鹿児島工業高等専門学校サイバーセキュリティ教職員規程

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鹿児島工業高等専門学校（以下「本校」という。）における情報セキュリティの維持向上のために本校の教職員が遵守すべき事項を定めるものである。

（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サイバーセキュリティポリシー対策規則（機構規則第９８号），及び独立行政法人国立高等専門学校機構サイバー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。以下「格付規則」という。），並びに本校のサイバーセキュリティ管理規程（以下「管理規程」という。）別表１から別表５まで及び別図１の定めるところによる。

（適用範囲）

第３条　この規程は独立行政法人国立高等専門学校機構（以下「機構」という。）の扱う情報及び本校の情報システムを対象とする。

２　本校の情報システムの範囲は管理規程別表１のとおりとする。

第４条　本校の教職員の範囲は，管理規程別表２のとおりとする。

２　本校の学生の範囲は，管理規程別表３のとおりとする。

３　本校の教職員，学生及び管理規程第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　管理規程第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。

第５条　本校の管理区域の範囲は管理規程別図１及び別表４のとおりとする。

（一般的遵守事項）

第６条　本校の教職員は，情報セキュリティ関連法令，機構の基本方針及び実施規則，並びに本校の実施規程及び実施手順を遵守しなければならない。

（一般的禁止事項）

第７条　本校の教職員は，次の各号に掲げる行為を行ってはならない。

一　差別，名誉毀損，誹謗中傷，人権侵害，ハラスメントにあたる情報の発信

二　個人情報やプライバシーを侵害する情報の発信

三　守秘義務に違反する情報の発信

四　著作権等の知的財産権や肖像権を侵害する情報の発信

五　公序良俗に反する情報の発信

六　本校の社会的信用を失墜させるような情報の発信

七　ネットワークを通じて行う通信の傍受等，通信の秘密を侵害する行為

八　不正アクセス行為の禁止等に関する法律（平成１１年法律第１２８号）に定められたアクセス制御を免れる行為，又はこれに類する行為

九　過度な負荷等により円滑な情報システムの運用を妨げる行為

十　その他法令に基づく処罰の対象となり，又は損害賠償等の民事責任を発生させる情報の発信

十一　上記の行為を助長する行為

（機構が扱う情報及び本校の情報システムの利用に係わる禁止事項）

第８条　本校の教職員は，機構が扱う情報及び本校の情報システムについて，次の各号に掲げる行為を行ってはならない。

一　本校の業務遂行以外の目的で利用すること，及び利用資格のない者に利用させること。

二　要機密情報（機密性３情報又は機密性２情報）である情報を開示すること。

三　契約担当者（用度係長）あるいはソフトウェア総括担当者への申請なしに，新たにソフトウェアをインストールすること及びコンピューターの設定の変更を行うこと。ただし，オープンソースソフトウェアについては「PC取扱ガイドライン」によるものとする。

四　グローバル・アクティブラーニングセンター長の許可を得ずに，新たにコンピューターシステムを本校内に設置すること及び本校のネットワークに接続すること。

五　情報セキュリティ副責任者の許可を得ずに，本校の情報システムを利用して情報公開を行うこと。

六　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の要請に基づかずに本校内通信回線と本校外通信回線を接続すること。
七　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の許可なくネットワーク上の通信を監視し，又は情報システムの利用情報を取得すること。ただし，本校の実施規程においてその実行が義務付けられる場合は除く。
八　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の要請に基づかずに管理権限のないシステムのセキュリティ上の脆弱性を検知すること。ただし，本校の実施規程においてその実行が義務付けられる場合は除く。

２　ファイルの自動公衆送信機能を持ったP2Pソフトウェアについては，教育・研究目的以外にこれを利用してはならない。なお，当該ソフトウェアを教育・研究目的に利用する場合は情報セキュリティ副責任者の許可を得なければならない。

第２章　情報システムの利用

（ユーザーIDの管理）

第９条　本校の教職員は，本校の情報システムに係わるユーザーIDについて，次の各号に掲げる事項を遵守しなければならない。
一　自分に付与されたユーザーID以外のユーザーIDを用いて，本校の情報システムを利用しないこと。
二　自分に付与されたユーザーIDを他者が情報システムを利用する目的のために付与及び貸与しないこと。
三　自分に付与されたユーザーIDを，他者に知られるような状態で放置しないこと。
四　職務のためにユーザーIDを利用する必要がなくなった場合は，情報セキュリティ推進責任者に届け出ること。ただし，個別の届出が必要ないと，あらかじめアカウント管理を行う者が定めている場合はこの限りでない。
五　管理者権限を持つユーザーIDを付与された者は，管理者としての業務遂行時に限定して，当該ユーザーIDを利用すること。

２　本校の情報システムに係るアカウントが停止されたときは，情報セキュリティ副責任者に停止からの復帰を申請することができる。

（パスワードの管理）

第１０条　本校の教職員は，本校の管理区域・安全区域への入退場又は本校の情報システムの利用認証に係わるパスワードについて，次の各号に掲げる事項を遵守しなければならない。
一　他者に知られないようにすること。
二　他者に教えないこと。
三　容易に推測されないものにすること。
四　パスワードを定期的に変更するように定められている場合は，その指示に従っ

て定期的に変更すること。
五　忘れないように努めること。
六　異なる識別コードに対して，共通のパスワードを用いないこと。
七　異なる情報システムに対して，識別コード及びパスワード情報の共通の組合せを用いないこと。（シングルサインオンを除く。）
２　前項のパスワードが他者に使用され又はその危険が発生した場合は，本校の教職員は直ちに情報セキュリティ推進責任者及び情報セキュリティ副責任者にその旨を報告しなければならない。

（ICカードの管理）
第１１条　本校の教職員は，本校の管理区域への入退場又は本校の情報システムの利用認証に係わるICカードについて，次の各号に掲げる事項を遵守しなければならない。
一　本人が意図せずに使われることのないように安全措置を講じること。
二　他者に付与及び貸与しないこと。
三　利用する必要がなくなった場合は，遅滞なく情報セキュリティ推進責任者に返還すること。
２　前項のICカードを紛失しないように管理すること。なお，紛失した場合は，本校の教職員は直ちにその旨を情報セキュリティ推進責任者及び情報セキュリティ副責任者に報告しなければならない。

（情報システムの取扱と注意事項）
第１２条　本校の教職員が本校の業務にPCを利用する場合は，「PC取扱ガイドライン」に従って取り扱い，当該PCおよび扱う情報を適切に保護しなければならない。

（自己が管理するPCへの対策）
第１３条　本校の教職員は，自己の管理するPCについて，情報セキュリティの維持を心がけるとともに，次の各号に掲げる対策を講じなければならない。
一　マルウェア対策ソフトウェアを導入し，マルウェア感染を予防できるよう努めること。
二　インストールされているOSやアプリケーションソフトの脆弱性が通知された場合は，速やかに当該ソフトウェアのアップデートを実施するか，代替措置を講じること。
三　自己の管理するPCの第三者による不正な遠隔操作を予防するための対策を講じること。
四　無許可で利用されることがないように，部屋に施錠する，アクセス制限をかける等の対策を講じること。
２　前項以外の情報セキュリティ対策については，別に定める「コンピューターシステムの情報セキュリティ対策実施手順」及び「モバイルPC情報セキュリティ対策実施手順」によるものとする。

（その他の情報システムの利用）

第１４条　本校の教職員が前条に係る以外の情報システムを利用する場合は，情報セキュリティ推進責任者の許可を得て，その指示に従って必要な措置を講じなければならない。

（電子メールの利用）

第１５条　本校の教職員が電子メールを利用する場合は，「電子メール利用ガイドライン」及び「本校外情報セキュリティ水準低下防止手順」に従うと共に，次の各号に掲げる事項を遵守しなければならない。

一　不正プログラムの感染，情報の漏えい，誤った相手への情報の送信等の脅威に注意すること。

二　機構の業務遂行目的以外での通信を行わないこと。

三　電子メール使用上のマナーに反する行為を行わないこと。

（ウェブの利用及び公開）

第１６条　本校の教職員がウェブブラウザを利用する場合は，「ウェブブラウザ利用ガイドライン」及び「本校外情報セキュリティ水準低下防止手順」に従うと共に，次の各号に掲げる事項を遵守しなければならない。

一　不正プログラムの感染，情報の漏えい，誤った相手への情報の送信等の脅威に注意すること。

二　機構の業務遂行目的以外でのウェブの閲覧を行わないこと。

第１７条　本校の教職員がウェブサーバーを運用しようとする場合は，事前に広報センター長の許可を得た上で，「ウェブサーバー設定確認実施書」に従ってサーバーを設定しなければならない。

２　本校の教職員がウェブページを作成し公開する場合は，広報センター長の許可を得た上で，セキュリティ及び著作権等の問題に配慮するとともに本校の社会的信用を失わせることのないように注意し，「ウェブ公開ガイドライン」に従わなければならない。

３　ウェブサーバー運用及びウェブページ公開に関して，情報セキュリティ関連法令，機構の基本方針又は実施規則，並びに本校の実施規程又は実施手順に違反する行為が認められた場合は，広報センター長が許可を取り消し，運用者の承諾なしにウェブコンテンツの削除，ウェブサーバーのネットワークからの切り離し等の措置を講ずることが出来るものとする。

第１８条　本校の教職員が，本校外の者に対して，アクセスや送信させることを目的としてドメイン名を告知する場合には，情報セキュリティ推進責任者によって許可されたドメイン名（kagoshima-ct.ac.jp）を使わなければならない。

２　特に必要な場合においては，次の各号に掲げる事項を遵守することを条件とし

て，前項以外のドメイン名の使用を申請し,情報セキュリティ推進責任者の許可を得るものとする。

一　電子メール送信を行う場合，告知内容についての問合せ先として，前項で定めたドメイン名による電子メールアドレスを明記する，あるいは前項で定めるドメイン名による電子署名を添付すること。

二　告知するドメイン名に管理する組織名を明記すること。

３　本校の教職員が本校外の者に対して電子メールを送信する場合は，第１項又は前項のドメイン上の電子メールアドレスを使用しなければならない。

４　本校の教職員が，本校外の者に対して，アクセスさせることを目的としてサーバーを使用する場合は，第１項又は第２項で定めるドメイン名を持つサーバーを使用しなければならない。ただし，次に掲げる場合を除く。

一　ソーシャルメディアサービスによる情報発信を行う場合。

（本校支給以外の端末からの利用及び本校支給以外の端末の持込）

第１９条　本校の教職員が本校支給以外の端末から公開ウェブ以外の本校情報システムへアクセスする場合又は本校支給以外の端末を利用し本校の業務を遂行する場合は，次の各号に掲げる事項を遵守しなければならない。

一　事前に情報セキュリティ推進責任者の許可を得ること。

二　利用する当該情報システムには，可能な限り強固な認証システムを備えるとともに，ログ機能を設定し，動作させること。

三　当該情報システムにマルウェア対策ソフトウェアをインストールし，最新のウィルス定義ファイルに更新すること。

四　当該情報システムを許可された者以外に利用させない措置を講ずるとともに，不正操作等による情報漏えい及び盗難防止に注意すること。

五　当該情報システムで動作するソフトウェアがすべて正規のライセンスを受けたものであることを確認すること。

六　情報セキュリティ副責任者の許可なく，当該情報システムに要保護情報（要機密情報・要保全情報・要安定情報のいずれかに該当するものをいう。）を複製保持しないこと。

（情報システムの導入）

第２０条　本校の教職員が新たにソフトウェアを購入又は借用し自己の管理するPCにインストールして利用しようとする場合は，事前に契約担当者（用度係長）に届出るとともに，「情報システム導入手順」に従って必要な措置を講じなければならない。

第２１条　本校の教職員が新たにコンピューターシステムを購入又は借用して利用しようとする場合は「情報システム導入手順」に従って必要な措置を講じなければならない。

（接続の許可）

第２２条　本校の教職員が本校情報システムに新たにコンピューターシステムを接続しようとする場合は，事前に「学内ＬＡＮ接続申請書」等による申請によりグローバル・アクティブラーニングセンター長の許可を得るとともに，「情報システム導入手順」に従って必要な措置を取らなければならない。

（ウェブ会議サービス利用時の対策・１）

第２３条　本校の教職員がウェブ会議サービスを利用する場合，以下の情報セキュリティ対策を実施するものとする。

一　原則として，本校が支給する端末を利用すること。

二　原則として，本校が利用を許可したウェブ会議サービスを利用すること。

三　利用するウェブ会議サービスのソフトウェアが，最新の状態であることを確認すること。

四　要機密情報を取り扱う場合は，可能な限りエンドツーエンド（E2E）の暗号化を行うこと。

（ウェブ会議サービス利用時の対策・２）

第２４条　本校の教職員は，無関係な者をウェブ会議に参加させないために，以下を例とする対策を行うものとする。

一　会議室にアクセスするためのパスワード等をかけること。

二　会議の参加者に会議室にアクセスするためのパスワード等を通知する際は，第三者に知られないよう安全な方法で通知すること。

三　待機室を設けて参加者と確認できた者だけを会議室に入室させること。

四　なりすましや入れ替わりが疑われるなどの不審な参加者を会議室から退室させること。

第３章　情報の取扱い

（情報の格付）

第２５条　本校の教職員が機構の業務遂行目的で情報を作成する時又は情報を入手してその管理を開始する時には，格付規則第６条から第９条までの措置を講じなければならない。

（情報の利用に関する遵守事項）

第２６条　本校の教職員は，機構が扱う情報の利用に際して，次の各号に掲げる事項を遵守しなければならない。

一　利用する情報に明示等された格付けに従って，当該情報を適切に取り扱うこと。この場合において，格付けに加えて取扱制限の明示等がされている場合は，当該取扱制限の指示内容に従って取り扱うこと。

二　本校の業務遂行以外の目的で，要保護情報を本校の管理区域外へ持ち出さないこと。
三　要保護情報を放置しないこと。
四　要機密情報を必要以上に複製しないこと。
五　要機密情報を必要以上に配付しないこと。

（情報の保存・バックアップに関する遵守事項）
第２７条　本校の教職員は，機構が扱う情報の保存に際して，次の各号に掲げる事項を遵守しなければならない。
一　電磁的記録媒体に保存された要保護情報について，適切なアクセス制御を行うこと。
二　情報の格付け及び取扱制限に応じて，情報が保存された外部記録媒体を適切に管理すること。
三　機密性３情報を機器等に保存する際，以下の措置を講ずること。
ア　インターネットに接続しない端末，サーバー等を使用すること。
イ　暗号化による保護を行うこと。
ウ　保存した機器等について，盗難及び不正な持ち出し等から保護する対策を講ずること。
四　要機密情報を適切に管理すること。
五　要機密情報を電磁的記録媒体に保存する場合は，パスワード等を用いて保護するか又は情報を暗号化したり，施錠のできる書庫・保管庫に媒体を保存したりするなどの措置を講ずること。
六　要機密情報を情報システム又は外部記録媒体に保存する場合は，暗号化を行う必要性の有無を検討し，必要があると認めたときは，暗号化すること。
七　要保全情報（完全性２情報）を電磁的記録媒体に保存する場合には，電子署名の付与を行うなど，改ざん防止のための措置を講ずること。
八　要保全情報又は要安定情報（可用性２情報）である電磁的記録又は重要な設計書について，バックアップを取得すること。
九　要保全情報若しくは要安定情報である電磁的記録のバックアップ又は重要な設計書のバックアップについて，災害等により生ずる支障の有無を検討し，支障があると認めたときは，適切な措置を講ずること。
十　電磁的記録媒体に保存された情報の保存期間が定められている場合は，当該情報を保存期間が満了する日まで保存し，保存期間を延長する必要性がない場合は速やかに消去すること。
十一　情報の保存方法を変更する場合には，格付，取扱制限及び記録媒体の特性に応じて必要な措置を講ずること。
十二　入手した情報の格付及び取扱制限が不明な場合には，情報の作成元又は入手元への確認を行うこと。

（情報の運搬・送信に関する遵守事項）

第２８条　本校の教職員は，機構が扱う情報の運搬・送信に際して，次の各号に掲げる事項を遵守しなければならない。

一　機密性３情報を運搬・送信する場合は，情報セキュリティ責任者の許可を得ること。また暗号化措置を施した上で情報セキュリティ責任者が指定する方法により運搬・送信すること。

二　機密性２情報を運搬・送信する場合は，情報セキュリティ責任者に届け出ること。

三　要保護情報を運搬・送信する場合は，安全確保に留意して，当該情報の運搬・送信手段を決定し，送信又は運搬のいずれによるかを選択すること。

四　要保護情報を運搬する場合は，情報の格付け及び取扱制限に応じて，安全確保のための適切な措置を講ずること。

五　要保護情報を含む電磁的記録を運搬・送信する場合は，次の措置を講ずること。

ア　パスワードを用いて保護する必要性の有無を検討し，必要がない場合を除き，情報にパスワードを設定すること。

イ　暗号化を行う必要性の有無を検討し，必要があると認めたときは，情報を暗号化すること。

ウ　電子署名の付与を行う必要性の有無を検討し，必要があると認めたときは，情報に電子署名を付与すること。

エ　バックアップを行う必要性の有無を検討し，必要があると認めたときは，情報のバックアップを取得すること。

オ　運搬・送信中の滅失，紛失，運搬・送信先への到着時間の遅延等により支障が起こるおそれに対し，同一の電磁的記録を異なる運搬・送信経路で運搬・送信するなどの措置を講ずる必要性の有無を検討し，必要があると認めたときは，所要の措置を講ずること。

（情報の公表に関する遵守事項）

第２９条　本校の教職員は，機構が扱う情報の公表に際して，次の各号に掲げる事項を遵守しなければならない。

一　当該情報が機密性１情報に格付けされるものであることを確認すること。

二　電磁的記録を公表する場合は，当該情報の付加情報等からの不用意な情報漏えいを防止する措置を採ること。

（情報の提供に関する遵守事項）

第３０条　本校の教職員は，機構が扱う情報の提供に際して，次の各号に掲げる事項を遵守しなければならないものとする。

一　機密性３情報を教職員以外の者に提供する場合は，情報セキュリティ責任者の許可を得ること。

二　機密性２情報を教職員以外の者に提供する場合は，情報セキュリティ責任者に届け出ること。

三　要保護情報を教職員以外の者に提供する場合は，提供先において，当該情報に付された情報の格付け及び取扱制限に応じて適切に取り扱われるための措置を講ずること。

四　電磁的記録を提供する場合は，当該記録の付加情報等からの不用意な情報漏えいを防止する措置を講ずること。

（情報の消去に関する遵守事項）

第３１条　本校の教職員は，情報の消去に際して，次の各号に掲げる事項を遵守しなければならない。

一　要機密情報を廃棄する場合は，復元が困難な状態にすること。

二　情報システム又は外部記録媒体を廃棄する場合は，すべての情報を復元が困難な状態にする（以下「抹消する」という。）こと。

三　情報システム又は外部記録媒体を他者へ提供する場合は，当該機器に保存された不要な要機密情報を抹消すること。

（適正なアクセス制御）

第３２条　本校の教職員は，情報システムに装備された機能を用いて，当該情報システムに保存される情報の格付けと取扱制限の指示内容に従って，必要なアクセス制御の設定をしなければならない。

（要保護情報等の処理等）

第３３条　本校の教職員がモバイルPCによって要保護情報等を処理する場合，管理区域外において要保護情報等を処理する場合又は本校支給以外の端末で要保護情報等を処理する場合においては，当該情報システムについて第１９条第二号から第六号までの措置を取るとともに，次の各号に掲げる事項を遵守しなければならない。

一　機密性３情報については，事前に情報セキュリティ責任者の許可を得，情報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うけること。

二　前号に係る情報処理の完了時にその旨を報告すること。ただし，報告を要しないとされた場合はこの限りでない。

三　機密性２情報については，事前に情報セキュリティ責任者に届け出ること。

２　本校の教職員が要保護情報等を取り扱う情報システム又は要保護情報等を含む記憶媒体を本校の管理区域外へ持ち出す場合は，次の各号に掲げる事項を遵守しなければならない。

一　機密性３情報については，事前に情報セキュリティ責任者の許可を得，情報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うけること。

二　前号に係る持出完了時にその旨を報告すること。ただし，報告を要しないとされた場合はこの限りでない。

三　機密性２情報については，情報セキュリティ責任者に届出ること。

（個人情報の取得と管理）

第３４条　本校の教職員が電子的に個人情報の提供を求める場合は，提供を求める情報の範囲，利用の目的及び当該情報が伝達される範囲を，あらかじめ相手方に示さなければならない。

２　前項の個人情報について当人から請求があった場合には，開示，訂正又は削除について適正に対応しなければならない。また，当該請求のための手続をあらかじめ示さなければならない。

第４章　物理的及び環境的セキュリティ対策

（物理的入退場管理）

第３５条　本校の教職員は，物理的セキュリティについて，次の各号に掲げる事項を遵守しなければならない。

一　管理区域へ入場する場合は，既に入場している他の教職員に自身の入場が認識されるよう努めること。また，管理区域から退場する際，退場前の他の教職員に自身の退場が認識されるよう努めること。

二　事務室，研究室，その他本校の情報資産を有する部屋を無人にする場合は必ず施錠すること。ただし，研究室については，遵守事項を周知徹底のうえ教職員以外の経常的利用者に部屋の管理を代行させることができる。

三　退職その他の事由により本校の教職員の身分を失う場合は，使用していた物理的アクセス権限を全て情報セキュリティ副責任者に返却すること。

四　要保護情報を取り扱う場合は，不正アクセスや情報への損傷等の危険性が及ばない物理的に保護された場所で行うこと。

五　安全区域の扉が開放状態にある場合は，情報セキュリティ副責任者及び当該区域の管理担当者へ報告し，報告を受けた管理担当者は状況監視を行うこと。

六　立入り権限のない安全区域へ立入らないこと。

七　要保護情報又はそれを取扱う情報システムの安全区域への持込み又は持出しを行う場合は，情報セキュリティ責任者の許可を得ること。

第３５条の２　前条第七号の場合において，グローバル・アクティブラーニングセンター長及び同副センター長，並びにキャンパス情報ネットワークシステム管理者がグローバル・アクティブラーニングセンターサーバ室への要保護情報又はそれを扱う情報システムの持込み又は持出しを行う場合は，この限りでない。

（委託業者，受渡業者及び臨時利用者等の管理）

第３６条　本校の教職員は，委託業者，受渡業者及び臨時利用者への対応において，次の各号に掲げる事項を遵守しなければならない。

一　管理区域へ委託業者，受渡業者又は臨時利用者を立入らせる場合は，本校の教職員が立ち会うこと。

二　前号の場合において，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，作業場所を確認できる場所で常に立ち会うこと。

三　管理区域内に不審者を発見した場合は，直ちに学生課又は守衛室へ連絡すること。

四　特定受渡場所以外で物品の受渡しを行う場合には，要機密情報又は要機密情報を処理する情報システムに触れさせない措置をとること。

第３７条　本校の教職員が面談等，学生の教育に関連する目的で本校の学生の保護者の来校をうける場合は，管理区域への入退場の記録を残すものとする。

第３８条　本校の教職員が体育祭，高専祭，学校開放事業等の行事で一般の来校者を受け入れる場合は，事前に情報セキュリティ副責任者の許可を得たうえで次の各号に掲げる措置をとらなければならない。

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，破壊等の行為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。

第５章　教育

（情報セキュリティ対策教育の受講義務）

第３９条　本校の教職員は，「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受講しなければならない。

２　前項が遵守できなかった場合は，本校の教職員は情報セキュリティ副責任者にその理由を報告しなければならない。

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の発生時における報告と応急措置）

第４０条　本校の教職員が情報セキュリティインシデント（以下「インシデント」という。）を発見したときは次の各号に掲げる措置を講じるとともに「情報セキュリティインシデント対応手順」に従わなければならない。

一　当該インシデントに関係する者に連絡するとともに，情報セキュリティ副責任者が定めた報告手順により，情報セキュリティ管理者及び情報セキュリティ推進責任者にその旨を報告すること。

二　当該インシデントが発生した際の対処手順の有無を確認し，当該対処手順を実

施できる場合は，その手順に従うこと。
三　当該インシデントについて対処手順がない場合又はその有無を確認できない場合は，その対処についての指示をうけるまで被害の拡大防止に努めるものとし，指示があった時にその指示に従うこと。

第７章　調達，ソフトウェア開発及び業務委託

第４１条　本校の教職員が情報システムを調達（購入に準ずるリース等を含む。）する場合，ソフトウェアを開発する場合及び本校の業務のすべて又はその一部を第三者に委託する場合は，情報セキュリティ副責任者に要請し，情報セキュリティ推進責任者に情報セキュリティ対策の実施を依頼するものとする。

第８章　違反と例外措置

（セキュリティ確保に関する義務）
第４２条　本校の教職員が，情報セキュリティ関連法令，機構の基本方針又は実施規則，若しくは本校の情報セキュリティ実施規程又は実施手順への重大な違反を知った場合は，情報セキュリティ副責任者にその旨を報告しなければならない。
２　前項の場合において，違反者が情報セキュリティ副責任者である場合は，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４３条　本校の教職員が例外措置の適用を希望する場合は，定められた審査手続に従い，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。）に例外措置の適用を申請することとし，申請の際には，次の各号に掲げる項目を明確にしなければならない。ただし，職務の遂行に緊急を要する等の場合であって，機構情報セキュリティ関連規程等の規定とは異なる代替の方法を直ちに採用すること又は規定を実施しないことが不可避のときは，事後速やかに申請し許可を得なければならない。
一　申請者の情報（氏名，所属及び連絡先）
二　例外措置の適用を申請する機構情報セキュリティ関連規程等の適用箇所（規程名と条項等）
三　例外措置の適用を申請する期間
四　例外措置の適用を申請する措置内容（講ずる代替手段等）
五　例外措置の適用を終了したときの報告方法
六　例外措置の適用を申請する理由
２　例外措置の適用について許可を受け，例外措置を適用した場合は，それを終了したときに，当該例外措置の許可権限者にその旨を報告しなければならない。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。

第９章　自己点検及び見直し

第４４条　本校の教職員は，別に定める「情報セキュリティ自己点検実施手順」に従って自らが実施した情報セキュリティ対策を点検しなければならない。

２　前項の規定に基づく点検結果において，課題又は問題点が認められる場合は，当該事項の見直しを行わなければならない。

３　自己点検の結果及び見直しの実施について，情報セキュリティ副責任者に報告しなければならない。

第１０章　管理的業務

（学外者による情報システムの利用）

第４５条　本校の教職員は，共同研究，地域協働教育，産官学連携活動等本校の業務を遂行するために，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取得させて，本校の情報システムを一定期間にわたり継続的に利用させることができる。

２　前項の利用にあたり，当該業務に責任を持つ教職員は「学外者による情報システム利用手順」に従って申請し，情報セキュリティ副責任者の許可を得なければならない。この場合において，情報セキュリティ副責任者は，当該利用者に対してアカウントを発行するものとする。また，利用を終了させる場合においては，アカウントを削除するものとする。

３　前項の教職員は，当該利用者が情報セキュリティ関連法令，機構の基本方針及び実施規則，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しなければならない。

第４６条　本校の教職員は，新たな情報システムの設置，情報システムのメンテナンス，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目的で，経常的利用者以外の者に本校の情報システムを短期間に限って利用させることができる。

２　前項の利用にあたり，当該業務に責任を持つ教職員は「学外者による情報システム利用手順」に従って申請し，情報セキュリティ副責任者の許可を得なければならない。また利用が終了した時に，情報セキュリティ副責任者に報告しなければならない。

３　前項の教職員は，当該利用者が利用を開始する前に「臨時利用者に対する注意事項」を周知し，また利用中において適正な利用が行われるよう監督しなければならない。

（利用記録の採取）

第４７条　複数の者が利用する情報システムを管理する教職員は，次の各号に掲げる条件が満たされる場合，情報セキュリティ副責任者の許可を得て当該情報システムに係る利用記録（以下「利用記録」という。）を採取することができる。

一　利用記録の使用目的が明確にされていること。

二　前号の目的が，法令の遵守，情報セキュリティの確保，課金，学生の教育その他当該情報システムの運用又は機構の業務遂行に必要なものに限られていること。

三　採取する利用記録の範囲が明確であり，第一号の目的にとって必要なものであること。

四　利用記録の採取の事実，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第３項により利用記録を伝達する対象者を利用者に開示すること。

２　当該教職員は，前項の目的のために必要な限りで，利用記録を閲覧することができる。

３　当該教職員は，第１項の目的のために必要な限りで，利用記録を他者に伝達することができる。

４　当該教職員又は利用記録の伝達を受けた者は，第１項の目的のために必要な限りで，これを保有することができる。

５　前項において，不要となった利用記録は，直ちに破棄しなければならない。ただし，情報セキュリティ副責任者の許可を得て，利用記録から個人情報に係る部分を削除したうえで，情報システムの運用管理又は機構の業務遂行のための資料とすることができる。この場合において，当該資料は，なるべく体系的に整理し，常に活用できるよう保存するものとする。

（管理的業務執行者としての責務）

第４８条　情報セキュリティ管理者，安全区域に常任する教職員及び情報セキュリティ管理者と同等の業務遂行を委ねられた教職員は，本校のサイバーセキュリティ管理規程及びサイバーセキュリティ推進規程を熟知し，必要に応じて情報セキュリティ副責任者の責務を補佐又は代行しなければならない。

第４９条　情報セキュリティ推進員及び情報セキュリティ推進員と同等の業務遂行を委ねられた教職員は，本校のサイバーセキュリティ管理規程及びサイバーセキュリティ推進規程を熟知し，必要に応じて情報セキュリティ推進責任者の責務を補佐又は代行しなければならない。

第４９条の２　第４８条及び前条に定める者は，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及び実施規則，並びに本校の実施規程及び実施手順に対する重大な違反を知った場合は，上司にその旨を報告しなければならない。ただし，違反者が上司である場合は，違反者でない上司まで委任経路を遡って報告するものとする。

附　則

1　この規程は，令和４年１２月７日から施行する。

2　鹿児島工業高等専門学校情報セキュリティ教職員規程（平成２３年３月１８日制定）は，廃止する。