印刷業 情報セキュリティマネジメントシステム（PISM）

規格要求事項

目次

1.適用範囲

この規格は、印刷業における、個人情報保護を含む情報セキュリティマネジメントに関する要求事項を規定するものである。ただし、当規格は、個人情報保護を含む情報セキュリティマネジメントに取組むあらゆる事業体も使用することができる。

また、個人情報保護とのかかわりでは、当規格は、次のような使い方ができる。

１）個人情報保護のみに限定した情報セキュリティに取組む。

２）個人情報保護を除く情報セキュリティに取組む。

３）個人情報保護を含む情報セキュリティ全般に取組む。

なお、この規格は、次の事項を行う際に用いることができる。

１）個人情報保護を含む情報セキュリティマネジメントシステムを構築し、実施し、維持し、改善する。

２）事業体の情報セキュリティマネジメントシステムが当規格に適合しているかどうかを自ら確認し、自ら宣言する。

３）事業体の情報セキュリティマネジメントシステムが当規格に適合しているかどうかについて、を外部機関に確認を求める。

２．要求事項

２．１ 一般要求事項

事業体は、この規格の要求事項にしたがって、情報セキュリティマネジメントシステムを確立し、文書化し、実施し、維持し、継続的に改善しなければならない。

２．２ 情報セキュリティ方針の策定

経営層は、情報セキュリティに取組むための方針を策定すること。その方針は、次の事項を最低限、満たさねばならない。

１）情報セキュリティに取組むことを記すること。

２）個人情報保護に取組む場合には、その旨を記すること。

３）適用を受ける法令や条例を遵守することを記すること。

４）構築した情報セキュリティマネジメントシステムの継続的改善に努めることを記すること。

５）情報セキュリティ方針は、文書化すること。

６）情報セキュリティ方針の文書には、事業体の代表者名を記すこと。

７）情報セキュリティ方針は、事業体内に周知するとともに、外部に公表すること。

２．３ 計画の策定

２．３．１ 対象の特定

事業体は、個人情報を含む情報セキュリティの対象を特定するための手順を確立し、実施し、維持しなければならない。

２．３．２ 法的ならびにその他の要求事項の特定

事業体は、対応すべき、情報セキュリティに関わる法令や条例、その他、事業体が同意した要求事項を特定し、参照する手順を確立し、実施し、維持しなければならない。

２．３．３ 情報リスクの分析

事業体は、２．３．１で特定した情報に関わるリスクを分析し、対策を特定する手順を確立し、実施し、維持しなければならない。

２．３．４ 目的・目標の策定

１）事業体は、情報セキュリティマネジメントに取組むための目的および目標を策定すること。

２）目的および目標は、定性評価ないし定量評価ができること。

２．３．５ 実施計画の策定

事業体は、策定した目的・目標を達成するための実施計画を文書で作成し、実施すること。

２．４ 実施

２．４．１ 経営資源

経営層は、特定した情報セキュリティに取組むための経営資源を利用できるようにすること。

２．４．２ 組織体制と役割

１）事業体は、情報セキュリティマネジメントに関わる組織体制を整えること。

２）経営層は、情報セキュリティに関わる管理責任者を任命すること。

３）管理責任者は、以下の事項についての責任と権限を持つこと。

①情報セキュリティマネジメントシステムの確立、実施、維持。

②情報セキュリティマネジメントシステムの実績を経営層に報告すること。

４）管理責任者については、組織内に周知すること。

２．４．３ 能力開発

事業体は、情報セキュリティに取組むために必要な力量を明確にし、その育成を図ること。教育・研修に当たっては、次のことを理解させる手順を確立し、実施し、維持すること。

１）情報セキュリティマネジメントシステムに適合する重要性や意味。

２）情報セキュリティマネジメントシステムを運用する役割と責任。

３）情報セキュリティに反することによって生ずる問題や損害。

２．４．４ 文書管理

事業体は、情報セキュリティマネジメントシステムの運用に必要な文書を適切に管理する手順を確立し、実施し、維持すること。なお、手順は、以下の事項を含むこと。

１）文書の適切性を確認して発行する。

２）定期的もしくは適宜見直しを行い、改訂版を発行する。

３）最新版が識別できる。

４）廃止文書が誤用されない。

５）文書がわかりやすく容易に理解できる。

２．４．５ 記録管理

事業体は、情報セキュリティマネジメントの実績および情報セキュリティマネジメントシステムの当規格への適合を客観的に示す記録を作成し、保管すること。

２．４．６ 運用管理

１）事業体は、情報セキュリティマネジメントのための規定を作成すること。規定は、最低限以下の事項を含むこと。

①情報の適正な取得、利用、提供、処分に関すること。

②情報媒体、情報機器、情報保管場所、人的対応などを含めた情報の適正な管理に関すること。

③苦情処理に関すること。

２．４．７ 危機管理

１）事業体は、情報クライシスを定義すること。

２）事業体は、情報クライシスの発生を防止するための手順を確立し、実施し、維持すること。

３）事業体は、情報クライシスが発生した際の対処の手順を確立し、実施し、維持すること。

４）事業体は、情報クライシスが発生した場合、情報クライシスに関する情報開示を適切に行う手順を確立し、実施し、維持すること。

５）事業体は、発生した情報クライシスの原因を明らかにし、再発防止のための是正措置を図ること。

２．５ 点検

２．５．１ 測定

事業体は、情報セキュリティマネジメントの成果を定常的に監視し、測定するための手順を確立し、実施し、維持すること。

２．５．２ 法的要求事項およびその他の要求事項の遵守評価

事業体は、「２．３．２」で特定した要求事項の遵守状況を定期的に評価する手順を確立し、実施し、維持すること。

２．５．３ 不適合の是正、是正措置、予防措置

事業体は、当規格への不適合に対する是正、是正措置、予防措置に関する手順を確立し、実施し、維持すること。手順には、以下の事項を含むこと。

１）不適合を特定し、それに対する応急措置をとり、影響を緩和するための是正を実施

すること。

2）不適合の発生原因を特定し、再発防止の是正措置をとること。

3）不適合を予防する必要性を評価し、必要に応じて予防措置をとること。

4）実施された是正措置や予防措置の結果を記録し、有効性を検討すること。

2．5．4 内部監査

事業体は、情報セキュリティマネジメントに関わる内部監査を実施するための文書化された手順を確立し、実施し、維持すること。手順は、以下の事項を盛ること。

1）経営層は、情報セキュリティに関わる監査責任者を任命すること。

2）事業体の情報セキュリティマネジメントシステムが当規格の要求事項や事業体の情報セキュリティマネジメントのために決定された事項に合致しているかを監査すること。

3）事業体の情報セキュリティマネジメントシステム適切に実施されており、維持されているか監査すること。

4）監査結果が経営層に確実に報告されること。

5）監査の計画、実施、結果報告、監査記録の保管に関する責任と要求事項を定めること。

6）監査の範囲、頻度、実施方法を規定すること。

2．6 マネジメントレビュー

2．6．1 マネジメントレビューの実施

経営層は、情報セキュリティマネジメントに関わるマネジメントレビューを実施する手順を確立し、実施し、維持すること。手順には、以下の事項を含むこと。

1）マネジメントレビューを定期的に実施する間隔に関すること。

2）マネジメントレビューを臨時で実施する条件に関すること。

3）マネジメントレビューでは、以下についてレビューされること。

①内部監査結果。

②情報セキュリティへの取り組み成果。

③情報セキュリティに関わる苦情を含む利害関係者の声や反応。

④情報セキュリティに関わる苦情への対応。

⑤前回のレビュー結果を受けたその後の経緯。

⑥「2．3．2」で特定された法令等の遵守状況。

⑦改善のための提案。

２．６．２ 情報セキュリティに関わるコミュニケーション

事業体は、情報セキュリティに関わる利害関係者とのコミュニケーションのための手順を確立し、実施し、維持すること。手順は、次の事項を含むこと。

１）情報セキュリティマネジメントの成果や課題を利害関係者に情報を伝える。

２）情報開示の頻度や時期、方法。

３）事業体の情報セキュリティに関わる取り組みや情報開示に関する利害関係者の声や反応を入手すること。

４）利害関係者の声や反応を入手する頻度や時期、方法。

５）利害関係者の声や反応を分析し、取り組みに生かすこと。