対策の手順（組織体制整備等）

ここで説明している手順は、P（プライバシー）マーク要求事項「JISQ 15001」　を基本としていますが、必ずしも、それに沿ったものとはなっておりません。学校での個人情報保護体制の整備に役立つよう解説しています。

1　計画

1）個人情報保護方針の決定

個人情報保護方針を定め、文書化する。

①　個人情報の収集、利用及び提供に関して
②　個人情報へのリスクの予防並びに是正に関して
③　個人情報に関する法令及びその他の規範の遵守に関して
④　継続的改善に関して

2）委員会の設置

①　個人情報保護管理者（CPO　チーフ・プライバシー・オフィサー）の設置

・学校の理念を実践的な個人情報保護計画として、活動する責任者を任命する
・学校責任者等による支援
・個人情報保護管理者は計画の展開を調整する

②　対策本部・プロジェクトチームの設置

・役員、各部門の代表者、監督者、技術者等
・部門の代表者は、各部門内でチームを結成する
・対策本部のスキルチェック、研修の実施
・スケジュール化、定期的ミーティング
・メンバー間で意思疎通をうまく図るための方法を確立する
・部門間での作業分担、誰がどのような責任を負い、誰がスケジュール管理をするか、等の特定

3）個人情報の特定（台帳の作成）

・学校で取り扱っている個人情報の特定
個人情報の入手目的、入手経路、学校内での取り扱い経路（部門）、保管（一時保管も含む）場所、保管形態（電子媒体、紙等）、保管期間、廃棄方法について明らかにする。

＊個人情報の特定（棚卸し）は、リスクの評価、対策などとも関わって来ます。最も大変な作業でもありますが、非常に重要な作業です。

4）リスクの認識・分析、対策の決定

特定した個人情報に対しての、合理的な安全対策

① 個人情報取扱業務の中で、どのようなリスクが存在するか、洗い出しを行う。

個人情報に関するリスクの例
- a 個人情報への不正アクセス
- b 個人情報の紛失
- c 個人情報の破壊
- d 個人情報の改ざん
- e 個人情報の漏えい

② リスクに合った対策

- a アクセス制限
- b 鍵（金庫、書庫、パスワード、暗号化等）による管理
- c PC 等の機器類の措置
- d 輸送路上の措置
- e 委託時の措置
- f 障害対策

③ 絶えずリスクの状況確認をする

5）各種規程類の作成

リスク評価、対策に基づく規程類の作成

① 基本規程（個人情報の取り扱いに関する基本原則を定めたもの）
個人情報の収集、利用、提供、適正管理義務、情報主体の権利への対応、社員教育、苦情等への対応、監査、文書管理などの基本的考え方を取り決めたもの。ガイドライン等の参考も必要。

② 詳細規程（担当部署、担当者が実際にとるべき行動を詳細に規定したもの）
・各部門、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
・個人情報の収集、利用、提供及び管理の規定
・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
・個人情報保護に関する教育の規定
・個人情報保護に関する監査の規定
・内部規程の違反に関する罰則の規定
・個人情報のリスクに対する予防措置の規定
・文書管理の規定

6）実施体制の整備

① 個人情報を保護するための権限及び責任の規定に基づいた、体制を整備する。役員、従業員に周知する。

② 監査担当・責任者の設置、監査実施体制の整備
内部監査、外部監査の何れの場合も、独立性が保たれること。

7）教育の実施 （教育、研修、学校内への周知徹底）

① 目的
従業員に個人情報保護の目的を知らせ、各従業員の役割の重要性を知らせる。

② 学校内研修例
・管理職レベル
・個人情報保護担当者レベル
・一般従業員レベル
・新人オリエンテーション時

③　学校内への周知徹底
個人情報保護に対する、学校内の認識を構築するため、既存のツールと技術を利用して、従業員に情報を伝える。

・ニュースレター
・掲示板
・回覧
・給与明細、保険書類に同封する
・ロゴ、スローガンの利用
・休憩所、事務所にポスター等を貼る
・管理者などからの発表
・学内でスケジュール化されている研修での発表

8）関係先への周知

①　保護者等へのメッセージ
②　関係企業、組織、取引先、メディア等も検討する。
・「個人情報を保護するために特別な努力」をしていることを伝える。
・ウェブサイト、ニュースレター、郵便物への同封書類、広告などの利用。

2　実施（運用）

1）個人情報の収集に関して
- 「目的」の達成に必要な範囲
- 適法、公正な手段
- 直接、間接収集する場合の措置

2）利用及び提供に関して
- 収集目的の範囲内で
- 収集目的の範囲外の場合の事前同意

3）適正管理業務に関して
- 正確かつ最新の状態
- 合理的な安全対策
- 委託先の選定基準

4）情報主体の権利に関して
- 開示、訂正、利用停止などを求められた場合

5）苦情、相談窓口の設定

3　監査

- 定められた規定類に従って業務手続が適切に行われたか、運用状況の定期的監査
- 監査実施結果の取りまとめと、代表者への報告

4　見直し

- 代表者による見直し
- 監査報告書、個人データに対する社会通念の変化及び情報技術の進歩に応じた定期的な見直し及び改善