システム管理者は、申請内容を精査したうえで、アクセス権限を付与し、「アクセス権限管理台帳」に記録する

③ 付与されたアクセス権限については、他人との共有および許可無く変更を行ってはならない。

（３）アクセス権限の抹消

①　部門所属者のアクセス権限が不要になった場合には、各部門責任者は、情報システム管理者に、遅滞なく抹消を申請する。申請は、「アクセス権限申請書」を提出することで行う。

②　情報システム管理者は抹消手続きを行ない、「アクセス権限管理台帳」に記録する。

２．ＩＤおよびパスワードの管理

（１）情報システム管理者によるＩＤおよびパスワードの管理

①利用者から、ＩＤまたはパスワードの再発行の申請等があった場合には、本人であることおよび申請理由の確認を行なう。

②パスワードの発行にあたっては、６文字以上のものを使用し、その際容易に推測可能なものは使用しない。

③パスワードは２ヶ月に一度の頻度で更新する。

（２）利用者によるＩＤおよびパスワードの管理

情報システムの利用者（以下、利用者）は、次のとおり、ＩＤおよびパスワードを個々の責任において管理する。

① 情報システムに関するＩＤが必要な場合には、Ⅲ１（２）に規定する手続により申請を行う。

② 与えられたＩＤおよびパスワードについては、利用者自らが厳重な管理を行ない、生命の危険および業務遂行に関する全社規模の重大問題を回避するために、必要な場合を除くいかなる事情によっても他人に開示してはならない。

③ ID およびパスワードの機密性を保持するために、利用者はパスワードを入力する際、他人に見られないよう留意する。

④ パスワードが何らかの理由で他者に漏洩した可能性がある場合、速やかに情報システム管理者に連絡し、パスワードの変更を依頼する。

３．不正アクセスの防止対策

（１）情報システム管理者は、情報システムを不正アクセスから防護するため、以下の事項を実施する。

① 外部から社内ＬＡＮへのアクセスは不可とする。

② 長期間利用しない機器は、ネットワークに接続しない。

③ システムファイルまたはデータへのアクセス権限は、必要最小限の範囲とする。

④ データの特性上必要な場合は、データの所有者と協議したうえで、個別に防止策を講ずる。

（２）情報システム管理者は、情報システムの不正アクセスの早期発見につなげるため、以下の事項に努める。

① 不正アクセスを発見するため、アクセス履歴を定期的に分析する。

② 問題発生時および情報システム管理者が必要と判断したタイミングで、ソフトウェアおよびシステムファイルの改ざんが生じてないことを確認する。

Ⅳ　サーバ／端末管理

１．サーバの物理的セキュリティ

（１）事務所内サーバ区画の物理的セキュリティ

情報システム管理者は、事務所内サーバ区画において、次に定める物理的なセキュリティ対策を実施し、サーバおよびネットワーク機器関連の事故発生の可能性を低減する。

① 誤って手を触れる等、不用意な操作ミスの発生の低減を考慮した措置。これにはサーバラックの施錠管理を含む。
② 機器の落下や損傷の防止措置。
③ 耐震、耐火、耐水、避雷等の防災対策。システムおよび電源や空調設備等も併せて行う。
④ 無停電電源設備または電圧安定化設備による電源対策。

（２）データセンターの物理的セキュリティ

情報システムの一部を、社外データセンター内のマシン室またはサーバラック内に設置する場合には、以下の事項を実施する。

① 情報システム管理者は、データセンターを、次の基準を考慮して選定する。
　ａ）厳重な入出制限がされており、入室の際は本人確認の仕組みを有すること。
　ｂ）他の入室者が誤って手を触れる等、不用意な操作ミスの防止を考慮した措置が講じられていること。
　ｃ）機器の落下や損傷の防止措置が講じられていること。
　ｄ）耐震、耐火、耐水、避雷等の防災対策おおび電源対策が施されていること。
② 上記①以外の詳細な安全対策については、当該データセンターの安全基準に従う。
③ データセンターとは、安全対策に関する事項を含めた契約を締結する。
④ 当社従業員がデータセンターへ入室する際は、情報システム管理者に事前の了解を得る。

２　データのバックアップおよびリストア

（１）バックアップの実施手順

部門個人情報管理者は、情報システム上のデータについて、バックアップの実施手順を以下のとおり明確にし、実施する。

① バックアップの頻度は、原則として毎日とする。

② バックアップの方法は、原則として、指定されたファイルサーバまたはＣＤ・ＭＯとする。

③ バックアップ媒体は、施錠可能なキャビネット等に保管し、容易に持ち出しが出来ないよう管理する。

④ バックアップデータは、最新データの保管を行う。

（２）リストアの実施手順

情報システム管理者は、情報システム上のデータについて、リストアの実施手順を以下のとおり明確にし、実施する。

① リストア直前のデータをバックアップする。

② 情報システム管理者の責任の下、リストアを実施する。

３．ウィルス等、悪質なソフトウェアからの防護

コンピュータウィルス等、悪質なソフトウェアおよびこれらを用いた攻撃から情報システムを防護するために、次の事項を規定する。

（１）社内の情報システム

① 当社内で使用する情報システムには、ウィルスチェッカ等を設置し、悪質なソフトウェアからの防護対策を行う。

② 情報システム管理者は、ウィルスチェッカ等のバージョン更新情報の確認を適宜行う。

③ 情報システム管理者は、ウィルス情報について常に収集に努め、必要に応じて、各利用者に対策を指示する。

（２）外部から持ち込む情報システム

① 顧客や協力会社等、外部から持ち込まれる端末は、原則として、当社の情報システムへの接続を認めない。ただし、ウィルスチェッカ等悪質なソフトウェアからの防護対策が十分なされていると各部門個人情報管理者が認めた場合は、接続を許可することをさまたげない。

４．システムの設置および変更

情報システム（社内ＬＡＮ含む）に関する設置、変更および撤去ならびに情報システム

を管理するため、以下を規定する。

（１）情報システムの構成要素

本項で意図する情報システムとは以下のものを含む。

① サーバ
② ＰＣ（デスクトップおよびノート）
③ 入出力装置（キーボード、マウス、スキャナ、ディスプレイ、プリンタ）
④ 媒体記録装置（ＦＤ、ＭＯ、ＣＤ－Ｒ、ＤＶＤ－Ｒ、外部メモリ等）
⑤ 外部記憶装置（外付けハードディスク等）
⑥ ＯＳ
⑦ アプリケーション（電子メールソフト／Ｗｅｂブラウザ含む）
⑧ ユーティリティソフト
⑨ Ｆ／W、ゲートウェイ
⑩ ルータ、スイッチングハブ
⑪ その他、ネットワーク関連設備

（２）情報システムの設置・変更の管理

① 情報システムの設置・変更および撤去作業は、以下の者（以下、作業者）が行う。
ａ）情報システム管理者
ｂ）情報システム管理者より権限を委譲された社員
ｃ）情報システム管理者が承認の上、当社と契約を締結した外部委託先
② 情報システムの設置・変更または撤去を行う場合、作業者は、「作業手順書」またはこれに替わるもの（チェックリスト等）を、情報システム管理者に提出する。
③ 情報システム管理者は、常に、情報システムの構成を把握し、作業を実施または指示する。
④ 情報システム管理者以外の者は、当社の情報システムへの外部からの接続を、許可無く行ってはならない。
⑤ 情報システムの撤去および廃棄を行う場合には、情報の消去等必要な対策を行う。
⑥ 作業終了後、情報システム管理者または権限を委譲された従業員は、変更の検証を実施し、変更点と動作を確認する。
⑦ ＰＣはワイヤーロック等、物理的な盗難対策を行なう。

５．パッチ等システムの更新（Windows Update 等）

情報システム管理者は、情報システムへのパッチ等の適用の要否を判断し、必要な更新

を行うと共に、利用者に対する指示を行う。

６．外部公開サーバの管理とデータの更新

（１）定義

外部公開サーバとは、インターネットなどを使用して外部の者に情報を公開するサーバを指し、Web サーバ等を含む。契約に基づき特定企業と定型的に情報交換を行なうサーバについては、本項の対象とはしない。

（２）外部公開サーバの管理

外部公開サーバについては、サーバ管理者を明確にし、以下の管理を実施する。

① ３．（１）および（２）に従い、不正アクセスの対策を講ずる。
② ぜい弱性攻撃など、外部からの攻撃に関する情報を適宜収集し、情報セキュリティ上の対策の改善を継続的に実施する。
③ 外部公開サーバのシステム設定などを更新可能な権限者は限定する。
④ 上記①、②、③を実施することが困難な場合および①、②、③を実施したとしても情報セキュリティ上の問題が残る場合は、遅滞なく情報システム管理者に報告する。
⑤ 外部公開サーバのメンテナンスまたは廃棄の際には、情報が漏えいしないよう、データ消去などの対策を行なう。

（３）外部公開サーバに対する入力データの暗号化

採用や資料請求申込みなど、外部公開サーバで個人情報を収集する場合、サーバ管理者は、ＳＳＬ等の通信の暗号化を行うこと。

（４）外部公開サーバ上のデータの更新

外部公開サーバ上に情報を公開する場合または外部公開サーバ上に情報を保管する場合、以下の管理を実施する。

① 外部公開サーバ上に情報を公開するために、データ更新を行うことができる権限者は限定する。また、作業履歴が特定できるよう外部公開サーバ用にアクセスするためのＩＤは個別に与える。
② 外部公開サーバ上に情報を公開する場合、新規または更新情報の適切性を、更新者以外の者が確認する。
③ 外部公開サーバ上での情報の保管は、短時間に限るものとする。情報が一時的に外部公開サーバ上に置かれる場合であっても、速やかに情報を社内のサーバ等に移管し、外部公開サーバ上に長期間放置されないよう、システムの設計および運用を行なう。

（５）外部公開サーバの管理およびデータ更新の外部委託

外部公開サーバの管理およびデータ更新の全部または一部を外部プロバイダー、ホスティングサービス等に委託する場合は、上記（１）～（４）を満たす業者を選定する。

Ⅴ　文書および電子媒体管理

１．文書および電子媒体の取扱い

（１）文書の取扱い

①文書の機密性について以下のとおり分類する。

機　密：社内の特定者のみに開示可能な情報。外部から預かる個人情報を含む。
営業、契約、財務、商品開発関連情報は、原則、機密扱いとする。

社外秘：社員のみに開示可能な情報。社員の個人情報を含む。
機密情報のうち、部門個人情報管理者によって社内開示を認められたものは社外秘扱いとする。

一　般：公開を目的とした情報（開示後のＩＲ情報含む）または開示されることにより当社に不利益をもたらさない情報。

②文書の取扱いのルールを以下のとおり規定する。

機　密：保管場所を特定し、持ち出しには保管場所の所轄部門の部門長の許可を必要とする。業務目的以外の複製は不可とする。
授受については授受を行なう部門の部門長がルールを定め、必要に応じて文書化する。

社外秘：社外への持ち出しには保管場所の所轄部門の部門長の許可を必要とする。
授受については授受を行なう部門の部門長がルールを定め、必要に応じて文書化する。

一　般：特に定めない。

（２）電子媒体の取扱い

①　電子媒体を保管する場合、上記１．（１）①の分類に従い、機密および社外秘のものは保管場所を定めて保管する。

②　外部から預る個人情報のうち、一覧またはデータベースに類する状態での電子媒体で授受する場合、パスワードの設定または暗号化を行なう。

Ⅵ　情報システムの利用

１．情報システムの利用

（１）利用状況の監視

当社は情報セキュリティの実現のために、利用者に事前承諾を得ることなく、利用者の使用状況について監視を行ない、電磁的記録（ＨＤ、ＦＤ、ＭＯ等）を調査することができる。またこの調査結果に関して、以下の場合には利用者に事前承諾を得ることなく、利用者以外に開示する場合がある。

①公的機関から法的な強制力のある命令があったとき

②会社が関与する紛争を解決するために必要と判断したとき

（２）情報システム（社内ＬＡＮ含む）利用にあたっての遵守事項

① 情報システムは、利用を許可された者のみが操作可能とする。利用者は、来訪者など利用を許可されていない者が情報システムの利用を試みた場合に、これを許してはならない。

② 情報システムは、許可無く外部に持ち出してはならない。

③ 情報システムは原則、当社から貸与されたものを用い、個人所有のものおよび他社所有のもの等は持ち込まない。ただし、やむを得ない理由により、部門長が認めた場合は、この限りではない。

④ 個人情報を含むファイルは、指定のファイルサーバに保管し、端末には、作業用の必要最小限かつ一時的なもの以外は保存してはならない。端末上の個人情報は、作業が終了次第、直ちにファイルを完全削除する。

（３）個人用端末の管理

① 個人用端末は、原則、情報システム管理者から貸与されたものを用い、プライベートなもの（個人所有のものなど）は持ち込まない。ただし、やむを得ない理由により、情報システム管理者が認めた場合は、この限りではない。

② 個人情報を含むファイルは、セキュリティが確保されたファイルサーバに保管し、個人用端末には、作業用の必要最小限かつ一時的なもの以外は保存してはならない。個人端末上の個人情報は、作業が終了次第、直ちにファイルを完全削除する。

（４）個人用端末の持ち出し

① 個人用端末の持ち出しは、情報システム管理者が認定した端末のみとする。

② 情報システム管理者が持ち出しを許可した個人用端末は、ＩＤとパスワードによる厳重なアクセス制限を施す。原則、外付け用の機器は接続しない。

③ 個人用端末を社外に持ち出す際は、利用者は「ＰＣ持ち出し管理台帳」を記入し、端末の所在を明らかにする。

④ 持ち出しを許可したノートＰＣには、個人情報は保存しない。ただし、情報システム管理者が、やむをえない事由と認めた場合には、暗号化されたデータ領域を設置し、その領域を用いることで許可する。

２．電子メールの利用

（１） 情報システム利用者は電子メールの利用に際して、次の事項を遵守しなければならない。

① 電子メールは秘匿性がないことに留意する。機密性を要する情報については、可能な限り電子メール以外の伝達手段を使用する。

② 外部にファイルを添付して電子メールを送信する際には、システム上でファイルについてウィルスチェックを実施してから送信する。

③ 電子メールは、業務利用を目的する。私的利用は、業務に影響を及ぼさない程度であれば許容するが、この場合であっても本項に反してはならない。電子メールの内容について、社員のプライバシーは保護されない。

④ ウィルスの疑いがあるメールを受信した場合、添付ファイルを開封もしくは保存等操作をしてはならない。直ちに情報システム管理者に連絡する。

⑤ 電子メールソフトについては、当社で指定したものを使用し、許可無く設定を変更してはならない。

⑥ 電子メールの利用者は、自己の責においてメールアドレス（ＩＤ）とパスワードを管理する。

３ Web（ホームページ）等の利用

（１）情報システムの利用者は、Web（ホームページ）等の利用に際して、次の事項を遵守する。

① インターネット上のサイトへのアクセスに関しては、業務目的以外の利用を禁ずる。

② Web ブラウザについては、当社標準のものを使用する。

③ インターネット上のサイトにアクセスする場合、当社標準の proxy サーバを経由してアクセスする。

④ ファイルのダウンロードを行う場合、ダウンロードしたファイルはウィルスチェックしてから使用する。

⑤ フリーメール等、インターネット上のＷｅｂサーバを利用した電子メールの利用は許可無く行ってはならない。

⑥ 社内外のＷｅｂサーバおよび関連機器等について、攻撃等不正なアクセスを行ってはならない。またこうした目的のために社内外のシステムを利用してはならない。

4　障害発生時の対応

（1）ウィルス感染の可能性がある場合

① ウィルス感染によりシステムに不具合が発生していると想定される場合、ただちにネットワークケーブルを取り外すなどにより、端末機をネットワークから物理的に切り離す。

② ネットワークに接続されていない状態でウィルスチェッカを作動させる。

③ 情報システム管理者に直ちに状況を報告し、指示に従う。

（2）その他、物理的障害などの場合

① 情報システム管理者に速やかに状況を報告し、指示に従う。

② 外部への修理の依頼等は、情報漏えいの危険がありうるため、情報システム管理者の許可なしに行なってはならない。

緊急対策細則

Ver.20170401

制定日：2017 年 4 月 1 日

株式会社青孔社

承認(社長)	審査(個人情報管理責任者)	作成

<u>目　　次</u>

改訂履歴

改訂履歴

年月日	改訂内容
平成 29 年 4 月 1 日	制定初版

Ⅰ　総則

１．目的

本細則は、当社における個人情報の収集、利用、提供および管理に関するリスク（個人情報への不正アクセス、個人情報の紛失、破壊、改ざんおよび漏えいなど）が顕在化した場合の、緊急対策手順を規定することを目的とする。

２．適用範囲

（１）　対象組織：全社（当社に勤務する社員、準社員、契約社員、派遣社員、パートおよびアルバイトを含む）／全業務

（２）　対象となる個人情報：全部もしくは一部を電子計算機などの自動処理システムによって処理している、又は自動処理による処理を行うことを目的して書面などによって処理している個人情報だけでなく、何らかの規則により索引付けされた個人情報であれば、媒体に関係なく含む。具体的には、「個人情報管理台帳兼保管一覧」に定めた個人情報とする。

Ⅱ　緊急対策

１．緊急事態対応

（１）細則

本細則で定める緊急事態とは、個人情報の保護に直接関係するものおよび個人情報の保護に大きく影響を与えるものを言う。以下に分類と、対象となる事件・事故の例を示す。なお、類似の事象が発生した場合は、以下の事例に捕われず緊急事態ととらえ、本手順を適用するものとする。

①個人情報に直接関係する緊急事態の例

・個人情報漏えい事故。この場合、発見された場所は社内外を問わない。
・個人情報の不正持ち出し。
・個人情報の盗難
・配送中など外部での個人情報の紛失
・大規模な個人情報の紛失・損傷

②情報システムに関する緊急事態の例

・ウィルスの侵入によるシステムダウン。
・ハッキング／クラッキング行為によるシステムの乗っ取り。
・社内外の不適切な者による管理者権限の取得。
・ＩＤ／パスワードなどの流出。
・ネットワーク上の個人情報の破壊および改ざん行為。
・ノートＰＣの紛失または盗難

（２）緊急事態の発見と連絡

①緊急事態の発見

緊急事態を発見した者は、直ちに個人情報管理責任者に報告する。

②個人情報管理責任者に連絡できない場合

緊急事態を発見したものは、「緊急連絡網」を用いた適切な報告、または部門個人情報管理者へ報告する。

（３）対応手順

①緊急対応責任者

緊急事態の内容ごとに緊急対応責任者を以下のように定める。

ａ）個人情報に直接関係する緊急事態

個人情報管理責任者。ただし、個人情報管理責任者が緊急対応を行えない場合には、内部監査責任者が状況把握の責任を持つ。

ｂ）情報システムに関する緊急事態

情報システム管理者。ただし、情報システム管理責任者が緊急対応を行えない場合には、個人情報管理責任者が状況把握の責任を持つ。

ｃ）上記のａ）およびｂ）に関わらず、経営者は緊急対応責任者を任命することができる。この場合、緊急対応責任者が複数となって指揮命令系統の混乱を招かぬよう留意する

②状況の把握

緊急対応責任者は、冷静・沈着に情報を収集、分析し、問題の大きさと影響範囲をできる限り特定する。同時に経営者に適切に問題点を連絡し、必要に応じて経営者の判断を仰ぐ。

③緊急対応策の決定と実施

緊急対応責任者は、収集、分析した情報を元に、以下の内容に関する緊急対策を検討し、決定する。必要に応じて、関係各部門と協議の上、緊急対策を決定する。緊急対策は、定常的な業務の遂行に優先して実施する。

ａ）被害の拡大の防止。

ｂ）情報システムの問題で、外部への二次的被害をもたらす可能性がある場合には、システムの一部切り離しまたは停止措置により、強制的に被害の拡大を防止。

ｃ）被害が顧客など外部の者に広範囲に及ぶ場合、緊急対策会議の召集。この会議には経営者をはじめ、必要と判断した者であれば、部門、階層を問わず参加を指示する。

ｄ）マスメディア等によって当社の信用に影響が出る懸念がある場合には、経営者と協議し、対策を講じる。

ｅ）必要に応じて、顧客、経済産業省、所属団体および(財)日本情報処理開発協会への連絡に関する立案および指示。

④発生原因および被害状況の分析

ａ）緊急対応責任者は、速やかに緊急事態の発生原因の特定を行う。同時に、被

害状況を正確に把握するため情報を収集する。

b）各部門は、緊急対応責任者の指示の下、定常的な業務の遂行に優先して指示事項を実施する。

⑤恒久対策（再発防止）の要否の判断

a）恒久対策を行わない限り被害の拡大を停止できない場合、緊急対応責任者は緊急対策会議を招集し、緊急対策会議にて恒久対策を検討する。

b）既に上記③の対応により、被害の拡大が発生しない状況になっている（沈静化している）場合には、緊急対応責任者が発生原因と被害状況を元に、恒久対策の要否を判断する。

⑥恒久対策の実施

緊急対応責任者は、関係各部署と調整を行いつつ、恒久対策を実施または指示する。

⑦対策の有効性の確認

緊急対応責任者は、緊急対応のみで終了した緊急事態に対しては緊急対応の有効性を、恒久対策を実施した緊急事態に対しては恒久対策の有効性の確認を実施する。

⑧事故報告書の作成

個人情報管理責任者または緊急対応責任者は、上記②から⑥について「個人情報事故報告書」として記録する。同報告書は、経営者によるコンプライアンス・プログラムの見直し（個人情報管理　実施細則を参照）のインプットとする。

（4）緊急事態からの学習

a）個人情報管理責任者は、緊急事態が発生し、取り得る緊急対応が完了した段階、または恒久対策が完了した段階のいずれかにおいて、社内で情報を共有化する必要性の有無を判断する。

b）情報共有化が必要であると判断した場合、電子メールまたは会議体により、緊急事態の内容・状況および対応によって学んだ点を社員に伝える。

内部監査細則

Ver.20170401

制定日：2017 年 4 月 1 日

株式会社ネクストページ

承認(社長)	審査(個人情報管理責任者)	作成

目　　次

改訂履歴

年月日	改訂内容
平成 29 年 4 月 1 日	制定初版

Ⅰ　総則

１．目的

本細則は、当社の個人情報保護に関するコンプライアンス・プログラムが、計画された通りに実行されているかを検証するとともに、個人情報保護体制の有効性を判定するため、内部監査（以下、「監査」とする）の計画および実施について規定するものである。

２．適用範囲

（１）　対象組織：全社（当社に勤務する社員、準社員、契約社員、派遣社員、パートおよびアルバイトを含む）

（２）　対象となる個人情報：全部もしくは一部を電子計算機などの自動処理システムによって処理している、又は自動処理による処理を行うことを目的して書面などによって処理している個人情報だけでなく、何らかの規則により索引付けされた個人情報であれば、媒体に関係なく含む。具体的には、「個人情報管理台帳兼保管一覧」に定めた個人情報とする。

Ⅱ　内部監査の計画および実施

１．　内部監査人の認定

（１） 内部監査責任者は、以下のいずれかの基準を満たす内部監査人を認定し、「内部監査人登録リスト」に登録する。

① 外部研修機関でプライバシーマークに関する内部監査人の研修を受けた者

② 社内において、上記①と同等の研修を受けた者

２．　監査の種類

（１） 内部監査は、以下のように定期監査と臨時監査とに区分する。

定期監査	監査される活動の状況及び重要性に基づいて、内部監査責任者が作成した「年度教育・内部監査計画書」に従い、年 1 回（9 月）実施する監査
臨時監査	定期的な監査以外に、経営者、個人情報管理責任者、内部監査責任者の判断により、臨時的に行われる監査。なお、抜き打ちの場合もある。

３．　内部監査の計画

（１） 作成者および承認者

① 定期監査

毎年 8 月に、内部監査責任者が、次年度の「年度教育・内部監査計画書」を作成し、経営者が承認する。

② 臨時監査

内部監査責任者が実施の 1 週間前までに計画を立案し、経営者が承認する。その際、「内部監査スケジュール表」で代用しても良い。また、抜き打ちで内部監査を実施する場合には、作成を省略してもよい。

（２） 計画立案時の考慮事項

① 原則として全部門年１回は、監査を実施するように計画する

② 次のいずれかの条件に該当する部門については、年２回以上行うものとする。

ａ）過去１年以内に個人情報の取扱いに関してのトラブルなどが発生した部門

ｂ）仕事の手順が大きく変更となった部門

c）前回の内部監査で、指摘事項が著しく多かった部門
d）その他、経営者または、個人情報管理責任者が必要と判断した部門

４．　事前準備

（１）　内部監査責任者は、「内部監査登録人リスト」から、被監査部門との独立性を考慮して、それぞれの部門を監査する監査人を選任する。

（２）　選任された監査人は、被監査部門と監査実施日時等を調整し、内部監査責任者に報告する。これに基づき、内部監査責任者は、監査当日の「内部監査スケジュール表」を作成する。

（３）　選任された監査人は次の準備作業を行い、監査が有効かつ効率的に実施できるよう努める。

a）被監査部門に関係する規定、細則、手順書および記録の確認
b）監査における質問事項の洗い出し、および「内部監査チェックリスト」の作成
c）被監査部門に対して複数の監査人で監査を実施する場合は、主任監査人の選任

５．　内部監査の実施（監査当日の流れ）

（１）　オープニングミーティング

内部監査人は、被監査部門に対し、監査の実施目的、監査の範囲および監査のスケジュール等を説明し、協力を依頼する。

（２）　監査の実施

内部監査人は、「内部監査チェックリスト」を活用し、監査を実施する。

（３）　監査結果のまとめ

内部監査人は、指摘事項・改善指示事項を整理し、「内部監査報告書」を作成する。

（４）　クロージングミーティング

内部監査人は、被監査部門に対し、「内部監査報告書」に基づき監査結果の報告ならびに指摘事項およびその後の対応手続きを説明する。

その際、必要に応じて、被監査部門と協議し、是正処置・改善策の必要性を確認すると共に、是正処置・改善策の検討および実施を要請する。

６．　監査の結果報告

（１）　内部監査人は、「内部監査報告書」を内部監査責任者に提出する。

（２）　内部監査責任者は、各内部監査人から提出された「内部監査報告書」をとりまとめる。

（３）　内部監査責任者は、とりまとめた内部監査の結果を、個人情報管理責任者および経営者に報告する。

７．　フォローアップ監査

（１）　被監査部門は、内部監査で指摘された指摘事項・改善指示事項について、原因の調査を行い、是正処置・改善策を立案する。

（２）　被監査部門は、立案した是正処置・改善策を実施し、内部監査責任者はその結果を「内部監査報告書」に追記する。

（３）　被監査部門は追記した「内部監査報告書」を、内部監査責任者に提出する。

（４）　内部監査責任者は、被監査部門から提出された「内部監査報告書」を確認し、承認する。ただし、是正処置・改善策に不備がある等、必要であれば、再度、是正処置または改善策の実施を要請する。