情報セキュリティ規程

平成 21 年規程第 78 号
（最終改正：令和６年規程第 21 号）

第１章　総則

（目的）

第１条　この規程は、地方独立法人青森県産業技術センター（以下「法人」という。）が取扱う法人内外の情報を適切に管理するため、情報システムのセキュリティを確保するとともに、個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「法」という。）第 66 条第１項の規定に基づき、保有個人情報の漏えい、滅失又は毀損の防止その他の保有個人情報の安全管理のために講ずべき必要かつ適切な措置について定め、もって、法人が継続的かつ効率的に業務を遂行し、社会的信頼を保持することを目的とする。

（用語の定義）

第２条 この規程において使用する用語は、次の各号に掲げるもののほか、青森県情報セキュリティ基本方針（平成 15 年５月２日）及び個人情報の保護に関する法律についての事務対応ガイド（行政機関等向け。以下「事務対応ガイド」という。）において使用する用語の例による。

（１）「情報セキュリティ」とは、情報資産及び保有個人情報（以下「情報資産等」という。）の機密性、完全性及び可用性を維持することをいう。

（２）「機密性」とは、許可された者だけが情報資産等にアクセスできることを保証することをいう。

（３）「完全性」とは、情報資産等が正確及び完全であることを常に維持することをいう。

（４）「可用性」とは、許可された者が、確実に情報資産等を利用できることをいう。

（５）「情報」とは、職員等が職務上作成し、又は取得した全ての文書、図画若しくは電磁的記録（電磁的方式（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式をいう。）で作られる記録をいう。以下同じ。）に記載され、若しくは記録され、又は音声、動作その他の方法を用いて表された一切の事項をいう。

（６）「情報システム」とは、ハードウェア、ソフトウェア、ネットワーク、記録媒体等で構成されるものであって、これら全体で業務処理を行うもの。これらの仕組みを開発、運用及び保守するために作成された資料等を含むもの（紙等の電磁的記録されたもの以外を含む。）をいう。

（７）「情報資産」とは、情報及び情報システムの総称をいう。
（８）「個人情報」とは、法第２条第１項に定めるものをいう。
（９）「職員等」とは、法人の役員及び職員並びに研修、共同研究その他の法人に継続的に駐在する者をいう。
(10)「脅威」とは、情報の流失、漏洩、改ざん、破壊、障害等により情報資産が侵害される恐れのあることをいう。
(11)「情報サービス」とは、情報について検索、編集、電送等の処理を行うことをいう。
(12)「情報機器」とは、情報の保存、蓄積した情報の提供又は情報の作成、検索、編集、伝送等の処理を行うハードウェアをいう。
(13)「ネットワーク」とは、複数の情報機器を接続して情報を伝送し、協調動作させるための配線、ルータ、スイッチ等のハードウェア及びアドレス、プロトコル、プログラム等のソフトウェアをいう。
(14)「青森産技ネットワーク」とは、法人の管轄区域内に設置されたネットワーク及びそこから論理的に延長されたネットワークをいう。

第２章　組織体制

（情報セキュリティ委員会の設置）
第３条　法人に、情報セキュリティ委員会（以下「委員会」という。）を置く。
２　委員会は、必要に応じて最高責任者が招集し、事務は本部事務局企画経営室が行う。
３　委員会は、最高情報責任者、統括責任者、委員で構成する。
４　委員会は、情報セキュリティに関する必要な事項を審議し、この規程を見直す。
５　委員会は、情報セキュリティの脅威に対する必要な措置を講ずる。
（管理体制）
第４条　法人における情報セキュリティ対策は、次の各号に定める者が行う。
（１）最高情報セキュリティ責任者
ア　法人に、最高情報セキュリティ責任者（以下「最高責任者」という。）を置き、副理事長をもって充てる。
イ　最高責任者は、法人において情報管理及びその運用を担当し、情報セキュリティ対策を統括する。
ウ　最高責任者は、事務対応ガイドに定める総括保護管理者を兼ねる。
（２）統括情報セキュリティ責任者
ア　法人に、統括情報セキュリティ責任者（以下「統括責任者」という。）を置き、本部事務局企画経営室長をもって充てる。
イ　統括責任者は、最高責任者を補佐し、最高責任者に事故があるときは、その職務を代理する。

（３）情報セキュリティ委員

ア　法人に、情報セキュリティ委員（以下「委員」という。）を置き、理事及び総務室長をもって充てる。

イ　委員は情報セキュリティに関する総合的な調整を行い、情報セキュリティ上重要な事項と判断したものに関しては委員会に報告する。

（４）情報セキュリティ責任者

ア　法人に、情報セキュリティ責任者（以下「責任者」という。）を置き、地方独立行政法人青森県産業技術センター組織規程（平成 21 年規程第２号）第２条に定める組織（以下「所属」という。）ごとに一人置くこととし、当該所属の長をもって充てる。

イ　責任者は、委員会の下、本規程の遵守に関する権限と責任を有する。

ウ　責任者は、事務対応ガイドに定める保護管理者を兼ねる。

エ　責任者は、所属における情報の適切な管理の確保に当たるものとし、かつ、管理の状況についての点検を行うものとする。

（５）システム管理者

ア　責任者は、情報資産等に対する緊急時を含めた具体的なセキュリティ対策を実施する担当者として、システム管理者及び事務対応ガイドに定める保護担当者（以下「システム管理者等」という。）を一人以上指名する。

イ　システム管理者等は、責任者の指示等に従い、法人または所属が運用する情報システムの管理に関する具体的な作業を行うとともに、責任者の業務を補佐し、当該所属の情報セキュリティマネジメントを適切に実施しなければならない。

ウ　システム管理者は、事務対応ガイドに定める保護担当者を兼ねることができる。

（６）監査責任者

ア　監査責任者を置き、企画経営室長をもって充てる。

イ　監査責任者は、各所属における情報の管理の状況についての監査に当たるものとする。

２　前項第１号から第５号までに定める者は、法人が必要と認める運営上の組織に出席又は参加し、情報セキュリティ対策を実施又は指導若しくは助言することができる。

第３章　情報の分類と取扱い

（情報の分類）

第５条　委員会は、情報を、機密性、完全性及び可用性を考慮し適切に分類し、必要に応じ取扱制限をするものとする。

２　前項の分類は、青森県情報セキュリティ対策基準（平成 15 年５月２日制定）に準じて行う。

（システムへのアクセス権限）

第６条　責任者は、職員等が情報システムを使用するにあたり、業務上の特別な事由がある場合を除き、最低限のアクセス権限を付与しなければならない。

２　職員等は、アクセス権限を有する場合であっても、業務上の目的以外の目的をもってその情報にアクセスし、又は利用してはならない。ただし、責任者が許可した場合はこの限りではない。

（閲覧の制限）

第７条　責任者は、保有個人情報を閲覧する権限を有する職員等の範囲と権限の内容について、当該保有個人情報の秘匿性等その内容（特定の個人の識別の容易性の程度、要配慮個人情報の有無、漏えい等が発生した場合に生じ得る被害の性質・程度などを考慮するものとする。以下同じ。）に応じて、当該職員等が業務を行う上で必要最小限の範囲に限るものとする。

２　保有個人情報を閲覧する権限を有する職員等であっても、業務上の目的以外の目的で保有個人情報を閲覧してはならず、また、必要最小限の閲覧としなければならない。

３　保有個人情報を閲覧する権限を有しない職員等は、保有個人情報を閲覧してはならない。

（複製等の制限）

第８条　責任者は、職員等が業務上の目的で保有個人情報を取り扱う場合のうち、次に掲げる行為について、当該保有個人情報の秘匿性等その内容に応じて、当該行為を行うことができる場合を必要最小限に限るものとする。また、職員等は、責任者の指示に従い当該行為を行うものとする。

（１）保有個人情報の複製

（２）保有個人情報が記録されている文書（図画等を含む。以下同じ。）の外部への送付又は持ち出し

（３）その他保有個人情報の適切な管理に支障を及ぼすおそれのある行為

（誤りの訂正等）

第９条　職員等は、保有個人情報の内容に誤り等を発見したときは、責任者の指示に従い、訂正等を行うものとする。

（誤送付等の防止）

第 10 条　職員等は、保有個人情報を含む電磁的記録や媒体（文書の内容のほか、付加情報（PDF ファイルの「しおり機能表示」やプロパティ情報等）に個人情報が含まれている場合があることに注意するものとする。）の誤送信・誤送付、誤交付、ウェブサイト等への誤掲載等を防止するため、当該保有個人情報の秘匿性等その内容に応じて、複数の職員による確認、チェックリストの活用等の必要な措置を講ずるものとする。

（情報セキュリティの脅威又は侵害への対応）

第 11 条　職員等は、情報セキュリティの脅威又は侵害されたことを確認した場合は、直ちに責任者に報告しなければならない。

2　責任者は、情報セキュリティの侵害を確認した場合は、次に掲げる措置を行わなければならない。

（1）被害の拡大防止、復旧等のための必要な措置

（2）発生した事案の経緯、被害状況等の調査及び統括責任者への報告

（3）発生した事案の内容等に応じた原因の分析及び再発防止のための必要な措置

3　統括責任者は、情報セキュリティの脅威及びその侵害の状況等を責任者を通じて職員等に周知しなければならない。

第 4 章　人的セキュリティ

（職員等の責務）

第 12 条　職員等は、この規程の趣旨にのっとり、関連する法令及び規程等の定め並びに最高責任者、責任者及びシステム管理者等の指示に従い、情報資産等を取り扱わなければならないものとする。

2　職員等は、情報資産等の利用にあたり、パスワード又は暗号化による制限等の措置を講じて、情報セキュリティの脅威からの保護に努めなければならない。

3　職員等は、著作権、特許権等の知的財産権、個人情報その他の関係法令の保護対象となっている情報の権利を侵害してはならない。

4　職員等は、情報資産等の利用を通じて、法令及び公序良俗に反する行為を行ってはならない。

5　職員等は、情報資産等の利用を通じて、職務上知ることのできた秘密を漏らしてはならない。

6　職員等は、情報資産等の利用にあたって、これを破損又は亡失することのないように十分に注意しなければならない。

（アカウントとパスワードの管理）

第 13 条　職員等は、責任者から付与されたアカウントを用いなければならない。

2　職員等は、パスワードを他者に教えてはならない。

3　パスワードは他者が容易に想像できない固有のものを設定することとし、情報機器や情報サービス間で使い回してはならない。

（コンピュータウイルス等の対策）

第 14 条　職員等は、コンピュータウイルス等の情報セキュリティの脅威を防止するために、自己が管理する端末等へのセキュリティ対策ソフト導入等の対策を講じなければならない。

（外部からの接続）

第 15 条　職員等は、外部から青森産技ネットワークに接続する場合は、統括責任者の承認を得た上で、適切なアクセスに努めなければならない。

（部門等における独自ネットワークの構築）

第 16 条　責任者は、部門等の独自ネットワークを構築する場合は、委員会の承認を得た上で、構築しなければならない。

2　責任者は、部門等の独自ネットワークを運用する場合は、本規程に準拠し職員等の適切な利用に努めなければならない。

（無許可ソフトウェアの導入等の禁止）

第 17 条　職員等は、パソコン等の端末に、無断でソフトウェアを導入してはならない。

2　職員等は、業務上の必要がある場合は、責任者の許可を得て、ソフトウェアを導入することができる。なお、導入する際に責任者は、必要に応じてソフトウェアのライセンスを管理しなければならない。

3　職員等は、ソフトウェアを不正に使用してはならない。

（システム利用の制限等）

第 18 条　責任者は、情報システムの利用に関し、職員等を指導し、助言し、及び調整することができる。

2　責任者は、情報セキュリティの脅威の防止のため、職員等に対して報告を求めることができる。

3　責任者は、法令又はこの規程に反すると認める職員等に対して、警告をし、改善を求めることができる。

4　責任者は、前項の措置を講じてもなお当該職員等に改善が見られない場合は、情報及び情報システムの全部又は一部の利用を制限することができる。

（保有個人情報の取扱状況の記録）

第 19 条　責任者は、保有個人情報の秘匿性等その内容に応じて、台帳等を整備して、当該保有個人情報の利用、保管等の取扱いの状況について記録するものとする。

（外的環境の把握）

第 20 条　保有個人情報が外国において取り扱われる場合は、当該外国の個人情報の保護に関する制度等を把握した上で、保有個人情報の安全管理のために必要かつ適切な措置を講じなければならないものとする。

（入力情報の照合等）

第 21 条　職員等は、情報システムで取り扱う保有個人情報の重要度に応じて、入力原票と入力内容との照合、処理前後の当該保有個人情報の内容の確認、既存の保有個人情報との照合等を行うものとする。

第５章　物理的セキュリティ

（文書等の管理）

第 22 条　職員等は、保有個人情報が記録されている文書等について、責任者の指示に従い、定められた場所に保管するとともに、必要があると認めるときは、耐火金庫への保管、施錠等を行うものとする。

（端末の管理）

第 23 条　職員等は、自己が管理する情報機器を盗難、紛失、不正アクセス、災害等から適切に保護するため、必要な措置を講じなければならない。

（ネットワーク接続の制限）

第 24 条　職員等は、青森産技ネットワークに接続する情報機器をそれ以外のネットワークに接続してはならない。ただし、責任者の許可を得た場合はこの限りではない。

（情報機器の廃棄）

第 25 条　職員等は、情報システムの廃棄等処分を行う場合は、情報の漏洩等を防ぐための適切な措置を講じなければならない。

（文書等の廃棄）

第 26 条　職員等は、保有個人情報又は保有個人情報が記録されている文書等が不要となったときは、責任者の指示に従い、当該保有個人情報の復元又は判読が不可能な方法により当該情報の消去又は当該文書の廃棄を行うものとする。

２　保有個人情報の消去又は保有個人情報が記録されている文書等の廃棄を委託する場合（二以上の段階にわたる委託を含む。）は、必要に応じて、職員が消去及び廃棄に立ち会う、写真等を付した消去及び廃棄を証明する書類を受け取るなど、委託先において消去及び廃棄が確実に行われていることを確認するものとする。

（情報機器の持ち出し）

第 27 条　職員等は、情報機器を、法人以外に持ち出してはならない。ただし、責任者の許可を得た場合はこの限りではない。

（情報機器の持ち込み）

第 28 条　責任者は、許可した場合を除き、法人以外の者が管理する情報機器を法人内に持ち込ませてはならない。ただし、一時的に持ち込む場合であって、青森産技ネットワークに接続しないときはこの限りではない。

（無線ＬＡＮの接続）

第 29 条　職員等は、青森産技ネットワークに無線ＬＡＮを用いて接続する場合は、責任者の許可を受けた上で、盗聴、不正利用等を防止するために必要な措置を行わなければならない。

（コンピュータウイルス等の対策）

第 30 条　責任者は、コンピュータウイルス等の情報セキュリティの脅威を防止するために、青森産技ネットワークに対して必要な措置を講じなければならない。

２　職員等は、自己の端末がコンピュータウイルス等に侵害された場合は、直ちにネットワークへの接続を停止しなければならない。

（ネットワークの区分）
第 31 条　責任者は、青森産技ネットワークについて、その利用目的により適切に区分して管理しなければならない。
（情報システムの監視）
第 32 条　責任者は、必要に応じて、情報システムの利用状況等の監視を行うことができる。

第 6 章　技術的セキュリティ

（相互接続の承認等）
第 33 条　責任者は、法人以外の者が保有又は管理する情報システムに影響を与えるおそれのある行為を行う場合は、あらかじめ委員会の承認を得なければならない。
2　責任者は、安全性が確保されていないネットワークを経由して行う情報システムの保守作業等を許可してはならない。
（情報の暗号化）
第 34 条　責任者は、情報セキュリティを確保するため、必要に応じて、職員等に情報を暗号化するための措置を講じさせなければならない。

第 7 章　情報セキュリティの運用

（規程遵守の徹底）
第 35 条　責任者は、この規程を職員等に周知徹底しなければならない。
（情報システムに関する資料等の保管）
第 36 条　責任者は、自らが管理する情報システムの設計書、構成図等の文書について、これを業務上利用する者以外の者が利用できないようにその保管、複製、廃棄等について必要な措置を講じなければならない。
（情報セキュリティに関する情報の収集）
第 37 条　責任者は、最新の情報セキュリティ情勢に関する情報収集に努めるとともに、これをシステム管理者を通じて職員等に周知しなければならない。
2　責任者は、職員等の端末情報を把握しなければならない。
3　責任者は、前二項に規定する情報で緊急の措置を講ずる必要があると認める場合は、直ちに統括責任者に報告しなければならない。
4　統括責任者は、緊急の措置を講ずる必要があると判断した場合、これを責任者を通じて職員等に周知しなければならない。
（守秘義務等）
第 38 条　情報システムの運用又は保守管理の業務（外注する場合を含む。）に従事する者は、当該業務に関して知ることのできた秘密を関係者以外の者に漏らしてはならない。

また、業務上付与された権限を逸脱して当該業務を行ってはならない。

（職員等の教育研修）

第 39 条　統括責任者は、職員等の情報セキュリティに関する意識の高揚を図るための啓発、適切な安全管理に関する研修その他必要な教育研修を行うことができる。

2　責任者は、統括責任者の実施する教育研修への参加の機会を付与する等の必要な措置を講ずるものとする。

（保有個人情報の提供を受ける者に対する措置）

第 40 条　責任者は、法第 69 条第２項第３号及び第４号の規定に基づき行政機関等以外の者に保有個人情報を提供するときは、法第 70 条の規定に基づき、措置を講ずるものとする。

2　原則として、提供先における利用目的、利用する業務の根拠法令、利用する記録範囲及び記録項目、利用形態等について、提供先との間で書面（電磁的記録を含む。）を取り交わすものとする。

3　漏えいの防止その他の提供に係る個人情報の適切な管理のために必要な措置を求めるとともに、必要があると認めるときは、当該措置の状況を確認するために提供前又は随時に実地の調査等を行い、その結果を記録するとともに、改善要求等の措置を講ずるものとする。

（行政機関等に保有個人情報を提供する場合の措置）

第 41 条　責任者は、法第 69 条第２項第３号の規定に基づき他の行政機関等に保有個人情報を提供する場合において、必要があると認めるときは、法第 70 条の規定に基づき、前条に掲げる措置を講ずるものとする。

（個人情報の取扱いの委託等における対応）

第 42 条　個人情報の取扱いを外部に委託する場合における個人情報の安全管理のために講ずべき措置については、令和５年３月 20 日付け青総第 1600 号総務部長通知「個人情報の取扱いを委託する場合における個人情報の安全管理の措置について」に基づき対応するものとする。

（安全管理上の問題への対応）

第 43 条　保有個人情報の漏えい等安全管理上問題となる事案の発生（そのおそれがある場合を含む。）を認識したときは、令和５年５月１日付け青総第 183 号総務学事課長通知「保有個人情報の漏えい等事案が発生した場合の報告体制について」に基づくほか、次に掲げるところにより対応するものとする。

（１）責任者は、被害の拡大防止、復旧等のために必要な措置を速やかに（直ちに行い得る措置については直ちに）講ずるものとする。

（２）責任者は、事案の内容等に応じて必要があると認めるときは、その内容を速やかに最高責任者に報告するものとする。

（３）最高責任者は、国の個人情報保護委員会による法第 156 条の規定に基づく資料の提

出の要求又は実地調査その他事案の把握等についての協力要請があった場合は、適切に対応するものとする。

（定期の点検）

第 44 条　統括責任者は、情報システムについて、アクセスログ等により定期的に運用及び保守管理の状況を点検し、必要があると認めるときは、その結果を最高責任者に報告するものとする。

（自己点検及び監査）

第 45 条　最高責任者は、各所属における情報資産等の安全措置等の実施状況について、必要があると認めるときは、責任者に点検を行わせ、その結果を報告させるものとする。

2　最高責任者は、前項の点検結果により、必要があると認めるときは、監査責任者に監査を行なわせ、その結果を報告させるものとする。

（評価及び見直し）

第 46 条　責任者及び最高責任者は、点検又は監査の結果等を踏まえ、実効性等の観点から情報資産等の適切な管理のための措置について評価し、必要があると認めるときは、その見直し等の措置を講ずるものとする。

附　則

この規程は、平成 21 年 10 月 16 日から施行する。

附　則（平成 27 年規程第 29 号）

この規程は、平成 27 年４月１日から施行する。

附　則（平成 30 年規程第 22 号）

この規程は、平成 30 年４月１日から施行する。

附　則（令和６年規程第 21 号）

この規程は、令和６年９月３日から施行する。