

情報セキュリティ・管理規程

第1章 総則

(目的)

第1条 本規程は、認定特定非営利活動法人育て上げネット（以下、「当法人」という。）の保有する情報資産の適切な管理のために必要な事項を定めることにより、当法人の業務の適正かつ円滑な運営を図るとともに、情報セキュリティに関する行動規範を示し高い情報セキュリティレベルを確保することにより、法人活動に寄与することを目的とする。

(定義)

第2条 本規程において、次の各号に掲げる用語の定義は、当該各号のとおりとする。

①情報資産

情報およびその関連の資産をいい、情報記録媒体、情報利用手段、情報保管手段、情報システム、ネットワークなどを含む。

②秘密および機密情報

法人の情報資産の中で、許可した者以外への開示、目的外に利用された場合、法人の経営資源としての価値を損ね、法人の信用を毀損する恐れのある以下の情報をいう。

1. 業務で取扱う個人情報（記録画像・映像等を含む）
2. 業務上知り得る技術や営業に関する情報
3. 財務、人事、組織等に関するもので特定個人情報を含む情報
4. 他関係機関との業務提携および業務取引に関する情報
5. その他、法人が秘密保持対象として取扱う一切の情報

③総括保護管理者

法人の情報セキュリティを統括管理しその責任を負う者をいう。

④情報セキュリティ担当者

総括保護管理者の指揮、監督の下で保護管理者と連携を取り、情報セキュリティ管理の維持および充実に努める者をいう。

⑤保護管理者

情報セキュリティ確保のため各職員を統括し、情報資産および情報セキュリティの管理を行う者をいう。

⑥職員

理事、役員、職員、フェロー、インターン等名称や雇用条件にかかわらず、当法人の業務及び活動にかかわるすべての者をいう。

(適用範囲)

第3条 本規程は、全ての職員および元職員に適用する。

(規程の改廃)

第4条 本規程の施行および変更並びに廃棄は、総括保護管理者が提案し、経営ボード会議で承認した後、総務担当が通達するものとする。

第2章 情報セキュリティの保持義務

(情報セキュリティの方針)

第5条 情報セキュリティの保持は、日常の法人活動、業務推進、組織運営の一環として取り組む。

- 2 情報セキュリティの保持は、全職員の責務であり、経営資源と同様に組織を通じて管理する。
- 3 上記に基づく法人の情報セキュリティ・管理に関する方針を「情報セキュリティ・管理の基本方針」として定め、常に法人内外より確認出来る状態に置く。
- 4 「情報セキュリティ・管理の基本方針」に基づき承認された情報セキュリティの維持・管理のために必要な規程、規則等を、職員及び元職員は、それらの内容を遵守しなければならない。

(目的外利用の禁止)

第6条 情報は、定められた目的以外には使用してはならない。

- 2 情報資産および情報システムは、私的な目的に利用してはならない。
- 3 情報は、非法的な手段による利用、各規程・規則に違反した利用および社会通念に反する利用をしてはならない。
- 4 情報は、提供を強要してはならない。

(誓約書の提出)

第7条 職員は、入職時に「秘密保持及び個人情報に関する誓約書」に署名・捺印をしなければならない。

- 2 上記誓約書は、退職後も効力を持つものとする。

第3章 情報セキュリティの管理体制

(総括保護管理者)

第8条 当法人に、総括保護管理者1名を置き、事務局長をもって充てる。

- 2 総括保護管理者は、法人の情報セキュリティ・管理に関する事務を統括する。

(情報セキュリティ担当者)

第9条 当法人に情報セキュリティ担当者1名を置き、総務担当プロジェクトマネージャーをもって充てる。

- 2 総括保護管理者の指揮、監督の下で保護管理者と連携を取り、情報セキュリティ管理の維持および充実に努める。

(保護管理者)

第10条 法人内の各事業所に保護管理者1名を置き、当該事業所の長をもって充てる。

- 2 保護管理者は、情報セキュリティ確保のため、各職員を統括しなければならない。
- 3 保護管理者は、情報資産および情報セキュリティの管理を行う。
- 4 保護管理者は、情報セキュリティ・管理の維持および充実に努め、点検を行い、その結果を情報セキュリティ担当および担当執行役員に報告するものとする。

(監査責任者)

第11条 当法人に監査責任者1名を置き、総務担当執行役員をもって充てる。

- 2 監査責任者は、年1回定期的に全事業所の情報セキュリティ・管理について監査を行い、また必要に応じて監査を行う。
- 3 前項の監査結果を総括保護管理者に報告する。

(重要事項の決定等)

第12条 当法人における情報セキュリティ・管理に係る重要事項の決定および変更は経営ボード会議にて行う。

- 2 前項の決定および変更の通達等は総務担当執行役員が行う。

第4章 秘密および機密情報の管理

(職員の責務)

第13条 職員は、その趣旨に則り関連する法令及び諸規程等の定め並びに総括保護管理者及び保護管理者の指示に従い、秘密および機密情報を取り扱わなければならない。

- 2 関係機関との業務提携および業務取引に関して、関係機関が秘密もしくは機密と指定し提供した情報は秘密および機密情報として取扱う。

(秘密および機密情報区分の設定)

第14条 法人の秘密および機密情報は、区分を設定する。

- 2 区分の付与および変更は、関連情報との整合性確保をし、総括保護管理者および総務執行役員並びに情報セキュリティ担当が協議をして立案し、経営ボード会議にて決議する。
- 3 総括保護管理者は、法人の秘密および機密情報の区分を適宜、見直さなければならない。
- 4 総括保護管理者は、秘密および機密情報区分とその変更内容について、法人内に周知徹底しなければならない。

(アクセス権限の管理)

第15条 秘密および機密情報へのアクセス権限は、保護管理者が内容を確認し、情報セキュリティ担当者へ申請する。

- 2 情報セキュリティ担当者は、内容を確認しアクセス権限を付与するものとする。
- 3 秘密および機密情報へのアクセス許可は、担当業務に必要な範囲とする。
- 4 保護管理者は、秘密情報へのアクセス状況を定期的に点検しなければならない。

- 5 他社の秘密もしくは機密情報へのアクセス管理は、秘密保持契約に基づき行う。契約締結先よりアクセス状況の開示要求がある場合は、速やかにこれに応じるものとする。

(個人情報の取扱い)

第16条 個人情報の取扱いについては、個人情報保護法、特定個人情報保護法および関連する規程に準じて行うものとする。

(立入禁止区域)

第17条 法令および情報セキュリティ・管理に関する諸規程に基づき、立入禁止区域を設定する。

- 2 立入禁止区域への入退出は、総括保護管理者により指定された者のみとする。

(情報機器利用の制限)

第18条 以下の機器については利用をしてはならない。

- ① 私有IT機器 (パソコン、スマートフォン、携帯電話など)

ただし、業務上必要があると情報セキュリティ担当が認める場合には、私有IT機器取扱規程に基づき利用を認める。

- ② USB メモリ

原則利用してはならないが、業務上必要があると認める場合には、保護管理者の許可のもとに認める。

(通信サービス、ソフトの利用の制限)

第19条 以下の環境、サービスについては利用をしてはならない。

- ① FreeWiFi
- ② ファイル交換ソフト (Winny など)

第5章 秘密保持の契約

(契約前の秘密情報の管理)

第20条 契約を締結するに際して、事前に一定の情報を開示する場合には、情報開示の前に「秘密保持契約書」を締結するものとする。

- 2 秘密保持契約を締結するにあたって、次の点に留保し、実行することとする。

- ① 法人の情報セキュリティ・管理規程に従って、契約書を確認し、締結すること。
- ② 提供する必要のある情報は、事前に総括保護管理者の承諾を得ること。
- ③ 提供する、あるいは提供された情報のすべてを記録しておくこと。

- 3 保護管理者は、秘密保持契約を締結した後において、常時、提供した情報の管理状況、担当者の変更の有無、変更した場合は新たに秘密保持義務の確認を実施し、かつ現実の管理状況を把握し、管理するものとする。

(取引先との契約)

第21条 秘密および機密保持契約を締結しない場合は、当該契約書に次の各号を規定しなければ

ばならない。

- ①秘密情報の複製
- ②秘密情報の送信
- ③秘密情報が記録されている媒体の外部への送付又は持出し
- ④その他秘密情報の適切な管理に支障を及ぼすおそれのある行為
- ⑤情報開示

(取引先との契約)

第22条 取引先に秘密情報を開示する必要がある場合には、情報開示に関する契約を締結しなければならない。

(契約)

第23条 秘密保持契約の承認は、理事長もしくは総括保護管理者が行うものとする。

(取引先秘密情報へのアクセス)

第24条 取引先の秘密および機密情報へのアクセスは、総括保護管理者もしくは保護管理者が許可した場合に限る。

- 2 職務上の立場を利用して、他法人に秘密情報の提供を強要してはならない。

第6章 危機管理

(危機管理)

第25条 危機管理に関しては、その方針と危機管理を必要とする事態を想定したマニュアルを定めるものとする。

- 2 保護管理者は、上記方針及びマニュアルに定める内容に従い、事業所職員に危機管理策の内容を周知し、徹底するものとする。

(危機発生時の対応)

第26条 情報セキュリティ・管理に関する緊急事態が発生した場合は、上記マニュアルに基づき対応を行う。

第7章 教育

(教育)

第27条 保護管理者は、事業所職員に対し情報セキュリティ教育を定期的実施する。

- 2 情報セキュリティ担当は、総括保護管理者の管理の下で情報セキュリティの管理状況について保護管理者に発信し、情報セキュリティの質の向上に努める。

第8章 リスク評価

(リスク評価)

第28条 総括保護管理者は、技術の進歩や業務環境の変化等も考慮のうえ、情報資産のリスク評価を多方面から継続的に実施し、それを情報セキュリティ・管理の基本方針およびそれに基づく各種施策に反映させることにより、情報セキュリティ・管理の維持・向上に努めるものとする。

第9章 監査

(監査の実施)

第29条 監査責任者は、年1回定期的に全事業所の情報セキュリティ・管理監査を実施し、また必要に応じて監査を行う。

- 2 総括保護管理者は、監査責任者による監査結果に基づき是正措置を行う。
- 3 監査責任者は、監査の実施方法、内容、時期など監査実施計画書を作成する。

第10章 罰則

(罰則)

第30条 法令ならびに情報セキュリティ・管理規程および情報セキュリティに関する諸規程に違反した者は、就業規則に基づき懲戒に処す。

- 2 退職した者についても、違反行為が認められる場合は前項に準じた扱いとする。

付 則

この規程は、平成28年11月1日から施行する。

平成31年4月1日 改定