電動モビリティシステム専門職大学情報セキュリティ対策規程

（目的）

第１条　この規程は、電動モビリティシステム専門職大学セキュリティポリシー（以下「ポリシー」という。）に基づき、電動モビリティシステム専門職大学（以下「本学」という。）における情報及び情報システムの情報セキュリティ対策について必要な事項を定め、もって本学の保有する情報の保護と活用及び情報セキュリティ水準の適切な維持向上を図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意義は、当該各号に定めるところによる。

(1)　情報コンテンツ　本学が収集し管理・運用する教育研究及び事務処理に係る全ての情報（媒体（電磁的媒体、光学的媒体、紙媒体等）の種類を問わない。）をいう。

(2)　情報システム　情報処理及び情報ネットワークに係わるシステムで、次のいずれかに該当するものをいう。

ア　本学により、所有され、又は管理されているもの

イ　契約又はその他協定に基づき、本学に提供されるもの

ウ　本学情報ネットワークに接続する機器

(3)　情報資産　情報システム及び情報コンテンツを合わせたものをいう。

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

(5)　学生等　本学学則に定める学部学生、科目等履修生、研究生、聴講生、外国人留学生その他学長が認めた者をいう。

(6)　教職員等　本学を設置する法人の役員及び本学に勤務する常勤又は非常勤の教職員（派遣職員を含む。）、客員教授等、共同研究員等その他学長が認めた者をいう。

(7)　利用者　教職員等及び学生等で、情報資産を利用する許可を受けて利用する者をいう。

(8)　インシデント　情報資産への侵害又は情報セキュリティを脅かす事案をいう。

(9)　クラウドサービス　事業者との相互契約に基づき、事業者によって定義されたインタフェースを用いて、共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスでき、利用者によって自由にリソースの設定・管理が可能なサービスをいう。

(10)　約款によるクラウドサービス　クラウドサービスのうち、画一的な約款に基づいた契約により、事業者がインターネット上の不特定多数の利用者に提供する電子メール、ファイルストレージ、グループウェア等のサービスをいう。

（適用範囲）
第３条 この規程は、情報資産を管理・運用する全ての者及び利用者に適用する。
（秘密保持）
第４条　前条の者は、職務上知り得た秘密を漏らしてはならない。その職を退いた後も、同様とする。
（情報セキュリティ最高責任者）
第５条　本学に、情報セキュリティ最高責任者(Chief Information Security Officer。以下「CISO」という。)を置き、学長をもって充てる。
２　CISOは、本学の情報セキュリティに関する全ての権限及び責任を有し、情報セキュリティに関する事項を統括する。
３　CISOは、本学及び学外組織の情報資産に対する重大な侵害又は脅威等のインシデントが発生し、又は発生するおそれがある場合は、速やかに第18条に規定する対策本部を設置し、当該インシデントに対処しなければならない。
４　CISOは、学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を講じなければならない。
（情報セキュリティ副責任者）
第６条　本学に、CISOを補佐するため、情報セキュリティ副責任者(以下「副CISO」という。)を置き、学部長をもって充てる。
２　副CISOは、CISOに事故がある時は、その職務を代行する。
（情報セキュリティ委員会）
第７条　本学に、情報セキュリティ委員会(以下「委員会」という。)を置く。
２　委員会に、委員長及び委員を置き、CISOが指名する者をもって充てる。
３　前項の委員長及び委員の任期は2年とし、再任を妨げない。
４　第２項の委員の指名に当たっては、委員会委員長は、委員会の業務について適任者がいる場合は、CISOに推薦することができる。
５　監事は、委員会に陪席し、意見を述べることができる。
６　委員会は、次の各号に掲げる業務を実施する。
(1) この規程の改廃及びポリシーの評価・見直し等の重要事項に係る検討及び関係部門との連絡調整
(2)　情報セキュリティに関する注意喚起又は各種通知等の業務
(3)　インシデント情報の集積及び分析並びにインシデントの予防対策及び再発防止策の検討及び策定
(4)　インシデントが発生した場合又は発生するおそれがある場合の迅速かつ円滑な対応に関する必要措置
(5) 特に緊急を要するインシデントが発生した場合又は発生することが想定される場合において、初動体制としての緊急措置
(6) その他情報セキュリティに関すること。
７　前各項に定めるもののほか、委員会に関し必要な事項は、CISO が別に定める。

８　委員会の事務は、事務局で処理する。

(管理責任)

第８条　情報資産の管理について、CISO は適切な措置を講じなければならない。

(利用者の責任)

第９条　情報コンテンツを利用する者は、その機密性、完全性及び可用性を踏まえ、別表第１に規定する格付けに応じて適切に利用する責任を負う。

２　情報システムの利用者は、当該情報システムの利用マニュアル等を始め学内諸規則を遵守して利用する責任を負う。

(物理的セキュリティ)

第１０条　CISO は、情報システムを保護するため、必要な措置を講じなければならない。

(人的セキュリティ)

第１１条　利用者は、この規程及び関係法令等を遵守し、本学の情報資産に対する情報セキュリティを確保しなければならない。

２　CISO は、本学に帰属する情報資産に対する情報セキュリティを確保するため、必要な措置を講じなければならない。

(技術的セキュリティ)

第１２条　CISO は、本学の情報資産を不正アクセス等から保護するため、必要な措置を講じなければならない。

(外部委託)

第１３条　本学の業務を外部委託により遂行する場合は、委託先においてポリシー及びそれに基づく規程等に適合した情報セキュリティ対策を確実に実施させる必要があるため、次の各号に掲げる対策を実施するものとする。

(1)　契約

情報システムの開発、運用若しくは保守又は情報コンテンツの処理を外部委託事業者(下請けとして受託する業者を含む。)に発注する場合は、遵守事項を契約書に明記すること。

(2)　委託先選定

外部委託を実施する場合には、選定基準を定め選定条件に従って委託先を選定すること。

(3)　再委託

委託先がその役務内容を一部再委託する場合には、再委託され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よう、前号の選定条件を委託先に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を本学に提供し承認を受けるよう、仕様に含めること。

(4)　委託先管理

事務局長は、委託先における情報セキュリティ対策や情報セキュリティの履

行状況及び情報の取扱事項が遵守されていること等を確認すること。

(5)　クラウドサービスの利用

クラウドサービスを利用する場合には、クラウド基盤部分を含む情報の流通経路全般を俯瞰し、総合的に対策を検討又は構成した上でセキュリティを確保すること。

(6)　約款によるクラウドサービスの利用

約款によるクラウドサービスを利用する場合には、本学の情報をサービス提供事業者等に送信していることを十分認識し、リスクを十分に踏まえた上で利用の可否を判断し、情報セキュリティ対策を適切に講ずること。

(個人情報の取扱い)

第１４条　個人情報の取扱いに関しては、電動モビリティシステム専門職大学個人情報保護規程（令和５年３月 29 日制定）によるものとする。

(管理体制)

第１５条　CISO は、本学及び学外組織の情報資産に対する侵害が発生した場合の連絡、証拠保全及び被害拡大の防止並びに復旧等の必要な措置を迅速かつ円滑に講じるとともに、再発防止のための必要な対策が講じられるよう、情報危機管理体制を整備しなければならない。

(連絡体制)

第１６条　インシデントを認めた者は、速やかに CISO に連絡し、次の各号に掲げる事項について報告しなければならない。

(1)　インシデントの内容

(2)　インシデントが発生した原因として想定される行為

(3)　確認した被害・影響範囲

(4)　その他連絡に必要な事項

(対応体制)

第１７条　前項の連絡を受けた CISO は、当該インシデントを調査の上、侵害度及び被害度等の重大性を迅速に判断し、適切に対処しなければならない。

２　CISO は、前項の対処内容、対処結果等について、文部科学省に報告するものとする。

３　CISO は、第 1 項の判断の結果、必要な場合には、当該インシデントに対する対策本部(以下「対策本部」という。)を設置するものとする。

(対策本部)

第１８条　対策本部は、次に掲げる者をもって組織する。

(1)　本部長　CISO

(2)　副本部長　副 CISO

(3)　本部員　事務局長及び CISO が指名する教職員

２　対策本部は、必要に応じ委員会に協力を求めることができる。

３　対策本部は、当該インシデントに対処した経過を記録する。

４　対策本部は、当該インシデントに係る証拠保全の実施を完了し、再発防止の暫定措置について検討する。
５　対策本部は、当該インシデントを調査し、関係部署にその調査結果について連絡する。
６　CISO は、前項の調査結果を受け、当該インシデントを文部科学省に報告する。
７　対策本部は、被疑ユーザがいる場合は、調査及び審査を実施する。
８　対策本部は、再発防止の暫定措置を講じた後には、情報システム等を速やかに復旧するための措置を講じるものする。
９　委員会は、事後対策案を作成し、CISO に報告する。
１０　CISO は、事後対策案に基づき、当該インシデントの事後対策について必要な措置を講じるものとする。
１１　本部長は、当該インシデントの対処終了をもって対策本部を解散する。

(再発防止の措置)

第１９条　委員会は、当該インシデントに係るリスク分析を行い、実施手順及び各種セキュリティ対策の改善等の再発防止計画を策定し、CISO に報告しなければならない。
２　CISO は、再発防止計画が有効であると認める場合には、当該計画を実施する。
３　学長は、再発防止のため必要と認める場合には、不正アクセス行為の禁止等に関する法律(平成 11 年法律 128 号)の規定に基づき、都道府県公安委員会に対し援助の申出を行うものとする。

(罰則)

第２０条　CISO は、第３条に掲げる者が、具体的な命令や注意喚起に従わない場合、本学の情報セキュリティ水準を低下させると認められる行為を繰り返す場合又は情報セキュリティの確保に必要な対策を怠った場合は、情報システムの利用を停止する等の措置を講じるものとする。
２　前項の措置のほか、懲戒処分に該当するものについては、本学の就業規則又は電動モビリティシステム専門職大学学生の懲戒等に関する規程(令和５年 11 月 15 日制定)の定めるところによる。

(その他)

第２１条　この規程に定めるもののほか、本学の情報セキュリティに関し必要な事項は、教授会の議を経て学長が定める。

附　則

この規程は、令和６年３月 27 日から施行する。

別表第１（第９条関係）

情報コンテンツの格付け

１　機密性

格付け	内容
機密性３情報	秘密保全の必要が高く，特定の者以外に公開することのできない情報コンテンツ
機密性２情報	学外に公開することのできない情報コンテンツ
機密性１情報	公表済みの情報など機密性３情報又は機密性２情報以外の情報

２　完全性

格付け	内容
完全性２情報	改ざん，破損等により，本学の活動遂行に支障を及ぼすおそれがある情報（書面を除く。）
完全性１情報	完全性２情報以外の情報（書面を除く。）

３　可用性

格付け	内容
可用性２情報	滅失，紛失など当該情報が利用不可能であることにより，本学の活動遂行に支障を及ぼすおそれがある情報（書面を除く。）
可用性１情報	可用性２情報以外の情報（書面を除く。）

参考：取扱制限の種類・指定例

区分	取扱制限の種類	指定例
機密性についての取扱制限	複製・配付	複製・配付禁止，複製・配付要許可
	転送・転記	転送・転記禁止，転送・転記要許可
	暗号化	保存時暗号化必須，通信時暗号化必須
	再利用	再利用禁止，再利用要許可
	参照者の範囲	構成員限り，関係者限り
完全性についての取扱制限	保存期間・場所	○年期間保存、施錠可能な書庫で保存
	書換え	書換禁止，書換要許可
	削除	削除禁止，削除要許可
	保存期間満了後の措置	保存期間満了後要廃棄
可用性についての取扱制限	復旧までに許容できる時間	○時間以内復旧，○日以内復旧
	保存場所	DVD 等光学ディスクに保存，共有ファイルサーバ保存必須