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、特定非営利活動法人 NPO まんま（以下「この団体」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、この団体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、団体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

この団体の情報資産の中で、許可した者以外への開示、目的外に利用された場合、この団体の経営資源としての価値を損ね、この団体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、この団体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

この団体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、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 職員

理事、役員、職員等名称や雇用条件にかかわらず、当団体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、理事会で承認した後、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、日常の団体活動、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　上記に基づくこの団体の情報セキュリティ・管理する方針を「情報セキュリティ・管理の基本方針」として定め、常にこの団体の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、それらの内容を順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、非合法な手段による利用、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、１年に一度「秘密保持及び個人情報に関する誓約書」に署名をしなければならない。

２　上記誓約書は、退職時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　当団体に、総括保護管理者１名を置き、代表理事をもって充てる。

２　総括保護管理者は、この団体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　この団体に情報セキュリティ担当者１名を置き、理事をもって充てる。

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

（重要事項の決定等）

第１２条　この団体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理事会にて行う。

２　前項の決定および変更の通達等は代表理事が行う。

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及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　この団体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情報セキュリティ担当者が協議をして立案し、理事会にて決議する。

３　総括保護管理者は、この団体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、この団体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、総括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　他団体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。

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 この団体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。

（取引先との契約）

第２１条　秘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、総括保護管理者が行うものとする。

（取引先機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、総括保護管理者が許可した場合に限る。

２　職務上の立場を利用して、他団体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　総括保護管理者は、上記方針及びマニュアルに定める内容に従い、団体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　総括保護管理者は、事業所職員に対し情報セキュリティ教育を定期的に実施する。

２　情報セキュリティ担当者は、総括保護管理者の下で、情報セキュリティ・管理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。

（監査の実施）

第９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、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。

附則

この規定は２０２４年１０月１０日から施行する。