

# 情報セキュリティ基本規程

特定非営利活動法人 せたがや子育てネット

## 第1章 総則

### (目的)

第1条 この規程は、当法人の情報セキュリティ管理に関する基本的な事項を定めたものです。

### (定義)

第2条 この規程に用いる用語の定義は、次のとおりです。

- (1)「情報資産」とは、情報処理により収集・加工・蓄積される情報・データ類、情報処理に必要な情報システム資源（ハードウェア、ソフトウェア等）、情報通信ネットワーク及び情報システムとそれらを支える関連インフラの総称。情報資産には個人情報が含まれます。
- (2)「情報セキュリティ」とは、情報の機密性、完全性および可用性を維持すること。
- (3)「機密性」とは、アクセスを許可された者のみが情報にアクセスできることを確実にすること。
- (4)「完全性」とは、情報及び処理方法が、正確かつ完全であることを保護すること。
- (5)「可用性」とは、許可された利用者が、必要なときに、情報及び関連する資産にアクセスできることを確実にすること。
- (6)「個人情報」とは、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、または個人別に付けられた番号、画像、音声等によって当該個人を識別できるもの。
- (7)「情報形態」とは、情報が記録・保管される機器・設備の状態をいい、紙、電子媒体、電子ファイルの3つに区分されます。
- (8)「情報機器」とは、情報が収集・加工・蓄積される PC、サーバー、コピー機、Fax、電話等の機器類。
- (9)「情報システム」とは、情報機器・媒体などのハードウェア、プログラムなどのソフトウェア及び通信回線で構成される情報処理を行うシステム。

### (適用範囲)

第3条 本規程は、全ての職員に適用されます。

## 第2章 情報セキュリティ基本方針

### (基本方針)

第4条 情報セキュリティの基本方針は次のとおりです。

- (1)情報資産は、当法人の経営を支える重要な資源であることを全職員が十分に認識し、情報セキュリティの確保に努めること。

- (2)情報資産の重要度に応じた適正な保護と有効活用を行うこと。
- (3)顧客情報資産に関して、当法人の情報資産と同等の適正な管理を行うこと。
- (4)個人情報保護に関する関係法令、各省庁のガイドライン及び当法人の関連規程を遵守すると共に、これらに違反した場合には厳正に対処すること。

#### (個人情報保護)

第5条 個人情報保護に関しては、「個人情報保護法」第3条に規定される、「個人の人格尊重を基本理念として慎重かつ適正な取扱いを行う」に準じてください。

2 個人情報保護に関する関連規程「個人情報保護規程」等に、具体的な定めがある場合にはそれに従ってください。

### 第3章 情報セキュリティ管理体制

#### (情報セキュリティ管理者)

第6条 当法人は、情報セキュリティ管理者を選任します。

2 情報セキュリティ管理者は、以下の業務を実施する責任を負います。

- (1)本規程に定められた、情報セキュリティに関する事項の遵守
- (2)職員に対する情報セキュリティ教育・訓練を統括
- (3)本基本規程及び関連する規程・マニュアル等の管理
- (4)情報セキュリティに対する、改善計画を立案し合理的な安全対策を講ずる
- (5)その他、情報セキュリティ確保に必要な業務

### 第4章 情報資産の分類とリスク評価

#### (情報資産の分類と管理)

第7条 情報セキュリティ管理者は、情報資産の機密分類を行い適正な管理を実施します。

2 セキュリティ管理者は、定期的に情報資産の棚卸、機密分類の見直しを実施します。

3 情報資産は機密分類に基づき取扱います。

#### (情報資産の棚卸しとリスク評価)

第8条 情報セキュリティ管理者は、管理対象となる情報資産の棚卸しを定期的に行い、その情報資産の価値を把握し、また、その情報資産に対して発生可能性のある自然発生的災害・故障及び人為的故意・過失によってもたらされる脅威の大きさを把握し、情報資産のリスクを評価します。

### 第5章 情報資産の管理

(情報資産の調達)

第 9 条 情報セキュリティ管理者は、基本方針に基づき、セキュリティ管理を実現する上で必要な情報システム資源・設備の導入を検討します。

(教育訓練)

第 10 条 情報セキュリティ管理者は、全職員に対し、情報セキュリティに関する教育訓練を計画的に実施します。

(職員の管理)

第 11 条 情報セキュリティ管理者は、職員が情報を取り扱うに際しては、情報セキュリティの安全管理が図られるよう、当該職員に対して必要かつ適切な監督します。

2 セキュリティ事故の発生に備え、重要な情報資産についてはデータ更新の都度バックアップを取ります。

(情報資産の持出し)

第 12 条 情報セキュリティ責任者は、情報資産が記録されている機器、情報媒体等を社外に持出す場合には、漏えい、改ざん、盗難、紛失等が生じないような安全対策を実施します。

(情報資産の廃棄)

第 13 条 情報セキュリティ責任者は、重要な情報を記録保管した装置・媒体に対しては、物理的にデータ域を破壊するか、データ域を確実に上書きした後に廃棄処分します。

2 記憶媒体（ハードディスク等）を内蔵している装置に対して、その全ての部品をチェックし、重要なデータやライセンス供与のソフトウェアが完全に削除または上書き消去されていることを確認した後に廃棄処分します。

(業務委託先等の管理)

第 14 条 情報セキュリティ責任者は、セキュリティ管理に関する必要事項を、システムの利用を希望する関連会社及び業務委託先等へ提示し遵守します。

2 情報セキュリティ責任者は、関連会社及び業務委託先等が、セキュリティ管理の関連規程に対する違反を行った場合は、直ちに必要な処置を行います。

3 情報セキュリティ責任者は、関連会社及び業務委託先等との間で機密保持契約を取り交わします。

## 第 6 章 人的管理

(教育及び訓練)

第 15 条 情報セキュリティ責任者は、職員に対して情報セキュリティに関する教育を実施し、情報セキュリティに関する関係法令及び本基本規程を含む規程等を理解・遵守させることに努めます。

## 第7章 アクセス管理

### (アクセス管理の基本原則)

第16条 職員は、ユーザID、パスワードを適切に管理してください。

### (システムのアクセス管理)

第17条 第三者による不正なアクセスを防止するため、侵入検知・監視システムの導入、ネットワークの分離・接続制御及びアクセス経路の統一等適切な管理を実施します。

### (リモートアクセス)

第18条 社外からネットワークを介して当法人の情報資産にアクセスする場合には、定められた手続きにより申請を行ってください。

## 第8章 通信

### (通信手段の選択)

第19条 通信対象となる情報資産の重要度を考慮して、適切な通信手段を選んでください。

### (電子メール)

第20条 電子メールを使用する場合は、漏えい、改ざんのリスクを考慮し、対象となる情報資産の重要度によっては、利用可能な別の通信手段を用いることを検討します。

2 個人情報が含まれる情報通信には、電子メールを使用してはいけません。緊急時等でやむを得ず利用する場合には、暗号化処理をします。

### (Fax)

第21条 Faxを通信手段として利用する場合には、送信前後に相手と電話連絡を取り交わし、安全確保に努めてください。

## 第9章 情報システムの利用者の責務

### (情報システム利用者の義務)

第22条 当法人の職員は、情報システム利用にあたり以下の事項を守ってください。

(ア) 情報システムの利用者は、本基本規程及び関連規程を守ってください。

(イ) 情報システムの利用者は、情報漏えい防止に努めてください。

(ウ) 情報システムの利用者が本規程に違反した場合には、就業規則等に定める罰則が適用されます。

(工) 情報システムの利用者は、当法人が実施する情報セキュリティに関する教育・訓練を定期的に受講し、セキュリティ意識の向上と適正な管理運用に努めてください。

(セキュリティ事故発生時の対応)

第 23 条 職員は、セキュリティ欠陥、ソフトウェア誤動作及びセキュリティ事故等を発見した場合、速やかに情報セキュリティ責任者へ報告しその指示に従ってください。

## 第 10 章 重大事故への対応

(重大事故への対応)

第 24 条 システム事故の発生に備え、その対応手順については別に定めます。

2 重大事故が発生した場合、情報セキュリティ管理者は、事故の拡大防止に努めるとともに復旧対策をたてます。

## 第 11 章 雑則

(その他)

第 25 条 この規程の実施に必要な事項は、別に定めるものとします。

附則

この規則は平成 27 年 4 月 1 日から実施します。

以上