奈良工業高等専門学校情報セキュリティ管理規程

平成２３年１月１７日制定
令和　３　年１月１４日改正

目次

第１章　総則

（目的）

第１条　この規程は，独立行政法人国立高等専門学校機構奈良工業高等専門学校（以下「本校」という。）における情報セキュリティ対策に関する全般的事項および管理的事項を定めることにより，情報セキュリティの維持向上に資することを目的とする。

２　情報セキュリティ対策に関する専門的及び技術的な事項については，別に定める情報セキュリティ推進規程による。

（定義）

第２条　この規程における用語の定義は，この規程で定めるものを除き，独立行政法人国立高等専門学校機構情報セキュリティポリシー対策規則（機構規則第９８号。以下「対策規則」という。）及び独立行政法人国立高等専門学校機構情報セキュリティポリシーに係る情報格付規則（機構規則第９９号）の定めるところによる。

（適用範囲）

第３条　この規程を適用する情報資産の範囲は，機構が扱う情報及び本校の情報システムとする。

２　本校の情報システムの範囲は，次のとおりとする。

　コンピュータシステム，情報ネットワーク，情報ネットワーク機器及びソフトウェア

第４条　本校の教職員の範囲は，次のとおりとする。

常勤又は非常勤の教職員，研究員その他情報セキュリティ管理責任者が認めた者をいう。

２　本校の学生の範囲は，次のとおりとする。

本科生，専攻科生，研究生，聴講生及び科目等履修生

３　本校の教職員，学生，及び第９条第１項に基づき情報資産を本校の業務遂行を目的として一定期間にわたり継続的に利用する許可を得て利用する者を「経常的利用者」と称する。

４　第９条第２項に基づき情報資産を臨時に利用する許可を得て利用する者を「臨時利用者」と称する。

５　本校の教職員，及び第９条第１項に基づき情報資産を本校の業務遂行を目的として一定期間にわたり継続的に利用する許可を得て利用する者を「業務従事者」という。

第５条　この規程の適用区域は，本校の管理区域とする。

２　本校の管理区域の範囲は，別図１及び別表２のとおりとする。

（組織体制）

第６条　本校の情報セキュリティ対策における管理的業務は，情報セキュリティ管理委員会及び情報セキュリティ推進委員会が責任を持ち,情報セキュリティ責任者,情報セキュリティ副責任者及び情報セキュリティ推進責任者が主として執り行うものとする。

２　前項に係る各委員会及び役職の役割分担は，次の各号に掲げるとおりとする。

一　情報セキュリティ管理委員会　一般的管理業務について責任を持つ。

二　情報セキュリティ推進委員会　専門的及び技術的管理業務について責任を持つ。

三　情報セキュリティ責任者　情報セキュリティ対策業務の統括，実施規程及び実施手順の制定並びに改廃を主として執り行う。

四　情報セキュリティ副責任者　一般的管理業務を主として執り行う。

五　情報セキュリティ推進責任者　専門的及び技術的管理業務を主として執り行う。

３　情報セキュリティ責任者が不在の場合の代理の者については，別に定めるものとし，前項第三号から第五号の規定にかかわらず，代理の者は，その責任において前項各号に掲げる業務を直接執り行うことができるものとする。

４　情報セキュリティ責任者又は前項に定める代理の者は，専門的・技術的課題への緊急時の対応のために，前項各号に掲げる業務に係る権限を，指名する者に対し委任することができる。指名された者は，善良な管理者の注意をもって業務を行うものとする。

５　情報セキュリティ管理者は第２項第四号に規定する情報セキュリティ副責任者の，情報セキュリティ推進員は第２項第五号に規定する情報セキュリティ推進責任者の役割をそれぞれ割り当てられた範囲で補佐し又は代行するものとする。

６　本校の情報セキュリティ全般に関する事務は，総務課が執り行うものとする。

（管理的業務遂行における禁止事項）

第７条　情報セキュリティ責任者,情報セキュリティ副責任者,情報セキュリティ管理者,

情報セキュリティ推進責任者，情報セキュリティ推進員，第６条第３項及び第４項に規定する者は，管理者権限を濫用してはならない。

第２章　情報システムの利用

（規程・手順等の整備）

第８条　情報セキュリティ責任者は，情報セキュリティ推進責任者の協力の下で，本校の情報システムの利用について次の各号に掲げる場合に対応する規程又は手順等を整備するものとする。

一　本校の教職員又は学生に対して本校の情報システムについてのアカウントを発行又は廃止する場合

二　本校の教職員又は学生のいずれでもない者に対して，本校の情報システムを利用させる場合

三　経常的利用者が，コンピュータシステムを利用する場合及び特にモバイル PC を利用する場合

四　経常的利用者が，電子メール又はウェブページを利用する場合

五　経常的利用者が，本校支給以外の情報システムから本校の情報システムへアクセスする場合

六　業務従事者が，新たにソフトウェアを購入又は借用しインストールして利用する場合並びにインストールを解除する場合

七　業務従事者が，新たにコンピュータシステムを購入又は借用し業務に利用する場合及び当該コンピュータシステムを本校情報システムに接続する場合，並びにその利用を終了する場合

八　業務従事者が，本校の情報システムを利用して新たに情報公開等を行う場合

九　業務従事者がサーバー装置を設置して運用する場合

（学外者に対する利用許可）

第９条　情報セキュリティ副責任者は,次の各号に掲げる条件がすべて満たされる場合は,本校の教職員又は学生のいずれでもない者にアカウントを発行して本校の情報システムを利用させることができる。

一　利用目的が共同研究・地域協働教育・産学官連携活動など本校の業務の遂行であって，一定期間にわたって継続的に情報システムを利用する必要が認められること。

二　利用に責任を持つ教職員が定められており，当該利用者が情報セキュリティ関連法令，機構の情報セキュリティポリシー及び実施規則，並びに本校の実施規程及び実施手順を遵守し，適正に情報システムを利用するよう監督できること。

三　前号に定める教職員から所定の手続きがなされていること。

四　当該利用者から，第二号を遵守する旨を含む所定の誓約書が提出されていること。

２　情報セキュリティ副責任者は，次の各号に掲げる条件がすべて満たされる場合，経常的利用者以外の者に本校の情報システムを臨時に利用させることができる。

一　利用目的が，情報システムの設置又はメンテナンス，本校主催又は共催の講習会の受講など本校の業務達成に資するものであり，利用期間が短期であること。
二　利用できる情報資産が明確にされており，その範囲以外の情報資産を利用しないこと。
三　利用を管理する教職員が定められており，前号の規定が遵守されるよう管理できること。
四　前号に定める教職員から所定の手続きがなされていること。

３　前２項の実施は，第８条第二号に基づいて定められる「学外者による情報システム利用手順」によるものとする。

（ウェブ公開の取消）

第１０条　情報セキュリティ副責任者は，本校内で運用され公開されているウェブサーバ及びウェブコンテンツについて，情報セキュリティ関連法令，機構の情報セキュリティポリシー及び実施規則又は本校の実施規程及び実施手順に違反する行為が認められた場合には，必要に応じてウェブコンテンツの削除，ウェブサーバのネットワークからの切り離し等の措置をとらせるものとする。

（本校外の情報セキュリティ水準の低下を招く行為の防止）

第１１条　情報セキュリティ責任者は，本校外の情報セキュリティ水準の低下を招く行為の防止に関する措置についての手順等を整備するものとする。

（利用記録の採取の許可）

第１２条　情報セキュリティ副責任者は，複数の者が利用する情報システムを管理する教職員に，当該情報システムに係る利用記録（以下「利用記録」という。）の採取を許可することができる。

２　前項の許可に当たっては，利用記録の使用目的，採取しようとする利用記録の範囲及び利用記録を伝達する対象者を申請させ，不適切と認められる場合には採取を却下するものとする。

３　第１項の許可を与える場合においては，本校の情報セキュリティ教職員規程第４５条の遵守を誓約させるものとする。

第３章　情報の取扱い

（情報の運搬・送信）

第１３条　要機密情報（個人情報及び同等の取り扱いが必要な情報）の管理区域外への持ち出しは原則禁止とするが，持ち出しがやむを得ない場合，情報セキュリティ責任者は，教職員等が情報を運搬・送信する場合の安全管理措置について別に定める。

２　前項に定める場合において，機密性３情報については情報セキュリティ責任者による

許可制とし，機密性２情報については情報セキュリティ責任者への届出制とするものとする。

（情報の提供）

第１４条　情報セキュリティ責任者は，教職員等が情報を提供する場合の安全管理措置についての規程及び手順等を整備するものとする。

２　前項に定める場合において，機密性３情報を教職員以外の者に提供する場合は情報セキュリティ副責任者による許可制とし，機密性２情報を教職員以外の者に提供する場合は情報セキュリティ副責任者への届出制とするものとする。

（要機密情報等の取扱）

第１５条　情報セキュリティ責任者は，要機密情報等の取扱いについて，次の各号に掲げる場合に講ずるべき安全管理措置についての規程及び手順等を整備するものとする。

一　モバイルＰＣにより処理を行う場合

二　本校支給以外の情報システムにより処理を行う場合

三　管理区域外で処理を行う場合

四　要機密情報を取り扱う情報システム並びに要機密情報を含む記憶媒体を管理区域外に持ち出す場合

２　前項に定める場合において，機密性３情報に関する場合は情報セキュリティ責任者による許可制とし，セキュリティ対策について情報セキュリティ推進責任者の確認を受けるものとする。

３　第１項に定める場合において，機密性２情報に関する場合は情報セキュリティ責任者への届出制とするものとする。

第１６条　情報セキュリティ責任者は，情報セキュリティ推進責任者の協力の下で，次の各号に掲げる措置を講ずるものとする。

一　前条に係る情報処理及び持ち出しについての記録を取得すること。

二　要保護情報については，前条に係る情報処理又は持ち出しを許可した期間が終了した時に，報告を受けること。

三　前号に定める場合において，許可を受けた者から終了した旨の報告がない場合には，その状況を確認し対処すること。

四　機密性２情報については，情報処理又は持ち出しを届け出た期間が終了した時に，必要に応じてその状況を確認し対処すること。

第４章　物理的及び環境的セキュリティ対策

（管理区域への入退場管理）

第１７条　情報セキュリティ副責任者は，管理区域への入退場について次の各号に掲げる措置を講ずるものとする。

一　経常的利用者には，職員証，学生証又は身分証明書を携行させること。

二　管理区域へ立入る委託業者，受渡業者又は臨時利用者がある場合には，訪問先で受付けをする。

三　前号による訪問があった後，管理区域内で委託業者，受渡業者又は臨時利用者による作業等の行為が引き続き行われる場合には，作業場所まで経常的利用者を同伴させること。

四　委託業者，受渡業者及び臨時利用者には，第１９条に定める安全区域へ立入らせないこと。ただし，情報システム又はその他の設備・機器等の設置又はメンテナンス，建物の補修等の作業の必要がある場合については第２０条第三号及び第四号の規定に従って立入らせることができる。

２　第１項の規定にかかわらず，本校の学生の保護者が教職員との面談，授業の参観，入退寮の補助等，学生の教育に関連する目的で来校する場合には，入退場させることができるものとする。

３　第１項の規定にかかわらず，体育祭，高専祭，学校開放事業等，一般の来校者を受け入れる行事を開催する場合には，次の各号に掲げる措置を講じた上で，時間を限って一般来校者を入退場させることができるものとする。

一　事務室，研究室，その他本校の情報資産を有する部屋（安全区域を含む。）について，施錠するか入退室を管理する教職員を常駐させること。

二　本校内の通信回線（無線等を含む）及び掲示等を目的とした情報システムについて，盗聴・侵入・破壊等を防止する対策をとること。

三　行事に使用する情報システムについて，十分な情報セキュリティ対策を講じること。

（物理的セキュリティ境界の管理）

第１８条　情報セキュリティ副責任者は事務室，研究室，その他本校の情報資産を有する部屋について，扉等に施錠等の物理的な入退場管理の措置を施し，必要に応じて受付け担当又はセキュリティカード，暗証番号，生体認証等を使った入退場管理システムによる入退場管理を行うものとする。

（安全区域の設置）

第１９条　情報セキュリティ副責任者は，本校の管理区域内に安全区域を設け，要保護情報及びそれを取り扱う情報システムを安全区域に設置するものとする。この場合において，要保護情報又はそれを取り扱う情報システムを安全区域に設置することが困難な場合は，要保護情報又はそれを取り扱う情報システムを設置した場所に対して必要なアクセス制限を設定するものとする。

２　本校の安全区域の範囲は，別表３のとおりとする。

３　情報セキュリティ副責任者は，安全区域について次の各号に掲げる措置の必要性を検討し，必要である場合にはその措置を講ずるものとする。

一　水や火を扱う場所から隔離し，外壁から離れた窓の無い内壁に囲まれた場所へ設置

すること。
二　開けたら直ちに自動的に閉じる扉を使用するとともに，一定時間開いた状態の時に作動するアラームを設置し，それが確実に動作するか定期的に検査すること。
三　出入口に主体認証を行うための措置を講ずること。
四　可能な限り不燃性又は難燃性の防火壁を用い，室内には当該環境に適した消火設備及び消火器を設置すること。

（安全区域の管理）
第２０条　情報セキュリティ副責任者は，安全区域及び要保護情報又はそれを取り扱う情報システムを管理する区域について次の各号に掲げる措置を講ずるものとする。
一　安全区域である掲示をしないこと。
二　機密性３情報を保管する安全区域にはコピー機，ＦＡＸ装置等を設置しないこと。
三　入退場を管理する教職員を常任させ，当該者が不在になる場合は施錠させること。ただし，教職員を常任させることが困難な場合においては，セキュリティカード，暗証番号，生体認証等を使った入退場管理で代えることができる。
四　委託業者に情報システム又はその他の設備・機器等の設置又はメンテナンス，建物の補修等の作業をさせる場合には，制限時間を設けた上で教職員に監視させること。
五　前号の場合においては，作業者の氏名，所属，作業目的，作業日時並びに立入り及び退出の時刻を記録させること。
２　情報セキュリティ副責任者は，特に重要な情報資産を設置した安全区域について，次の各号に掲げる措置の必要性を検討し，必要である場合にはその措置を講ずるものとする。
一　すべての者の入退場を記録し監視すること。
二　不正な盗聴装置や録音装置等の有無を，定期的に捜索をすること。

（アクセス記録の保持）
第２１条　情報セキュリティ管理部署は，第２０条に係るアクセス記録を，最低三ヶ月間，保持するものとする。

（環境の脅威からの保護）
第２２条　情報セキュリティ副責任者は，必要に応じて特に重要な情報についてはバックアップを取り，当該バックアップを別の建物に保管する等，同時被災等しない適切な環境に保管するものとする。

（廃棄情報資産の管理）
第２３条　情報セキュリティ副責任者は，廃棄処分となった情報資産の格納場所を施錠するものとする。

第５章　教育

（情報セキュリティ教育の実施体制）
第２４条　情報セキュリティ副責任者は，情報セキュリティ推進責任者の協力のもとに，次の各号に掲げる措置を講ずるものとする。
一　経常的利用者に対し，情報セキュリティに関する啓発を行うこと。
二　情報セキュリティ関連法令，機構の情報セキュリティポリシー及び実施規則，並びに本校の実施規程及び実施手順について，経常的利用者それぞれに教育すべき内容を検討し，教育のための資料を整備すること。
三　別に定める「情報セキュリティ教育実施手順」に従って情報セキュリティ教育を実施する体制を整備すること。
四　経常的利用者の情報セキュリティ教育受講状況を管理できる仕組みを整備すること。
２　情報セキュリティ副責任者は，経常的利用者の情報セキュリティ教育受講状況について，次の各号に掲げる措置を講ずるものとする。
一　当該経常的利用者が所属する部署の情報セキュリティ管理者に通知すること。
二　毎年度一回，情報セキュリティ責任者及び情報セキュリティ管理委員会に対して，経常的利用者の情報セキュリティ教育受講状況について報告すること。
３　情報セキュリティ管理者は，経常的利用者が情報セキュリティ教育を受講しない場合には，受講を勧告するものとする。経常的利用者が当該勧告に従わない場合には，情報セキュリティ副責任者にその旨を報告するものとする。
４　情報セキュリティ推進委員会は，利用者からの情報セキュリティ対策に関する相談に対処するものとする。

（教育の主体と客体）
第２５条　経常的利用者に対する教育は，別に定める「情報セキュリティ教育実施手順」に従って実施するものとする。
２　前項の規定にかかわらず，情報セキュリティ副責任者，情報セキュリティ推進責任者及び情報セキュリティ推進員に対する教育には，機構又はセキュリティ専門機関等が開催する専門的情報セキュリティ対策教育を利用することができる。
３　情報セキュリティ責任者及び情報セキュリティ管理者は，自身の知識・能力に応じ，前２項のいずれかの教育を選択して受講するものとする。

第６章　情報セキュリティインシデント対応

（情報セキュリティインシデント対応）
第２６条　情報セキュリティインシデント対応は，奈良工業高等専門学校危機管理規程によるものとする。

（業務継続計画と情報セキュリティ対策の整合性の確保）
第２７条　情報セキュリティ管理委員会は，機構において業務継続計画又はその整備計画

がある場合には，本校の情報セキュリティ対策と当該業務継続計画との整合性の検証を行うものとする。

第７章　調達，ソフトウェア開発及び外部委託

（情報システムの調達）

第２８条　情報システムの調達（購入に準ずるリース等を含む。以下同じ。）における情報セキュリティ対策は，情報セキュリティ副責任者の要請に基づき情報セキュリティ推進責任者が実施するものとする。ただし，必要な場合には情報セキュリティ管理者に実施させることができる。

２　情報システムの調達における情報セキュリティ対策は，別に定める「情報システムの購入における情報セキュリティ対策実施手順」によるものとする。

（ソフトウェア開発）

第２９条　本校が使用するソフトウェアの開発（以下「ソフトウェア開発」という。）における情報セキュリティ対策は，情報セキュリティ副責任者の要請に基づき情報セキュリティ推進責任者が実施するものとする。ただし，必要な場合には情報セキュリティ管理者に実施させることができる。

２　ソフトウェア開発における情報セキュリティ対策は，別に定める「ソフトウェア開発における情報セキュリティ対策実施手順」によるものとする。

（外部委託）

第３０条　本校の情報資産に関する業務のすべて又はその一部を第三者に委託（以下「外部委託」という。）する場合の情報セキュリティ対策については，情報セキュリティ副責任者の要請に基づき情報セキュリティ推進責任者が実施するものとする。ただし，必要な場合には情報セキュリティ管理者に実施させることができる。

２　外部委託における情報セキュリティ対策は，別に定める「外部委託における情報セキュリティ対策実施手順」及び「外部委託における情報セキュリティ対策実施に関する評価手順」によるものとする。

３　外部委託において委託先がその請負内容の全部又は一部を第三者に再請負させることを禁止するものとする。ただし，委託先からの申請を受け，再請負させることにより生ずる脅威に対して情報セキュリティが十分に確保される措置が担保されると情報セキュリティ副責任者が判断する場合は，その限りではない。また，委託先によるアクセスを認める情報及び情報システムの範囲を判断する基準及び委託先の選定基準に従って再委託の承認の可否を判断するものとする。

第８章　違反と例外措置

（違反への対処）

第３１条　情報セキュリティ副責任者は，情報セキュリティ関連法令，機構の情報セキュリティポリシー若しくは実施規則，又は本校の実施規程若しくは実施手順に関する重大な違反（以下「重大な違反」という。）の報告を受けた場合及び自らが重大な違反を知った場合には，速やかに調査を行い，事実を確認するとともに，情報セキュリティ責任者に報告するものとする。この場合において，事実の確認にあたっては，可能な限り当該行為を行った者の意見を聴取するものとする。また，違反者が情報セキュリティ責任者である場合においては，報告を最高情報セキュリティ責任者に行うものとする。

２　前項の規定にかかわらず，情報セキュリティ責任者は，情報セキュリティ副責任者による重大な違反の報告を受けた場合及び自らが重大な違反を知った場合には，速やかに調査を行い，事実を確認しなければならない。この場合において，事実の確認にあたっては，可能な限り情報セキュリティ副責任者の意見を聴取するものとする。

３　情報セキュリティ責任者又は情報セキュリティ副責任者は，調査によって違反行為が判明した場合には，次の各号に掲げる措置を講ずることができる。

一　当該違反者に対する当該行為の中止命令

二　情報セキュリティ推進責任者に対する当該行為に係る情報発信の遮断命令

三　情報セキュリティ推進責任者に対する当該行為者のアカウント停止命令又は削除命令

四　本校で懲罰等を管轄する各種委員会への報告

五　独立行政法人国立高等専門学校機構法（平成１５年法律第１１３号）及び独立行政法人国立高等専門学校機構教職員就業規則（機構規則第６号。以下「就業規則」という。）に定める処罰の依頼

六　その他法令に基づく措置

４　情報セキュリティ責任者又は情報セキュリティ副責任者は，機構本部の情報セキュリティ副責任者を通じて前項第二号及び第三号と同等の措置を依頼することができる。

５　情報セキュリティ責任者は第１項の報告を受けた場合又は情報セキュリティ副責任者による重大な違反を知った場合は，速やかにその旨を最高情報セキュリティ責任者に報告するものとする。

（例外措置）

第３２条　情報セキュリティ責任者は，情報セキュリティ管理委員会の審議に基づき例外措置の適用の申請を審査する者（以下「許可権限者」という。）を定め，審査手続を整備するものとする。

２　許可権限者は，利用者による例外措置の適用の申請を，定められた審査手続に従って審査し，許可の可否を決定するものとする。この場合において，決定の際には，次の各号に掲げる項目を含む例外措置の適用審査記録を整備し，情報セキュリティ責任者に報告するものとする。

一　決定を審査した者の情報（氏名，役割名，所属及び連絡先）

二　申請内容

ア　申請者の情報（氏名，所属及び連絡先）
イ　例外措置の適用を申請する情報セキュリティ関係規程の該当箇所（規程名及び条項等）
ウ　例外措置の適用を申請する期間
エ　例外措置の適用を申請する措置内容（講ずる代替手段等）
オ　例外措置の適用を終了した旨の報告方法
カ　例外措置の適用を申請する理由
三　審査結果の内容
ア　許可又は不許可の別
イ　許可又は不許可の理由
ウ　例外措置の適用を許可した情報セキュリティ関係規程の適用箇所（規程名及び条項等）
エ　例外措置の適用を許可した期間
オ　許可した措置内容（講ずるべき代替手段等）
カ　例外措置を終了した旨の報告方法

３　許可権限者は，例外措置の適用を許可した期間の終了期日に，許可を受けた者からの報告の有無を確認するとともに，報告がない場合には，その状況を確認し，必要な措置を講ずるものとする。ただし，許可権限者が報告を要しないとした場合は，この限りでない。

４　情報セキュリティ責任者は，例外措置の適用審査記録の台帳を整備し，例外措置の適用審査記録の参照について，情報セキュリティ監査を実施する者からの求めに応ずるものとする。

第９章　評価，見直し及び監査協力

（脅威と脆弱性の評価・見直し）

第３３条　情報セキュリティ責任者は，情報資産の価値と脅威並びに脆弱性を評価するために「情報システム運用リスク評価手順」を定めるものとする。

２　情報セキュリティ責任者は，情報セキュリティ副責任者，情報セキュリティ管理者，情報セキュリティ推進責任者及び情報セキュリティ推進員を含む各情報資産の管理者に対して，少なくとも年に一回，リスク管理を次の各号に掲げる事項に従って実施し，その結果を情報セキュリティ管理委員会に報告するよう指示するものとする。

一　当該管理者が扱う情報資産について，情報システム運用リスク評価手順に基づきリスク評価を行うこと。

二　評価結果に従い，リスクに対する事前の対策を必要とするものについてはその具体策を定め，必要に応じ，情報セキュリティインシデント対応手順に反映させるべき要件を明確にすること。この場合において，対策を施さないと判断したものについても報告するものとする。

３　情報セキュリティ管理委員会は，前項の報告結果に基づき実施規程及び実施手順の見

直しを行う必要性の有無を検討し，必要があると認めた場合にはその見直しを行うものとする。
４　前項において，実施規則に影響すると判断する事案があった場合には，情報セキュリティ責任者が最高情報セキュリティ責任者に報告するものとする。

（自己点検）
第３４条　情報セキュリティ責任者は，業務従事者ごとの情報セキュリティ対策実施状況を把握し，必要に応じてその改善を図るために，情報セキュリティ自己点検実施手順を整備するものとする。
２　情報セキュリティ自己点検実施手順には「年度自己点検計画」及び「自己点検票」を含めるものとする。

第３５条　情報セキュリティ副責任者は，情報セキュリティ責任者が定める情報セキュリティ自己点検実施手順に基づき，業務従事者に対して，自己点検の実施を指示するものとする。

第３６条　情報セキュリティ副責任者は，業務従事者による自己点検が行われていることを確認し，その報告を求めて結果を評価するものとする。
２　情報セキュリティ責任者は，情報セキュリティ副責任者による自己点検が行われていることを確認し，その報告を求めて結果を評価するものとする。

第３７条　情報セキュリティ責任者は，自己点検の結果を全体として評価するとともに，必要に応じて情報セキュリティ副責任者に改善を指示するものとする。

（監査協力）
第３８条　情報セキュリティ責任者，情報セキュリティ副責任者，情報セキュリティ推進責任者及びその他の関係者は，機構の情報セキュリティ監査者が行う監査の適正かつ円滑な実施に協力するものとする。

第１０章　その他

第３９条　情報セキュリティ副責任者は，この規程又は情報セキュリティ推進規程で定められた業務の一部を，範囲を明確にして情報セキュリティ管理者に代行させることができる。

第４０条　情報セキュリティ推進責任者は，この規程又は情報セキュリティ推進規程で定められた業務の一部を，範囲を明確にして情報セキュリティ推進員に代行させることができる。

第４１条　この規程に定めるもののほか，情報資産の適正な管理及び運用並びに情報セキュリティの維持向上に関し必要な事項は，別に定める。

附　則

この規程は，平成２３年１月２３日から施行する。

附　則

この規程は，平成２８年１２月６日から施行する。

附　則

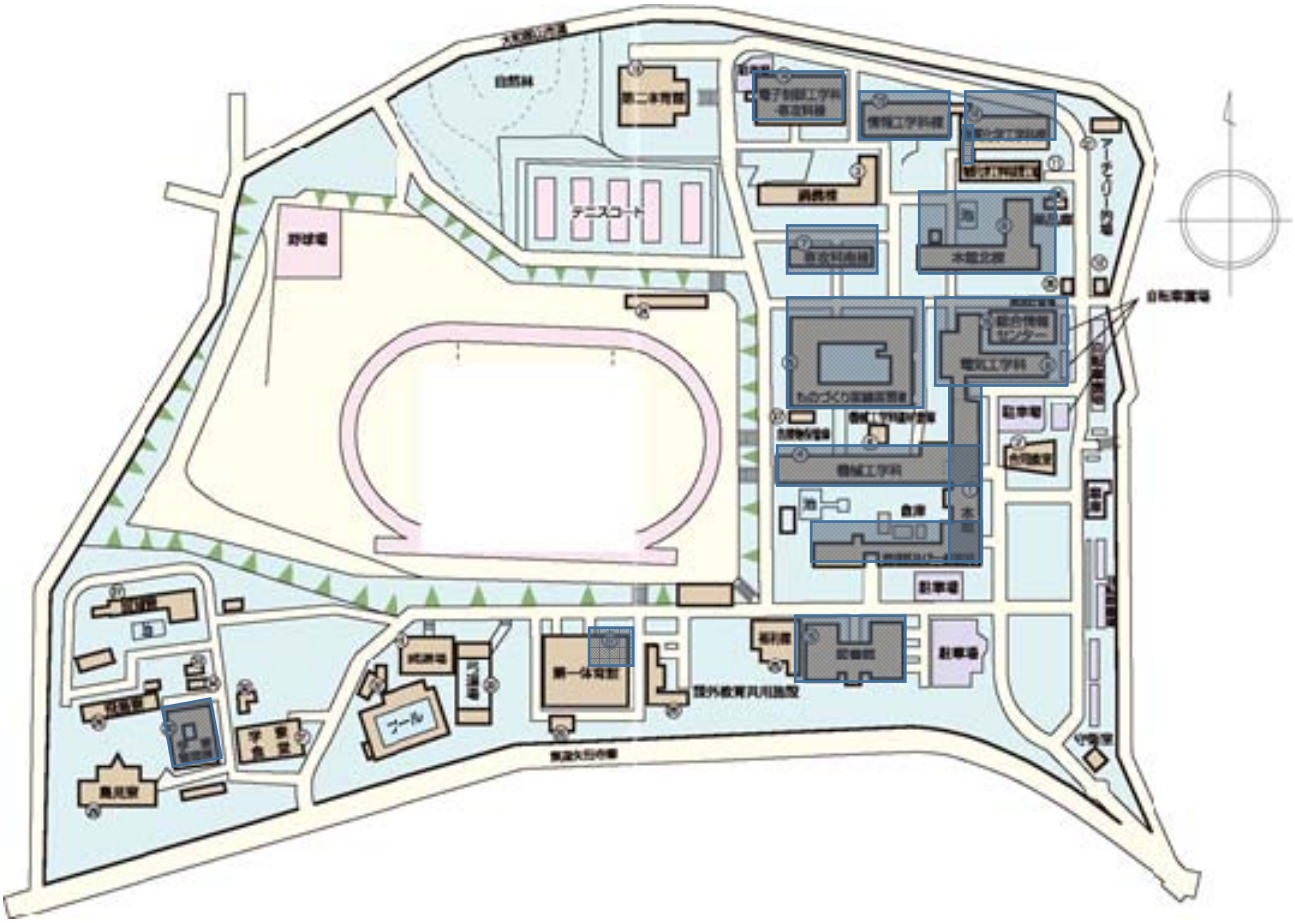
この規程は，令和２年５月１４日から施行し，令和２年４月１日から適用する。

附　則

この規程は，令和３年１月１４日から施行する。

管理区域

別図１（本校の管理区域の範囲）　第５条関係



別表２(本校の管理区域の範囲)　第５条関係

施設等名称		
独立行政法人国立高等専門学校機構が契約するMicrosoft365のテナント(クラウド)		
独立行政法人国立高等専門学校機構が契約するZygnath，人事給与システム，マイナンバーシステム		
本館	事務室	総務課(総務)
		事務電算室
		総務課(会計)
		学生課
		校長室
		事務部長室
	各教員研究室	
	印刷室	
	非常勤講師控室	
機械工学科棟	各教員研究室	
	デザインシステム実験室	
電気工学科棟	各教員研究室	
	ネットワーク管理室	
電子制御工学科・専攻科棟	各教員研究室	
	共同研究室	
情報工学科棟	各教員研究室	
	電算機室	
	進路指導室	
物質化学工学科棟	各教員研究室	
	ネットワーク機器室	
	進路指導室	
本館北棟	各教員研究室	
	マルチメディア準備室	
	教育研究支援室事務室	
専攻科南棟	各教員研究室	
図書館棟	図書館事務室	
	グローバル交流サロン	
総合情報棟	サーバー室	
	管理室	
第一体育館	教員控室	
ものづくり実験実習棟	教育研究支援室(ものづくり棟)	
学寮	学寮事務室	

別表３(本校の安全区域の範囲)　第１９条第２項関係

施設等名称		備考
本館	事務電算室	要保護情報またはそれを処理する情報システムを設置する区域
電気工学科棟	ネットワーク管理室	
電子制御工学科・専攻科棟	共同研究室	
情報工学科棟	電算機室	
物質化学工学科棟	ネットワーク機器室	
図書館棟	図書館事務室	
総合情報棟	サーバー室	