情報セキュリティ関連規程

第１章　総　　則

（目的）

第１条　この規程は、社会福祉法人青谷学園（以下「法人」という）が、デジタル技術を活用した事業変革（以下「ＤＸ」という）を推進するにあたり、情報セキュリティ基本方針に基づき、情報資産を適切に活用・保全・運用するための情報セキュリティ対策に関する事項を定める。

（適用範囲）

第２条　この規程は、法人の情報資産にアクセスするすべての者（以下「従業者」という）に適用する。ここでの従業者とは、役員、正規職員、非正規職員、および業務委託先など、法人の業務に関わるすべての者を指す。

（ＤＸ推進と情報セキュリティ）

第３条　法人は、ＤＸ戦略ビジョンの実現に向け、情報セキュリティを事業継続の基盤と位置づけ、組織全体で計画的かつ継続的に取り組む。

（用語の定義）

第４条　この規程における主な用語の定義は次のとおりとする。

（1）情報セキュリティ：情報資産の機密性、完全性、可用性を維持することをいう。

（2）情報資産：法人が業務上保有するすべての情報、情報システム、ネットワーク、情報機器、記録媒体等をいう。

（3）ＤＸ推進：データとデジタル技術を活用し、サービスやビジネスモデルを変革するとともに、組織や業務プロセス、企業文化・風土を変革し、競争上の優位性を確立することをいう。

第２章　情報セキュリティ体制

（最高情報責任者）

第５条　業務執行理事は、最高情報責任者（以下ＣＩＯという）を兼務し、情報セキュリティ対策に関する最終的な責任を負う。ＣＩＯは、ＤＸ戦略ビジョンと情報セキュリティ施策の整合性を確保し、以下の職務を遂行する。

（1）ＤＸ戦略ビジョンの立案、全体最適化の推進、および主要なプロジェクトの管理

（2）ＤＸ推進成果の評価と、それに基づく戦略の見直しおよび経営層への提言

（3）情報セキュリティ基本方針および関連規程の改定の検討・提案

（4）ＤＸ推進・情報セキュリティ体制の構築と適切な人員配置

（5）ＤＸ推進・情報セキュリティ関連予算の確保

（6）インシデント発生時の最終的な判断と対応指示

（ＤＸ推進・情報セキュリティ管理者）

第６条　各事業所には、ＤＸ推進・情報セキュリティ管理者（以下管理者という）を置く。管理者はＣＩＯの指示のもと以下の職務を遂行する。

（1）ＤＸ戦略ビジョンに基づく施策の実行と管理、ならびに具体的な進捗および効果の測定
（2）日常的な情報セキュリティ対策の実施と管理
（3）ＤＸ推進および情報セキュリティに関する従業者への規程の周知と教育の実施
（4）情報資産の管理状況の確認と定期的な報告
（5）インシデント発生時の初動対応
（6）ＤＸ推進における成功事例やノウハウの収集、および組織内での共有促進

（ＤＸ推進・情報セキュリティ担当者）

第７条　ＤＸ推進・情報セキュリティ管理者を補佐するため、ＤＸ推進・情報セキュリティ担当者(以下担当者という)を置き、以下の職務を遂行する。
（1）現場の声を集約し、ＤＸ推進・情報セキュリティに関する課題や改善提案を管理者に報告する。
（2）情報セキュリティ対策の遵守状況について、現場での定期的な点検・確認を実施し、管理者に報告する。
（3）現場で発生した情報セキュリティに関する軽微な事象や懸念事項を速やかに管理者に報告する。
（4）管理者が実施する情報セキュリティ教育への協力(例：現場での実施支援、参加促進など)を行う。
（5）ＤＸ関連プロジェクトにおける施策が現場で円滑に実行されるよう、現場への説明や導入のサポートを行う。

第３章　情 報 資 産 の 管 理

（情報資産の分類）

第８条　情報資産は、その機密性、完全性、可用性の観点から、重要度に応じて次のとおり分類し、重要度に応じた適切な保護策を講じる。
（1）極秘情報：漏洩した場合、法人の事業継続に著しい影響を与える情報（例：個人情報、財務情報、知的財産）
（2）部外秘情報：漏洩した場合、法人に不利益をもたらす可能性のある情報（例：業務ノウハウ、内部資料）
（3）公開情報：漏洩した場合でも、法人に著しい影響を与えない情報

（情報システムの管理）

第９条　情報システムは、不正アクセス、マルウェア、情報漏洩等から保護するため、以下の対策を講じる。
（1）パソコンや法人のネットワークに対する外部からの攻撃と、内部からの情報漏洩を阻止するために多層防御によるＵＴＭ装置を設置する。
（2）無線ＬＡＮ機器を設置する際は、信頼性が高くセキュリティ強度の高い機種とするなど、不正接続されない対策を講じる。
（3）情報システムへのアクセス権限は、業務上の必要性に応じて最小限に設定し、定期的に見直す。
（4）クラウドサービスや外部サービスを利用する場合、事前にＣＩＯの承認を得る。また、サービスのセキュリティレベル、利用規約、責任範囲を評価・確認する。
（5）パソコンやスマートフォンなどの情報機器のＯＳや業務上使用するソフトウェアは、事前に許可されたもののみとし、常に最新の状態にする。
（6）パソコンやタブレットにはウイルス対策ソフトを常駐させ、ウイルス定義ファイルは常に最新の状態にする。
（7）従業員に貸与している携帯は、リモートワイプ機能のあるＭＤＭで管理し、紛失時の情報漏洩に備える。

（8）重要情報を２つのクラウドにバックアップするなどし、消失に備える。

（情報機器の管理）

第１０条　従業者は、法人から貸与された情報機器（パソコン、スマートフォン、タブレット等）を適切に管理し、以下の事項を遵守しなければならない。

（1）盗難・紛失に備え、画面ロックやパスワード設定、暗号化等の対策を講じなければならない。

（2）パスワードは、他者から推測されにくく、長く、複雑なものとし、他者に漏らさないこと。また、定期的に変更しなければならない。

（3）パソコンの不正使用防止と、セキュリティリスクを軽減するため、次のとおり取り扱わなければならない。

ア パソコンはスクリーンセーバーと「再開時にログオン画面に戻る」と設定し、待ち時間を３０分以上にしない。

イ パソコンから離れるときはスクリーンロックをする。

ウ パソコンから１５分以上離れるときはシャットダウンする。

エ 情報機器及び記憶媒体並びに重要情報を外部へ持ち出す場合は、管理者の許可を得なければならない。その記録を残し、持ち出し中はロックをかけるなど保管に注意し、終了した際は不要なデータを廃棄するなどし、管理者はそれらを確認しなければならない。

オ 個人所有の情報機器に法人所有のソフトをインストールしたり、法人から与えられたＩＤとパスワードを使用したりしない。ただし、緊急の事由で法人から指示が合った場合はこれを認める。

（4）ＵＴＭ等のセキュリティ機器、情報機器、記憶媒体や重要情報を置いている場所は、部外者の立ち入りを制限し、また、職員がいなくなる間は出入口扉を施錠する。また夜勤者は施錠を確認する。

（5）貸与している情報機器で、許可のない公衆無線ＬＡＮに接続したり、法人外で重要情報を送受信したりしない。また、覗き見にも注意する。

（6）退職時は、速やかに貸与されたすべての情報機器を返却する。

第4章　情 報 の 取 り 扱 い

（機密保持）

第１１条　従業者は、業務上知り得た機密情報、個人情報を、正当な理由なく他者に開示、漏洩してはならない。

（個人情報の保護）

第１２条　個人情報を取り扱う際は、個人情報保護法および関連規程を遵守し、適切な保護措置を講じる。

（ソーシャルメディア等の利用）

第１３条　法人アカウントのソーシャルメディアやブログ等で、業務に関連する情報を発信する際は、情報漏洩や法人の信頼性を損なうことがないよう、次の点に十分留意しなければならない。

（1）守秘義務、個人情報保護の原則を遵守すること。

（2）事実に基づかない不正確な情報や誤解を招く表現で発信しないこと。

（3）個人のプライベートに関する情報は、プライバシーに配慮し、慎重に取り扱うこと。

（重要情報の保管等）

第１４条　重要情報は基本的に指定のクラウドに保管することを原則とする。
２　紙で保管されている重要情報や、その他の記録媒体は、机の上に放置せず、鍵付き書庫等に保管し施錠しなければならない。

（重要情報の廃棄）
第１５条　重要情報が記録された媒体(書類、記憶媒体、情報機器等)を廃棄するときは、情報が復元できない方法で確実に処理しなければならない。
２　外部業者に溶解･焼却処分を委託する場合は、処理後に｢溶解証明書｣や｢廃棄証明書｣を徴し５年間保管しなければならない。

第5章　外部委託先の管理

（外部委託先の選定）
第１６条　情報システムの運用やデータ処理等の業務を外部に委託する場合は、委託先の情報セキュリティ対策状況を十分に評価し、ＣＩＯの承認を得なければならない。

（契約内容）
第１７条　外部委託先との契約には、情報セキュリティに関する以下の事項を明記しなければならない。
（1）遵守すべき情報セキュリティ対策
（2）秘密保持義務
（3）委託元(法人)による監査の受け入れ
（4）違反時の措置

第6章　教　育・訓　練

（情報セキュリティ教育）
第１８条　法人は、すべての従業者に対し、次の事項に関して情報セキュリティに関する教育・訓練を行う。
（1）新たな脅威や攻撃の手口についての対策
（2）電子メールの添付ファイルや本文中のＵＲＬリンクを介したウイルス感染
（3）ClickFix 攻撃などのインターネットを介したウイルス感染等
（4）電子メールやＦＡＸの送信ミスの防止策
（5）重要情報などはメール本文ではなくパスワード設定した添付ファイルとすること
（6）機密保持・守秘義務
（7）その他、社会的・技術的変化に合わせたセキュリティ

第7章　インシデント対応と事業継続

（インシデントの報告）

第１９条　情報セキュリティインシデント（情報漏洩、不正アクセス、マルウェア感染等）が発生、またはその兆候を察知した場合、ただちにネットワークから切り離し、速やかに管理者に報告し、管理者はＣＩＯに報告しなければならない。

（インシデント対応）

第２０条　管理者は、インシデント発生時に迅速に対応するための体制を整備し、被害の拡大防止、原因究明、再発防止策を講じなければならない。

（事業継続計画）

第２１条　法人は、大規模な災害、感染症流行、サイバー攻撃等の緊急事態発生時においても、重要な事業を継続できるよう、情報システムに関する事業継続計画（ＢＣＰ）を策定する。

第8章　評　価　・　見　直　し

（定期的な監査と見直し）

第２２条　ＣＩＯは、情報セキュリティ対策の有効性、適切性および遵守状況を確認し、継続的な改善を目的として、この規程に基づき、情報セキュリティ監査を年１回実施する。

２　前項の監査は、情報資産を適切に活用・保全・運用するための情報セキュリティ対策に関する事項すべてを対象とし実施する。

３　監査の実施者は、ＣＩＯまたは外部の専門機関とし、情報システムのアクセス権限、情報資産の取り扱い、インシデント対応体制、教育・訓練の実施状況等について、規程への準拠状況を評価する。

４　ＣＩＯは、監査結果に基づき、改善が必要な事項に対して是正措置を講じるとともに、ＤＸの進捗状況や社会情勢の変化に合わせ、必要に応じて規程の見直しを行う。

（規程の改廃）

第２３条　この規程の改廃は、理事会の承認を得て行う。

第9章　罰　　則

（規程違反に対する措置）

第２４条　この規程に違反した従業者には、就業規則に基づき懲戒処分の対象とする。

附　　則

この規程は、２０２５年１０月１７日制定、２０２５年１０月１７日から施行する。