神戸市公立大学法人　情報セキュリティポリシー

2023年４月１日
規則第20号

第１章　情報セキュリティ基本方針

１　目的

神戸市公立大学法人（以下「法人」という。）の情報システムが取り扱う情報には、学生（科目等履修生、研究生を含む。）および教職員の個人情報や運営上重要な情報が多数含まれており、情報資産を人的脅威や災害、事故等様々な脅威から防御することは、プライバシー保護や、質の高い教育研究活動、高等教育の実施及び適切な法人運営を確保するためにも必要不可欠である。

このため、法人が保有する情報資産の機密性、完全性及び可用性を維持することを目的として神戸市公立大学法人情報セキュリティポリシー（以下「情報セキュリティポリシー」という。）を定める。

２　定義

(1) ネットワーク

情報機器を相互に接続するための通信網及びその構成機器（ハードウェア及びソフトウェア）をいう。

(2) 情報システム

情報機器、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

(3) データ

電子計算機処理に係る入出力帳票、磁気テープ、磁気ディスク、光ディスク、その他の電磁的記録媒体及び紙資料に記録されている情報又は通信回線により送受信される情報をいう。

(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) インシデント

情報セキュリティに関して生じる、法令又は法人の例規に反する事故または事件をいう。

(6) 機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

(7) 完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

(8) 可用性

情報にアクセスすることを認められた者が、必要なときに中断されることなく、

情報にアクセスできる状態を確保することをいう。

(9) 学生及び教職員

学生（科目等履修生、研究生等を含む。）及び教職員など情報資産を取り扱うすべての者をいう。

3　情報セキュリティポリシーの位置付け及び構成

情報セキュリティポリシーは、法人が保有する情報資産に関する情報セキュリティ対策について総合的かつ体系的にまとめられた情報セキュリティ対策の基本となるものであり、情報セキュリティ基本方針及び情報セキュリティ対策基準により構成される。

4　情報セキュリティポリシーの適用範囲

情報セキュリティポリシーの適用範囲は、法人における情報資産及び情報資産に接するすべての学生及び教職員とする。

また、情報資産の範囲は次のとおりとする。

(1)　物理資産

情報機器・ネットワーク・電磁的記録媒体及び紙資料等物理的な形状を有する資産

(2)　データ資産

情報機器・電磁的記録媒体に保管されている情報及び紙資料の情報

(3)　ソフトウェア資産

コンピュータ等の情報機器において稼動するプログラム

(4)　サービス資産

電源、メールサービス等契約により提供される情報システムで必要なすべての構成要素（リソースと能力）

5　学生及び教職員の義務

学生及び教職員は、情報セキュリティの重要性について共通の認識を持つとともに、情報資産の利用にあたっては情報セキュリティポリシーを遵守するものとする。

6　情報資産への脅威

情報セキュリティ対策を講じるうえでは、情報資産に対する脅威の発生度合いや発生した場合の影響を考慮するものとする。特に次の脅威については、十分な措置を講じるものとする。

(1)　部外者による不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃、又は不正操作によるデータやプログラムの持ち出し・盗聴・改ざん・消去、情報機器及び媒体の盗難等

(2)　学生及び教職員並びに外部委託業者による情報資産の学外への無断持ち出し、無許可ソフトウェアの使用等の規定違反、意図しない操作、不正アクセス又は不正操作によるデータやプログラムの学外への持ち出し・盗聴・改ざん・消去、物

理資産の盗難、規定外の情報機器接続によるデータ漏えい等

(3)　地震、落雷、火災等の災害、事故、故障等によるサービス及び業務の停止

(4)　大規模・広範囲にわたる疾病による要因不足に伴うシステム運用の機能不全等

(5)　電力供給の途絶、通信の途絶等のインフラの障害からの波及等

7　情報セキュリティ管理体制

法人の情報資産について、適切に情報セキュリティ対策を推進・管理するための体制を確立するものとする。

そのために次に掲げるものを置く。必要な体制、役割、権限等については情報セキュリティ対策基準にて定める。

(1)　情報セキュリティ最高責任者

法人事務局長を情報セキュリティ最高責任者とする。

(2)　情報管理委員会

次に掲げる事項を審議する。組織等については、別途定める。

①　法人、神戸市外国語大学（以下「大学」という。）、及び神戸市立工業高等専門学校（以下「高等専門学校」という。）の情報セキュリティに関する重要事項

②　情報セキュリティポリシーの改廃

③　情報セキュリティポリシー遵守状況の把握と必要な措置の検討

④　前３号に掲げるもののほか、法人事務局、大学及び高等専門学校における情報セキュリティの確保に資する事項

8　情報セキュリティ対策

情報資産に対する脅威から情報資産を保護するため、以下の情報セキュリティ対策を講ずるものとする。

(1)　情報資産の分類と管理

法人の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を講じる。

(2)　物理的セキュリティ

情報機器の設置場所への入退室、サーバ等の管理、通信回線及び情報機器への物理的な対策を講じる。

(3)　人的セキュリティ

情報セキュリティに関し、すべての学生及び教職員が遵守すべき事項を定めるとともに、十分な研修・訓練及び啓発を実施するなど人的な対策を講じる。

(4)　技術的セキュリティ

情報機器の管理、アクセス制御、コンピュータウイルス等不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

(5)　運用面のセキュリティ

情報システムに関し、情報セキュリティポリシーの遵守状況の確認、外部委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じる。また、情報資産への侵害等インシデントが発生した場合に、迅速かつ適切に対応するため、緊急時対応計画を策定する。

(6)　外部サービスの利用

外部委託する場合には、外部委託業者を選定し、情報セキュリティ要件を明記した契約を締結し、外部委託業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。

９　情報セキュリティ監査及び自己点検の実施

情報セキュリティ対策の実施状況を評価するため、定期的及び必要に応じて情報セキュリティ監査及び自己点検を実施する。

１０　情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等を踏まえ、必要に応じ適宜情報セキュリティポリシーの見直しを行う。

１１　情報セキュリティ個別基準の策定

情報セキュリティポリシーを補完するために必要な内容に関して、具体的な内容を定める情報セキュリティ個別基準を策定するものとする。

１２　情報セキュリティ実施手順の策定

情報セキュリティポリシー及び情報セキュリティ個別基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。

第２章　情報セキュリティ対策基準

第１節　法人事務局及び大学

１　目的

本節情報セキュリティ対策基準とは、法人事務局及び大学（以下「大学等」という。）における、情報セキュリティ基本方針に基づき情報セキュリティ対策等を実施するために共通の基準として具体的な遵守事項及び判断基準を定めたものである。

２　適用範囲

法人事務局又は大学における情報資産及び情報資産に接する、学生及び教職員など法人事務局又は大学において情報資産を取り扱うすべての者（以下「大学等構成員」という。）とする。

３　情報セキュリティ管理体制

法人又は大学の情報資産について、適切に情報セキュリティ対策を推進・管理するための体制を確立するものとする。

そのために次に掲げるものを置く。

(1)　情報セキュリティ最高責任者

法人事務局長を情報セキュリティ最高責任者とする。

(2)　部門情報統括責任者

学生担当副学長、教務担当副学長、学術担当副学長、大学事務局長及び大学事務局次長を部門情報統括責任者とする。

(3)　情報基盤管理者

経営グループ課長及び総務グループ課長を情報基盤管理者とする。

(4)　情報管理者

情報資産を取り扱うグループの長を所管するグループの情報管理者とする。

(5)　業務システム管理者

各業務システムを所管するグループの長を当該業務システムに関する業務システム管理者とする。

(6)　情報監査統括責任者

法人事務局担当部長、大学事務局次長を情報監査統括責任者とする。

(7)　大学情報セキュリティ委員会

次に掲げる事項を審議し、その内容を情報管理委員会を経て情報セキュリティ最高責任者に報告する。組織等については、別途定める。

①　大学等の情報セキュリティに関する重要事項の審議・決定

②　情報セキュリティポリシー遵守状況の把握と必要な措置の検討

③　前２号に掲げるもののほか、大学等における情報セキュリティの確保に資する事項

4　権限と責任

情報セキュリティ基本方針で定めた情報セキュリティ管理体制における権限と責任については次のとおりとする。

(1)　情報セキュリティ最高責任者

ア　情報セキュリティ最高責任者は、法人における全てのネットワーク、情報システム、データ等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。

イ　情報セキュリティ最高責任者は、必要に応じ、情報セキュリティに関する専門的な知識及び経験を有する専門家をアドバイザーとして置くことができる。

(2)　部門情報統括責任者

ア　部門情報統括責任者は情報セキュリティ最高責任者を補佐しなければならない。

イ　部門情報統括責任者は、管轄する部門全てのネットワーク、情報システム、データ等の情報資産における開発、設定の変更、運用、見直し等を行う統括的な権

限及び責任を有する。

ウ　部門情報統括責任者は、管轄する部門全ての情報資産における情報セキュリティ対策に関する統括的な権限及び責任を有する。

エ　部門情報統括責任者は、所管する部門情報基盤管理者、情報管理者及び業務システム管理者に対して、情報セキュリティに関する指導及び助言を行う権限を有する。

オ　部門情報統括責任者は、所管する部門の情報資産に対するインシデントが発生した場合又は発生のおそれがある場合に、情報セキュリティ最高責任者の指示に従い、情報セキュリティ最高責任者が不在の場合には自らの判断に基づき、必要かつ十分な措置を行う権限及び責任を有する。

カ　部門情報統括責任者は、緊急時等の円滑な情報提供を図るため、情報セキュリティ最高責任者、部門情報統括責任者、情報基盤管理者、情報管理者及び業務システム管理者を網羅する連絡体制を整備しなければならない。

(3)　情報基盤管理者

ア　情報基盤管理者は部門情報統括責任者を補佐し、その実務を担当する。

イ　情報基盤管理者は、大学等の共通的なネットワーク、情報システム、データ等の情報資産における開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

ウ　情報基盤管理者は、大学等の共通的なネットワーク、情報システム、データ等の情報資産における情報セキュリティ対策に関する権限及び責任を有する。

エ　情報基盤管理者は、大学等の共通的なネットワーク、情報システム、データ等の情報資産に関する情報セキュリティ実施手順を策定し、その維持・管理を行う。

オ　情報基盤管理者は、大学等の情報資産に対するインシデントが発生した場合又は発生のおそれがある場合に、部門情報統括責任者及び情報セキュリティ最高責任者へ速やかに報告を行い、指示を仰がなければならない。

カ　情報基盤管理者は、大学等の共通的なネットワーク、情報システム、データ等の情報資産のうち情報機器についての物理的セキュリティに関する管理を情報管理者に行わせることができる。

(4)　情報管理者

ア　情報管理者は、所管グループ内におけるデータ等の情報資産の情報セキュリティ対策に関する権限及び責任を有する。

イ　情報管理者は、情報基盤管理者の指示に従い大学等の共通的なネットワーク、情報システム、データ等の情報資産のうち所管組織内の情報機器についての物理的セキュリティに関する管理を行う。

ウ　情報管理者は、所管グループ内におけるデータ等の情報資産に対するインシデントが発生した場合又は発生のおそれがある場合には、情報基盤管理者、業務シ

ステム管理者へ速やかに報告を行い、指示を仰がねばならない。

(5)　業務システム管理者

ア　業務システム管理者は、当該業務システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

イ　業務システム管理者は、当該業務システムの情報セキュリティ対策に関する権限及び責任を有する。

ウ　業務システム管理者は、当該業務システムに係る情報セキュリティ実施手順を策定し、その維持・管理を行う。

エ　業務システム管理者は、当該業務システムにおいて情報資産に対するインシデントが発生した場合又は発生のおそれがある場合には、情報基盤管理者へ速やかに報告を行い、指示を仰がねばならない。

オ　業務システム管理者は、当該業務システムにおける開発、設定の変更、運用等についての作業を業務システム管理者が指名する者に行わせることができる。

(6)　情報監査統括責任者

情報監査統括責任者は、情報セキュリティ監査の計画、実施、報告等を行う権限及び責任を有する。

(7)　兼務の禁止

ア　情報セキュリティ対策の実施において、やむを得ない場合を除き、承認又は許可の申請を行う者とその承認者又は許可者は、同じ者が兼務してはならない。

イ　監査を受ける者とその監査を実施する者は、同じ者が兼務してはならない。

5　情報資産の分類と管理

(1)　情報資産の管理責任

ア　管理責任

情報資産は、情報基盤管理者、業務システム管理者及び情報管理者等権限のある者（以下「情報資産管理責任者」という）がそれぞれ所管する情報資産についての管理責任を有する。また、情報資産管理責任者は、当該情報資産の利用範囲を定めなければならない。

イ　大学等構成員の責任

大学等構成員は、情報資産の作成・入手・利用に際しては、十分にその責任を自覚したうえで行わなければならない。

ウ　複製等の管理

データが複製又は送信された場合には、当該複製等も原本と同様に管理しなければならない。

(2)　情報資産の分類と管理方法

ア　情報資産の分類

（ア）　対象となる情報資産は、各々の情報資産の機密性、完全性及び可用性を踏

まえ、次の重要性分類に従って分類する。

機密性

3	大学等で取り扱う情報資産のうち、特に機密性を要するもの ・個人情報に関するもの ・法令の規定により秘密を守る義務を課されているもの ・部外に知られることが適当でない法人その他団体に関するもの ・部外に漏れた場合に法人事務局及び大学の信頼を著しく害するおそれのあるもの ・公開することでセキュリティ侵害が生じるおそれがあるもの
2	直ちに一般に公表することを前提としていないもの （機密性３には当てはまらないが、広報などは行っていないもの）
1	機密性２又は機密性３の情報資産以外のもの

完全性

3	大学等で取り扱う情報資産のうち、特に完全性を要するもの （改ざんあるいは誤りがあると学生等の権利が侵害される、又は法人事務局及び大学運営の適確な遂行に支障を及ぼす可能性があるもの） ・個人情報に関するもの ・法令の規定により秘密を守る義務を課されているもの ・部外に知られることが適当でない法人その他団体に関するもの ・部外に漏れた場合に大学等の信頼を著しく害するおそれのあるもの
2	改ざんあるいは誤りがあると組織に軽微な影響が発生する可能性があるもの
1	完全性２又は完全性３の情報資産以外のもの

可用性

3	大学等で取り扱う情報資産のうち、特に可用性を要するもの （利用できないと学生等の権利が侵害される、又は法人事務局及び大学事務の安定的な遂行に支障を及ぼす可能性があるもの） ・滅失し又は損傷した場合その復元が著しく困難であるため大学等の円滑な運営が妨げられるおそれのあるもの
2	利用できないことが一定時間以上継続すると学生等の権利が侵害される、又は大学等の事務の安定的な遂行に支障を及ぼす可能性があるもの
1	可用性２又は可用性３の情報資産以外のもの

（イ） 情報資産の機密性、完全性、可用性のいずれかの重要性分類２以上に分類される情報資産は、この対策基準の対象とする。

また、重要性分類１の情報資産も、必要なものはできる限りこの対策基準

に準じた対応を講じるものとする。

イ　情報資産に対するリスク分析の実施

（ア）　大学等が保有する情報資産に対して、あらかじめ定められた方法に従い、リスク分析を行わなければならない。

（イ）　情報セキュリティ最高責任者は、リスクを受容するための基準を作成し、受容可能なリスクの水準を定めなければならない。

（ウ）　リスク分析の結果、リスクの大きさが受容可能なリスクの水準を上回る場合、リスク対応計画書を作成し、情報セキュリティ最高責任者の承認を得たうえで、適切なリスク管理を行わなければならない。リスク対応計画書には、リスク対応を施すための活動内容、資源、責任体制及び優先順位等を記載すること。

（エ）　リスク分析及び受容可能なリスクの水準等は、情報セキュリティに関する状況の変化等を踏まえ、定期的に見直しを行うものとする。

ウ　情報資産の管理方法

（ア）　情報資産の管理

①　情報資産について、第三者が重要性の識別を容易に認識できないよう適切な管理を行わなければならない。

②　すべての情報資産を明確に識別し、重要な情報資産に対しては必要に応じて目録を作成して管理しなければならない。

（イ）　データの作成

①　次のデータを作成してはならない。

a　差別、名誉毀損、侮辱、ハラスメントにあたる情報

b　個人情報やプライバシーを侵害する情報

c　守秘義務に違反する情報

d　著作権等の財産権を侵害する情報

e　業務に必要のない情報

f　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

②　データの作成時に重要性分類に基づき、当該データの分類を定めなければならない。

③　作成途上のデータについても、紛失や流出等を防止しなければならない。また、データの作成途上で不要になった場合は、当該データを消去しなければならない。

（ウ）　情報資産の入手

①　大学等内の者が作成した情報資産を入手した者は、入手元の情報資産の分類に基づいた取扱いをしなければならない。

② 大学等外の者が作成した情報資産を入手した者は、重要性分類に基づき、当該情報の分類を定めなければならない。

③ 情報資産を入手した者は、入手した情報資産の分類が不明な場合、情報資産管理責任者に判断を仰がなければならない。

（エ） 情報資産の利用

① 情報資産を利用する者は、情報資産について定められた目的以外に利用してはならない。

② 情報資産の利用においては、情報資産の分類に応じ、利用者及びにアクセス権限を定めなければならない。

③ 機密性３のデータは、情報資産管理責任者の許可を得た場合、複写、複製、送付又は送信を行うことができる。ただし、暗号化等による情報漏えい対策を施さなければならない。

④ 電子メールにより機密性２のデータを送信する者は、必要に応じ暗号化等による情報漏えい対策を施さなければならない。

⑤ 情報資産を利用する者は、物理資産に情報資産の分類が異なるデータが複数記録されている場合、最高度の分類に従って、当該物理資産を取り扱わなければならない。

（オ） 情報資産の保管・運搬

① 情報資産管理責任者は、情報資産の重要性分類に従って、情報資産の保管を適切に行わなければならない。

② 最終的に確定したデータを記録した物理資産は、書込禁止措置を行ったうえで保管しなければならない。

③ 情報資産管理責任者は、持ち運び可能な物理資産を、耐火、耐熱、耐水及び耐湿対策を講じたうえ施錠可能な場所への保管等適切な管理を行わなければならない。

④ 情報資産管理責任者は、情報システムのバックアップで取得したデータを記録する物理資産を長期保管する場合は、自然災害を被る可能性が低い地域への保管を考慮しなければならない。

⑤ 機密性２以上の情報資産が保管された物理資産の搬送にあたっては、必要に応じ鍵付きのケース等に格納し、暗号化の設定を行う等、情報資産の不正利用を防止するための措置を施さなければならない。

⑥ 機密性２以上の情報資産が保管された物理資産を運搬する者は、情報資産管理責任者に許可を得なければならない。

（カ） 情報資産の提供・公表

① 機密性３の情報資産を外部に提供する場合、次の措置を行わなければならない。

a　事前に情報管理者の許可を得る。

b　提出日時・提出者及び提供概要を記録する。

c　必要に応じ暗号化の設定を行う。

② 情報資産管理責任者は、公開する情報資産について、完全性を確保しなければならない。

（キ） 情報資産の廃棄

① 情報資産の廃棄を行う場合、次の措置を行わなければならない。

a　事前に情報基盤管理者の許可を得る。

b　廃棄処理の日時、担当者及び処理内容を記録する。

② 電磁的記録媒体が不要となった場合は、当該媒体に含まれるデータの消去を行ったうえで焼却、裁断又は溶解等により物理的に破壊し、復元不可能な状態にして廃棄しなければならない。紙媒体が不要となった場合は、焼却、裁断又は溶解等により廃棄しなければならない。

エ　文書の管理

（ア） 情報セキュリティ対策基準を実施していくうえで必要とされる文書は、神戸市公立大学法人文書管理規程（2007年４月規程第96号）等の定めに従い管理しなければならない。

（イ） 情報セキュリティに係る文書（以下「文書」という）を作成又は更新する場合は、あらかじめ定められた者による承認を受けなければならない。

（ウ） 文書は、定期的に見直しを行い、必要に応じて更新しなければならない。

（エ） 文書を廃棄する場合は、廃棄文書が誤って使用されないようにしなければならない。ただし、廃棄文書を保持する必要がある場合には、廃棄文書と分かるように適切な識別を施さなければならない。

オ　記録の管理

情報セキュリティ対策基準の効果的運用の証拠を示すために、記録を作成し、適切な管理をしなければならない。

(3)　情報セキュリティに関する統一的な窓口の設置（ＣＳＩＲＴ）

ア　ＣＳＩＲＴ の設置

情報セキュリティ最高責任者は、情報セキュリティに関する事件・事故、システム上の欠陥及び誤動作（以下、「情報セキュリティに関する事件・事故等」という。）に対処する組織としてCSIRTを設置し、法人事務局経営グループがその役割を担う。

イ　ＣＳＩＲＴの役割

ＣＳＩＲＴは、情報セキュリティに関する事件・事故等に対処し、被害拡大防止、復旧、再発防止等に向けた対応を、迅速かつ的確に実施する。

ウ　ＣＳＩＲＴの連絡体制

ＣＳＩＲＴの統一窓口は、情報管理者とする。情報管理者は、情報セキュリティに関する事件・事故等が発生したときは、その内容に応じて、業務システム管理者等と適宜連絡し、国や県等の関係機関との情報共有を行う。

6　物理的セキュリティ

(1)　サーバ等の管理

ア　入退室の管理

情報資産管理責任者は、重要性分類３のデータが記録されている物理資産の保管場所及びそれを取扱う情報機器設置場所の入退室について、適正な管理を行わなければならない。

なかでも、ネットワークの基幹機器及び重要な情報システムを設置し、当該機器の管理及び運用を行う部屋（以下「管理区域」という）については、次の事項に従い厳重な管理を行わなければならない。

（ア）　外部からの侵入が容易にできないようにしなければならない。

（イ）　施設管理部門と連携して、管理区域から外部に通ずるドアは必要最小限とし、鍵、監視機能、警報装置等によって許可されていない者の立入りを防止しなければならない。

（ウ）　管理区域への入退室は、許可された者のみに制限し、ＩＤカード等による認証及び入退室管理簿の記載による入退室管理を行わなければならない。

（エ）　大学等構成員は、管理区域に入室する場合、身分証明書等を携帯し、求めにより提示しなければならない。

（オ）　外部からの訪問者が管理区域に入室する場合には、必要に応じて立ち入り区域を制限したうえで、管理区域への入退室を許可された職員が付き添うものとし、外見上職員と区別できる措置を施さなければならない。

（カ）　管理区域については、当該システムに関連しない情報機器、データ等を持ち込ませないようにしなければならない。

イ　装置の取付け等

（ア）　情報基盤管理者及び業務システム管理者は、ネットワーク機器及び情報システム機器の取付けを行う場合、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適切な固定を行う等必要な措置を施さなければならない。

（イ）　情報基盤管理者及び業務システム管理者は、システムの停止により、法人事務及び大学事務の執行等に重大な影響を及ぼすおそれがあるものについて二重化等を行い、同一データを保持し、システムの運用が停止しないように努めなければならない。

（ウ）　権限のある者以外の者が容易に操作できないように、情報基盤管理者及び業務システム管理者は、利用者を識別するためのクレデンシャルを設定する

等の措置を施さなければならない。

ウ　電源

（ア）　情報基盤管理者及び業務システム管理者は、サーバ等の機器の電源については、当該機器を適切に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。

（イ）　情報基盤管理者及び業務システム管理者は、落雷等による過電流に対してサーバ等の機器を保護するための措置を施さなければならない。

エ　配線

（ア）　配線の変更、追加については、情報基盤管理者及び業務システム管理者等限られた者の権限とする。

（イ）　情報基盤管理者及び業務システム管理者は、施設管理部門と連携し、通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用する等必要な措置を施さなければならない。

（ウ）　情報基盤管理者及び業務システム管理者は、主要な箇所の通信ケーブル及び電源ケーブルについて、施設管理部門から損傷等の報告があった場合、連携して対応しなければならない。

（エ）　情報基盤管理者及び業務システム管理者は、ネットワーク接続口（ハブのポート等）を他者が容易に接続できない場所に設置する等適切に管理しなければならない。

オ　機器の定期保守及び修理

（ア）　情報基盤管理者及び業務システム管理者は、可用性３のサーバ等の機器は、定期保守を実施しなければならない。

（イ）　情報基盤管理者、業務システム管理者及び情報管理者は、記憶装置を内蔵する機器を外部の業者に修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合、外部の業者に故障を修理させるにあたり、修理を委託する事業者との間で、守秘義務契約を締結するほか、秘密保持体制の確認などを行わなければならない。

カ　消火薬剤及び消防用設備

消火薬剤及び消防用設備等は、サーバや通信機器に影響を与えるものであってはならない。

キ　敷地外へのサーバや通信機器の設置

情報基盤管理者及び業務システム管理者は、大学の敷地外にサーバや通信機器を設置する場合、部門情報統括責任者の許可を得なければならない。また、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

ク　物理資産の廃棄等

情報基盤管理者、業務システム管理者及び情報管理者は、物理資産を廃棄、リース返却等をする場合、物理資産内部の記憶装置から、すべてのデータを消去の上、復元不可能な状態にする措置を施さなければならない。

ケ　物理資産等の搬出入

（ア）　情報基盤管理者及び業務システム管理者は、物理資産等を搬入する場合、あらかじめ当該物理資産等の既存情報システムに与える影響について、職員に確認を行わせなければならない。

（イ）　物理資産等の搬入出には職員が同行する等の必要な措置を施さなければならない。

(2)　ネットワークの管理

ア　情報基盤管理者及び業務システム管理者は、学内の通信回線及び通信回線装置を施設管理部門と連携し、適切に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適切に保管しなければならない。

イ　情報基盤管理者及び業務システム管理者は、通信回線による外部へのネットワーク接続は必要最低限のものに限定し、できる限り接続ポイントを減らさなければならない。

ウ　部門情報統括責任者は、所管する情報システムにおいて機密性３の情報資産を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適切な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。

エ　ネットワークに使用する回線は送信途上においてデータの破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策が実施されたものでなければならない。

(3)　情報機器の管理

ア　情報基盤管理者、業務システム管理者及び情報管理者は、執務室の情報機器について、盗難防止のため、ワイヤーによる固定等の物理的措置を講じなければならない。

イ　情報基盤管理者及び業務システム管理者は、情報システムにアクセスする場合には、利用者を識別するためのクレデンシャルの入力による認証を必要とするように設定しなければならない。

また、必要に応じてＢＩＯＳ認証、ハードディスク認証を併用しなければならない。

ウ　情報基盤管理者及び業務システム管理者は、端末のディスクデータの暗号化等の機能を有効にしなければならない。

(4)　複合機の管理

ア　情報基盤管理者、業務システム管理者及び情報管理者は、複合機を調達する場

合、当該複合機が備える機能、設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適切な情報セキュリティ要件を策定しなければならない。

イ　情報基盤管理者、業務システム管理者及び情報管理者は、複合機が備える機能について、運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。

ウ　情報基盤管理者、業務システム管理者及び情報管理者は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消又は再利用できないようにする対策を講じなければならない。

7　人的セキュリティ

(1)　大学等構成員の責務

ア　情報セキュリティポリシー等の遵守義務

大学等構成員は、情報セキュリティポリシー及びこれに基づく文書に定められている事項を遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点がある場合には、情報管理者等権限のある者に相談し、指示を仰がなければならない。

イ　法令等の遵守義務

大学等構成員は、職務の遂行において使用する情報資産を保護するために、法令等を遵守しこれに従わなければならない。

- 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）
- 著作権法（昭和45年法律第48号）
- 個人情報の保護に関する法律（平成15年法律第57号）
- サイバーセキュリティ基本法（平成26年法律第104号）
- 神戸市個人情報保護法の施行に関する条例（令和４年12月条例第17号）
- 神戸市公立大学法人職員就業規則（2023年４月規則第28号）
- 神戸市公立大学法人再雇用職員就業規則（2023年４月規則第29号）
- 神戸市公立大学法人契約職員就業規則（2023年４月規則第30号）
- 神戸市公立大学法人パート職員就業規則（2023年４月規則第31号）
- 神戸市公立大学法人留学生担当嘱託講師就業規則（2023年４月規則第32号）
- 神戸市公立大学法人非常勤講師就業規則（2023年４月規則第33号）
- 神戸市公立大学法人特任教員就業規則（2023年４月規則第34号）
- 神戸市公立大学法人文書管理規程

ウ　指示に基づいた情報資産の利用等

大学等構成員は、情報管理者等権限のある者の指示等に従い、情報資産を利用するとともに、開発、設定の変更、運用、更新等の作業を行う。

エ　情報資産利用上の注意事項

大学等構成員は、様々な情報の作成、利用、保存等のため物理資産の利用に際して、以下の事項を遵守しなければならない。

（ア） 大学等の管理するネットワークに新規かつ固定的に物理資産を接続する場合、又は新たに物理資産を使用する場合は、事前に情報基盤管理者及び業務システム管理者の許可を得なければならない。

物理資産の持込みについては、別途定める手順に従うものとする。

（イ） 物理資産のソフトウェアに関するセキュリティ機能の設定を情報基盤管理者又は業務システム管理者の許可なく変更してはならない。

（ウ） 物理資産は脆弱性を持たないよう可能な限り最新の状態でなければならない。

（エ） 許可を受けた物理資産の利用を取りやめる場合には、物理資産内にデータが残留した状態とならないよう、すべてのデータを復元できないよう措置を施し、情報基盤管理者又は業務システム管理者に届け出なければならない。

（オ） 物理資産やデータ資産について、第三者に使用されないこと、また、情報管理者等管理権限のある者の許可なく情報を閲覧されることがないように、離席時の端末のロックやデータ資産を容易に閲覧されない場所への保管等適切な措置を講じなければならない。

（カ） 物理資産の紛失及び盗難を発生させないように注意しなければならない。

（キ） 学外のインターネットカフェなどに設置されているような不特定多数の人が操作（利用）可能な情報機器を用いての学内情報システムへのアクセスを行ってはならない。

オ　学内ＬＡＮへの接続

学内ＬＡＮにコンピュータを接続する者は、学内ＬＡＮ接続申請書を事務局に提出し、情報基盤管理者から接続の許可を得なければならない。

また設置責任者が接続変更及び廃止するときは、情報基盤管理者に所定の申請書により申請を行い、承認を受けなければならない。

カ　情報資産の学外利用

教員は、情報資産の学外の利用にあたっては、以下の手順を遵守しなければならない。

① 情報資産で機密性、完全性、可用性分類２以上の情報を取り扱う場合、暗号化等による情報漏えい対策や作業中ののぞき見防止等を行わなければならない。

② 情報資産は可能な限り強固な認証システムを備え、ログ機能を持っており、それらの機能が設定され動作していなければならない。

またコンピュータウイルス等対策ソフトウェア及び定義ファイルは常に最新のものに保ち、システムを保護可能でなければならない。

③　情報資産の画面を他者から見える状態で利用してはならない。また当該システムを他者が支配操作可能な状態にしてはならない。（不正操作、情報漏洩及び盗難防止）

④　情報資産を大学情報システムに再接続する場合、接続に先だってコンピュータウイルス等対策ソフトウェアでチェックをしなければならない。

キ　学外の情報システムからの利用

教員は、学外の情報システムから大学等の管理するネットワークへ接続する場合、以下の手順を遵守しなければならない。

①　学外の情報システムを用いて、公開のウェブ以外の大学等の管理するネットワークの接続にあたって、事前に情報基盤管理者の許可を得なければならない。

②　本条の目的に利用する学外の情報システムは可能な限り強固な認証システムを備え、ログ機能を持っており、それらの機能が設定され動作していなければならない。

また、コンピュータウイルス等対策ソフトウェア及び定義ファイルは常に最新のものに保ち、システムを保護可能でなければならない。

③　これらの情報システムを許可された者以外に利用させてはならない。また当該システムを他者が支配操作可能な状態にしてはならない。（不正操作、情報漏洩及び盗難防止）

④　情報セキュリティ最高責任者の許可なく、これらの情報システムに機密性、完全性、可用性分類２以上の情報を複製保持してはならない。

⑤　これらの情報システムで動作するソフトウェアは正規のライセンスを受けたものでなければならない。

ク　情報資産の学外への持ち出し

情報資産を学外へ持ち出す場合、次の措置を行わなければならない。

①　持出し日時、持出し者、持出す情報資産概要及び持出す手段について記録を作成した上で、事前に情報資産管理者の許可を得る。

②　必要に応じ暗号化又は主体認証の設定を行う。

③　情報資産管理者の許可なくデータ資産の複製や保存を行ってはならない。

④　情報資産管理者は、機密性２以上、可用性３又は完全性３の情報資産を持ち出す場合、安全管理措置を定めなければならない。

教員については、別途定める手順に従うものとする。

ケ　利用上の禁止事項

大学等構成員は、法人事務局又は大学の情報システムについて、次の各号に定める行為を行ってはならない。

① 情報システム、データ、情報システムへのアクセス、電子メール及びインターネットの私的及び営利や娯楽目的に利用する行為
② 指定以外の方法による学外からの法人事務局又は大学の情報システムへのアクセスする行為
③ あらかじめ指定された情報システム以外を利用する行為
④ 持出した情報資産を情報資産管理責任者の許可がない他の情報機器へ複製や保存する行為
⑤ 守秘義務に違反する行為
⑥ 差別、名誉毀損、侮辱又はハラスメントにあたる行為
⑦ 個人情報又はプライバシーを侵害する行為
⑧ 情報基盤管理者又は業務システム管理者の許可を得ず、ソフトウェアのインストールや情報機器の設定の変更を行なう行為
⑨ 情報基盤管理者等権限のある者の許可なく情報機器をネットワークに接続する行為
⑩ 著作権等の財産権を侵害する行為
⑪ 通信の秘密を侵害する行為
⑫ 法人若しくは大学のネットワーク上の通信を監視し、又は情報機器の利用情報を取得する行為
⑬ 自情報機器宛以外のネットワーク通信を傍受又は盗聴する行為
⑭ Ｐ２Ｐファイル交換ソフトウェアを利用する行為
⑮ 過度な負荷等により大学等の円滑な情報システムの運用を妨げる行為
⑯ 不正アクセス禁止法に反する行為又はこれに類する行為
⑰ その他法令に基づく処罰の対象となる行為
⑱ 上記の行為を助長する行為

コ 異動、退職時等の遵守義務

大学等構成員は、異動、退職等により法人事務局又は大学を離れる場合には、利用していた情報資産を、返却しなければならない。また、その後も業務上知り得た情報を他に漏らしてはならない。

サ 人材派遣職員等

人材派遣職員および非常勤嘱託職員が情報資産を取り扱う必要が生じた場合は、情報管理者等管理権限のある者は従事させる事務の範囲を指定する。また、人材派遣職員および非常勤嘱託職員は「４．人的セキュリティ（１）大学等構成員の責務」のア～キに定める事項を遵守しなければならない。

(2) 研修・訓練

ア 大学等構成員に対する研修・訓練の実施

情報セキュリティ最高責任者は、定期的に大学等構成員に対する情報セキュリティに関する研修・訓練を実施させなければならない。

イ　研修計画の策定及び実施

（ア）　部門情報統括責任者は、大学等構成員に対する情報セキュリティに関する研修計画を定期的に策定し、情報管理委員会に報告しなければならない。

（イ）　大学等構成員を対象とする情報セキュリティに関する研修を毎年度最低１回実施しなければならない。

（ウ）　新規採用の職員を対象とする情報セキュリティに関する研修を実施しなければならない。

（エ）　研修は、部門情報統括責任者、情報基盤管理者、情報管理者、業務システム管理者及びその他の大学等構成員に対して、それぞれの役割、情報セキュリティに関する理解度等に応じたものにしなければならない。

（オ）　部門情報統括責任者は、毎年度１回、情報管理委員会に対して、情報セキュリティに関する研修の実施状況について報告しなければならない。

(3)　インシデントの報告・分析等

ア　インシデントの報告

（ア）　大学等構成員は、情報セキュリティに関するインシデント若しくはシステム上の欠陥及び誤動作を発見した場合、又は外部から報告を受けた場合は、速やかに情報管理者又は業務システム管理者等権限のある者に報告しなければならない。

（イ）　報告を受けた情報管理者又は業務システム管理者等権限のある者は、速やかに部門情報統括責任者並びに情報基盤管理者へ報告しなければならない。

（ウ）　情報基盤管理者は、報告のあったインシデントについて、必要に応じて部門情報統括責任者及び情報セキュリティ最高責任者に報告しなければならない。

イ　インシデントの原因調査と再発防止策

（ア）　インシデントを引き起こした部門の情報管理者又は業務システム管理者は、情報基盤管理者と連携し、インシデントの原因を調査し、再発防止策を策定し、その結果を部門情報統括責任者及び情報セキュリティ最高責任者に報告しなければならない。

（イ）　情報セキュリティ最高責任者は、情報基盤管理者からインシデントについての報告を受けた場合には、その内容を検討し、再発防止策を実施するために必要な措置を講じなければならない。

（ウ）　インシデントを引き起こした部門の情報管理者又は業務システム管理者は、インシデントと再発防止策の記録を保存しなければならない。

(4)　アカウントの発行と管理

大学等構成員である情報システムの利用者に付与された識別符号及び主体認証情報の組合せ、又はそれらのいずれかを指して「アカウント」と言う。

ア　アカウントの発行

（ア）　大学等構成員である情報システムの利用者は、情報基盤管理者及び業務システム管理者等権限のある者からアカウントの交付を受ける。

（イ）　情報基盤管理者及び業務システム管理者等権限のある者は、利用者等からのアカウント発行申請を受理した場合は、遅滞なくアカウントを発行するものとする。

（ウ）　利用する大学等構成員に姓名の変更等識別コードの変更、停止及び廃止が生じた場合には、速やかに所定の申請書により情報基盤管理者及び業務システム管理者等権限のある者に申請し、アカウントの変更、停止及び廃止を受ける。

（エ）　契約により操作を認められた外部委託業者等臨時的に利用させることを目的としてアカウントの交付を受ける場合、申請者は外部委託業者等にこの規則を遵守させなければならない。

（オ）　アカウントを発行するに当たって、暫定主体認証情報で発行する。

イ　アカウントの管理

（ア）　情報基盤管理者及び業務システム管理者等権限のある者はアカウントの適正な管理を行わなければならない。

（イ）　大学等構成員は、次の事項を遵守しなければならない。

①　アカウントを適切に管理しなければならない。

②　アカウントを利用して、学外から法人事務局又は大学の情報システムにアクセスする場合には、定められた手順に従ってアクセスしなければならない。

③　自分のユーザーアカウントを他者に使用させたり、他のユーザーアカウントを使用したり、又他者に開示してはならない。

④　他の者の主体認証情報を聞き出したり使用したり、またその行為を助ける行為をしてはならない。

⑤　アカウントは、大学等構成員間で共有しない。ただし、所属等ごとに配布されたアカウントについては除く。

⑥　共用アカウントを利用する場合は、共用アカウントの利用者以外に利用させてはならない。

⑦　アカウントを他者に使用され又はその危険が発生した場合には、直ちに情報基盤管理者及び業務システム管理者等権限のある者にその旨を報告しなければならない。

⑧　アカウントを紛失した場合には、速やかに情報基盤管理者及び業務シ

ステム管理者等権限のある者に通報し、指示を仰ぐ。

（ウ） 情報基盤管理者及び業務システム管理者は、利用されていないアカウントが放置されないよう、点検しなければならない。

（エ） 情報基盤管理者及び業務システム管理者等権限のある者は、次の場合アカウントを停止する。

① 法人事務局又は大学の情報システムの利用者資格を喪失した場合

② 臨時的に利用させる期間を超過した場合

③ アカウントの紛失通報があった場合

ウ 特権アカウントの管理

（ア） 情報基盤管理者及び業務システム管理者は、管理者権限等の特権を付与されたアカウントを利用する者を必要最小限にし、当該アカウントの漏えい等が発生しないよう、当該アカウントを厳重に管理しなければならない。

（イ） 情報基盤管理者及び業務システム管理者の特権を代行する者は、当該管理者が指名し、部門情報統括責任者が認めた者でなければならない。

（ウ） 情報基盤管理者及び業務システム管理者は、特権を付与されたアカウントの変更について、原則として外部委託事業者に行わせてはならない。

（エ） 情報基盤管理者及び業務システム管理者は、特権を付与されたアカウントについて大学等構成員の情報機器のアカウントと同等あるいはそれ以上のセキュリティ強化を実施しなければならない。

（オ） 情報基盤管理者及び業務システム管理者は、特権によるネットワーク及び情報システムへの接続時間を必要最小限に制限しなければならない。

（カ） 管理者権限を持つアカウントを付与された者は、管理者としての業務遂行時に限定して、当該アカウントを利用しなければならない。

エ 主体認証の管理

（ア） 大学等構成員は、自己の主体認証に関し、次の事項を遵守しなければならない。

① 主体認証は秘密にし、主体認証の照会等には一切応じない。

② 情報システム又は主体認証に対する危険のおそれがある場合には、情報基盤管理者及び業務システム管理者等権限のある者に速やかに報告し、主体認証を速やかに変更する。

③ 原則として、主体認証情報を記載したメモを作成しない。やむを得ず作成する場合は、他人に分からない場所に保管する。

④ 主体認証は定期的又はアクセス回数に基づいて変更し、また、職員は、自己の主体認証は半年を期限に変更する。

⑤ 複数の情報システムを扱う場合は、同一の主体認証を複数のシステムで用いない。

⑥　暫定の主体認証は、最初のログイン時に変更する。
⑦　情報機器の主体認証の記憶機能を利用しない。
⑧　大学等構成員の間で主体認証を共有しない。

（イ）　情報基盤管理者及び業務システム管理者は、主体認証の照会等には一切応じてはならない。

(5)　外部委託に関する管理

ア　契約書の記載事項

（ア）　ネットワーク及び情報システムの開発・保守及びデータ処理その他情報処理に係る業務を外部委託する場合は、当該委託先事業者との間で、下記事項を明記した契約を締結しなければならない。

①　データその他業務上知り得た情報（以下「データ等」という）の秘密の保持に関する事項
②　第三者への委託の禁止又は制限に関する事項
③　データ等の目的以外への使用及び第三者への提供の禁止に関する事項
④　データ等の複写及び複製の禁止に関する事項
⑤　データ等の取扱いに関する事故の発生時における報告義務に関する事項
⑥　データ等の取扱いに関する検査の実施に関する事項
⑦　契約に違反した場合における契約の解除及び損害賠償に関する事項
⑧　委託業務終了時の資産の返還及び廃棄に関する事項
⑨　情報セキュリティポリシー及びこれに基づく文書の遵守に関する事項
⑩　インシデント発生時の公表に関する事項
⑪　委託先の責任者、委託内容、作業者及び作業場所の特定に関する事項

（イ）　前項に加えて、次に掲げる事項を必要に応じて契約書等に明記するよう努めるものとする。

①　提供されるサービスレベルの保証に関する事項
②　従業員に対する研修の実施に関する事項
③　委託業務の定期報告及び緊急時報告義務に関する事項
④　外部施設等への情報資産の搬送時における紛失、盗聴、不正コピー等の防止に関する事項

イ　セキュリティ確保への取組み状況等の調査

情報基盤管理者及び業務システム管理者は、当該外部委託業者のセキュリティ確保への取組み状況、情報セキュリティマネジメントシステムに係る認証取得の状況、個人情報保護に関する取組み状況の調査を行うとともに、契約締結

後においても、定期的又は随時、調査を行い、安全の確保に努めなければならない。部門情報統括責任者から内容の報告を求められた場合には、報告を行わなければならない。

ウ　再委託

再委託を受ける事業者がある場合、「７．人的セキュリティ（５）外部委託に関する管理」のア、イに定める事項は再委託を受ける事業者にも適用する。

エ　クラウドサービスの利用

教職員がクラウドサービスを利用する場合は、別途定める手順に従うものとする。

８　技術的セキュリティ

(1)　情報機器及びネットワークの管理

ア　データの保存

データの保存については、情報基盤管理者等管理権限のある者の定める方法により保存を行わなければならない。

イ　ファイルサーバの設定等

情報基盤管理者がデータを共有するためのファイルサーバを設置する場合には、次の事項を守らなければならない。

（ア）　職員が使用できるファイルサーバのエリアを設定しなければならない。

（イ）　ファイルサーバを所属等の単位で構成又はし、職員が他所属等のフォルダ及びファイルを閲覧及び使用できないように、設定しなければならない。

ウ　アクセス記録の取得等

（ア）　情報基盤管理者及び業務システム管理者は、アクセス記録及び情報セキュリティの確保に必要な記録を取得し、窃取、改ざん、誤消去等を防止する措置を施したうえで一定期間保存する。また、不正アクセスが発見された場合は、それらを分析する。

（イ）　情報基盤管理者及び業務システム管理者は、システムから自動出力したアクセス記録等について、必要に応じてバックアップを取得しなければならない。

エ　仕様書の保管

情報基盤管理者及び業務システム管理者は、ネットワーク構成図、情報システム仕様書等に関し、記録媒体の形態に関わらず、業務上必要とするもの以外の者が閲覧したり、紛失したりすることがないよう、適切な保管をしなければならない。

オ　情報資産のバックアップ

情報基盤管理者及び業務システム管理者は、必要なものはサーバの二重化対策実施の有無に関わらず、定期的に情報資産のバックアップのための対応を行

うものとする。

カ　他団体との情報システムに関する情報等の交換

情報基盤管理者及び業務システム管理者は、他の団体と情報システムに関する情報及びソフトウェアを交換する場合、その取扱いに関する事項をあらかじめ定め、部門情報統括責任者の許可を得なければならない。

キ　外部の者が利用するシステム

情報基盤管理者及び業務システム管理者は、インターネット等により外部の者が利用できるシステムにおいては、必要に応じ他のネットワーク及び情報システムと物理的又は論理的に分ける等、情報セキュリティ対策について特に強固に対策をとらなければならない。

ク　Ｗｅｂサイトでの情報公開時の注意事項

情報基盤管理者及び業務システム管理者は、Ｗｅｂサイトにより情報を公開・提供する場合、次の各号を注意する。

①　当該サイトに係るシステムにおいて情報の漏えい・改ざん・消去、踏み台、サイバー攻撃等を防止しなければならない。

②　研究成果及び研究途中の情報を掲載する際には、公開に問題がないか十分留意すること。

③　古典資料などのデジタルアーカイブをネットで公開する際には、各種権利処理が済んでいるか確認しなければならない。

ケ　ソーシャルメディアサービスによる情報発信時の対策

（ア）　情報基盤管理者及び業務システム管理者は、利用するアカウントによる情報発信が実際の法人事務局又は大学のものであると認識できるようにするためのなりすまし対策として、以下の各号の対策を行うものとする。

①　法人事務局又は大学からの情報発信であることを明らかにするために、アカウント名やアカウント設定の自由記述欄等を利用し、法人事務局又は大学が運用していることを明示すること。

②　法人事務局又は大学からの情報発信であることを明らかにするために、法人事務局又は大学が、法人又は大学ドメイン名を用いて管理しているＷｅｂサイト内において、利用するソーシャルメディアのサービス名と、そのサービスにおけるアカウント名又は当該アカウントページへのハイパーリンクを明記するページを設けること。

③　運用しているソーシャルメディアのアカウント設定の自由記述欄において、当該アカウントの運用を行っている旨の表示をしている大学Ｗｅｂサイト上のページのURLを記載すること。

④　ソーシャルメディアの提供事業者が、アカウント管理者を確認しそれを表示等する、いわゆる「認証アカウント（公式アカウント）」と呼ば

れるアカウントの発行を行っている場合には、可能な限りこれを取得すること。

⑤　URL短縮サービスは、利用するソーシャルメディアが自動的にURLを短縮する機能を持つ場合等、その使用が避けられない場合を除き、使用しないこと。

（イ）　情報基盤管理者及び業務システム管理者は、第三者が何らかの方法で不正にログインを行い、偽の情報を発信するなどの不正行為を行う、いわゆる「アカウント乗っ取り」を防止するために、ソーシャルメディアのログイン主体認証や認証方法について、以下の各号の対策を行うものとする。

①　主体認証を知る担当者を限定し、主体認証の使い回しをせず、適切に管理すること。

②　ソーシャルメディアへのログインに利用する情報機器が不正アクセスされると、その情報機器が不正に遠隔操作されたり、情報機器に保存された主体認証情報が窃取されたりする可能性がある。これらを防止するため、少なくとも情報機器には最新のセキュリティパッチの適用や不正プログラム対策ソフトウェアを導入するなど、適切なセキュリティ対策を実施すること。

（ウ）　情報基盤管理者及び業務システム管理者は、アカウント乗っ取りを確認した場合、被害を最小限にするためログイン主体認証の変更やアカウントの停止を速やかに実施し、情報セキュリティ最高責任者へ速やかに報告を行い指示を仰がなければならない。

（エ）　教職員等が大学名を使用して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は、別途定める手順に従うものとする。

コ　情報機器構成の変更の禁止

大学等構成員は、ネットワーク及び各自に供与された物理資産に対して、情報機器の増設又は改造を行ってはならない。合理的な理由があり、業務を円滑に遂行するためにモデム、ルータ等の通信機器を増設して他の環境（インターネット等）へのネットワーク接続を行うことや、学外からのアクセスを可能とする仕組みを構築しなければならない場合は、部門情報統括責任者の許可を必要とする。軽微な情報機器や通信機器の増設の場合は、情報基盤管理者等権限のある者の許可を必要とする。

サ　電子メール

（ア）　大学等構成員は、電子メールを送受信する場合には、大学が運営又は外部委託した事業者により提供される電子メールサービスを利用するものとする。

（イ）　大学等構成員は、学外の者へ電子メールにより情報を送信する場合は、当

該電子メールのドメイン名に法人または大学ドメイン名を使用するものとする。

（ウ） 部門情報統括責任者は、電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能にしなければならない。

（エ） 部門情報統括責任者は、電子メールに添付されるファイルについて、セキュリティ上問題があると思われるファイルについては、送受信を制限できるようにしなければならない。

（オ） メールアドレス保有者は、複数のあて先に電子メールを送信する場合、必要がある場合を除き他の送信先の電子メールアドレスがわからないようにしなければならない。

（カ） メールアドレス保有者は、重要な電子メールを誤送信した場合、情報管理者及び情報基盤管理者に報告しなければならない。

（キ） 権利違反（知的財産権、著作権、商標権、肖像権、ライセンス権利等）、ハラスメント等の人権を侵害する内容、無礼及び誹謗中傷、ねずみ講に相当する内容、脅迫、個人的な儲け話や勧誘に相当する内容、チェーンメール（同じ内容の電子メールを別の人に転送するように要請するもの等）等に該当する電子メールを送信してはならない。

シ 電子署名・暗号化

（ア） 大学等構成員は、情報資産の分類により定めた取扱制限に従い、外部に送るデータの機密性又は完全性を確保することが必要な場合には、部門情報統括責任者が定める電子署名、暗号化等の方法を用いて、送信しなければならない。

（イ） 大学等構成員は、暗号化を行う場合に部門情報統括責任者が定める以外の方法を用いてはならない。また、部門情報統括責任者が定める方法で暗号のための鍵を管理しなければならない。

ス 利用可能なネットワークプロトコル

大学等構成員が利用できるネットワークプロトコルは、必要最低限のものとする。

セ 障害記録

情報基盤管理者及び業務システム管理者は、大学等構成員からのシステム障害の報告、システム障害に対する処理結果又は問題等及び、再発防止策を障害記録として体系的に記録し、適切に保存しなければならない。

(2) アクセス制御

ア 利用者の識別及び認証

情報基盤管理者及び業務システム管理者は、所管するネットワーク又は情報システムに権限がない大学等構成員がアクセスすることが不可能となるよう

に、利用者の識別及び認証等適切な対応を行わなければならない。

イ　利用者の点検

情報基盤管理者及び業務システム管理者は、アカウントに割り当てているアクセス権の正当性を確保するために、定められた方法に従って点検しなければならない。

ウ　ネットワークにおけるアクセス制御

情報基盤管理者及び業務システム管理者は、アクセス可能なネットワーク又はネットワーク上のサービス毎にアクセスできる者を定めなければならない。また、ネットワークサービスを利用する権限を有しない大学等構成員が当該サービスを利用できるようにしてはならない。

エ　強制的な接続制御及び経路制御

（ア）　情報基盤管理者及び業務システム管理者は、不正アクセスを防止するため、適切なネットワーク経路制御を施さなければならない。

（イ）　情報基盤管理者及び業務システム管理者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等に搭載されている通信ソフトウェア等を設定しなければならない。

オ　無人状態にある装置の管理

情報基盤管理者及び業務システム管理者は、サーバ又は情報機器が無人の状態になる場合、適切なセキュリティ対策を施さなければならない。

カ　外部からのアクセス

（ア）　外部からのアクセスの許可は、合理的理由を有する必要最低限のものに限定しなければならない。

（イ）　内部のネットワーク及び情報システムへのアクセス方法及び使用方法等は、通信途上の機密性及び利用者の真正性が確保できるものでなければならない。

（ウ）　外部からのアクセスに利用する物理資産を大学等構成員に貸与する場合、セキュリティ確保のために必要な措置を講じなければならない。

（エ）　大学等構成員は、外部から持ち帰った物理資産を内部ネットワークに接続する前に、コンピュータウイルスに感染していないこと等を確認しなければならない。

キ　内部ネットワーク間の接続

情報基盤管理者及び業務システム管理者は、他の内部ネットワークとの接続については、情報資産に影響が生じないことを確認し、それぞれの情報システムの責任範囲を明確にしたうえで、接続しなければならない。

なお、接続しようとする場合は、あらかじめ部門情報統括責任者と協議しなければならない。

ク　外部ネットワークとの接続

（ア）　情報基盤管理者及び業務システム管理者は、外部ネットワークとの接続にあたり当該外部ネットワークのネットワーク構成、情報機器構成、セキュリティ技術等を詳細に調査し、法人事務局又は大学の情報資産に影響が生じないことを確認したうえで、部門情報統括責任者の許可に基づき接続しなければならない。

（イ）　情報基盤管理者及び業務システム管理者は、接続に際して情報セキュリティの確保できるネットワーク構成を採らなければならない。情報基盤管理者及び業務システム管理者は、当該外部ネットワークの瑕疵により法人事務局又は大学のデータの漏えい、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対応するため、必要に応じて当該外部ネットワークの管理責任者による損害賠償責任を契約上担保するよう努めなければならない。

（ウ）　接続した外部ネットワークのセキュリティに問題が認められ、法人事務局又は大学の情報資産に脅威が生じるおそれがある場合には、情報基盤管理者及び業務システム管理者は当該外部ネットワークとの接続を物理的又は論理的に遮断することができるものとする。

ケ　ネットワーク機器の自動識別

情報基盤管理者及び業務システム管理者は、法人事務局又は大学で使用されるネットワーク機器について、情報機器固有情報等によって情報機器とネットワークとのアクセスの可否が自動的に識別されるように必要に応じてシステムを設定しなければならない。

コ　ログイン試行回数の制限等

情報基盤管理者及び業務システム管理者は、ログイン試行回数の制限及びアクセスタイムアウトの設定等により、正当なアクセス権を持たない者が利用できないようにシステムを設定するよう考慮しなければならない。

サ　主体認証情報の管理

（ア）　情報基盤管理者及び業務システム管理者は、大学等構成員を識別するためのクレデンシャルを設定した情報を厳重に管理しなければならない。

（イ）　情報基盤管理者及び業務システム管理者は、暫定主体認証も含めアカウントを発行する場合は他者が想像しにくいものとする。

(3)　システム開発、導入、保守等

ア　情報システムの調達

（ア）　情報基盤管理者及び業務システム管理者は、情報システムの調達にあたっては、一般に公開する調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

（イ） 情報基盤管理者及び業務システム管理者は、物理資産及びソフトウェアの調達にあたっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

（ウ） 部門情報統括責任者は、適切に情報セキュリティ対策を推進・管理するための基礎資料として、情報システム台帳を作成し、整理する。業務システム管理者は、情報システムを新たに調達したり、既にある情報システムを廃止したりしたときは、部門情報統括責任者からの求めに応じて、報告しなければならない。

イ　情報システムの開発等

（ア） 情報基盤管理者及び業務システム管理者は、ネットワーク及び情報システムの開発、導入、更新及び運用保守にあたっては、次の事項を定める。

① 責任者及び監督者
② 作業者及び作業範囲
③ 開発するシステムと運用中のシステムとの分離
④ 開発・保守に関する設計仕様などの成果物の提出
⑤ セキュリティ上問題となり得るおそれのあるハードウェア及びソフトウェアの使用禁止
⑥ アクセス制限
⑦ 物理資産の搬入出の際の許可及び確認
⑧ 記録の提出義務
⑨ 仕様書・マニュアル等の定められた場所への保管
⑩ 情報システムに係るソースコードの適切な方法での保管
⑪ 開発・保守を行った者の利用者アカウント等の当該開発・保守終了後に不要となった時点での速やかな抹消

（イ） 情報基盤管理者及び業務システム管理者は、ネットワーク及び情報システムの開発、導入、更新及び運用保守にあたって、不正にコピーしたソフトウェア及び個人所有のソフトウェアを導入又は使用等、問題のある行為が発生しないようにしなければならない。

（ウ） 情報基盤管理者及び業務システム管理者は、ネットワーク及び情報システムの開発、導入、更新及び運用保守にあたって、コンピュータウイルス等対策ソフトウェアを導入する等、ウイルス感染による情報漏えい等が発生しないようにしなければならない。

ウ　情報システムの移行

（ア） 情報基盤管理者及び業務システム管理者は、システム開発・保守計画の策定時に情報システムの移行手順を明確にしなければならない。また、移行の際、情報システムに記録されているデータの保存を確実に行い、移行に伴う

情報システムの停止等の影響が最小限になるよう配慮しなければならない。

（イ） 情報基盤管理者及び業務システム管理者は、新たに情報システムを導入する際には、既に稼働している情報システムに接続する前に、十分な試験を行わなければならない。また、既存のシステムを更新する際には、既に稼働している情報システムとの連携において、十分な試験を行わなければならない。

（ウ） 情報基盤管理者及び業務システム管理者は、擬似環境による動作確認後に情報システムの移行を行わなければならない。また、作業については、作業経過を確認しながら実施するとともに、作業内容を記録しなければならない。

（エ） 情報基盤管理者及び業務システム管理者は、原則として個人情報及び機密性の高い生データを、試験データに使用してはならない。ただし、合理的な理由がある場合で、部門情報統括責任者が許可したときは、この限りではない。

（オ） 情報基盤管理者及び業務システム管理者は、試験に使用したデータ及びその結果を５年間厳重に管理しなければならない。

エ 情報システムの入出力データ

（ア） 情報基盤管理者及び業務システム管理者は、情報システムに入力されるデータについて、範囲、妥当性のチェック機能及び不正な文字列等の入力を除去する機能を必要に応じて組み込むように情報システムを設計しなければならない。

（イ） 情報基盤管理者及び業務システム管理者は、内部処理において誤ったデータに書き換えられる等の可能性がある場合に、書き換え等を検出するチェック機能を組み込むように情報システムを設計しなければならない。

（ウ） 情報基盤管理者及び業務システム管理者は、情報システムから出力されるデータは、保存された情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。

オ ソフトウェアの保守及び更新

情報基盤管理者及び業務システム管理者は、ソフトウェア等を更新又は修正プログラムを導入する場合、不具合及び他のシステムとの相性の確認を行い、計画的に更新し又は導入しなければならない。

また、情報セキュリティに重大な影響を及ぼす不具合に対する修正プログラムについては、情報基盤管理者及び業務システム管理者は、速やかに対応を行わなければならない。

カ 作業の確認

契約により操作を認められた外部委託従事者が重要なシステム変更等の作業を行う場合は、２名以上で作業し、互いにその作業を確認しなければならない。

キ　作業管理記録

情報基盤管理者及び業務システム管理者は、担当するシステムにおいて行ったシステム変更等の作業については、作業記録を作成しなければならない。作成した作業記録は、窃取、改ざん等をされないように適切に管理を行わなければならない

(4)　コンピュータウイルス等不正プログラム対策

ア　情報基盤管理者の実施事項

情報基盤管理者は、次の事項を実施しなければならない。

（ア）　コンピュータウイルス等の情報について大学等構成員に対する注意喚起を行う。

（イ）　常時コンピュータウイルス等に関する情報収集に努める。

（ウ）　コンピュータウイルス等対策ソフトウェア及び定義ファイルは常に最新のものに保たせるよう指導等を行う。

イ　情報基盤管理者等の実施事項

情報基盤管理者、業務システム管理者及び情報管理者は、次の事項を実施しなければならない。

（ア）　所管するサーバ及び情報機器に、コンピュータウイルス等対策ソフトウェアを常駐させる。

（イ）　情報システムにおいて電磁的記録媒体を使用する場合、当該電磁的記録媒体の使用にあたりウイルスチェックを行う。

（ウ）　コンピュータウイルス等対策ソフトウェア及び定義ファイルは常に最新のものに保つ。

ウ　大学等構成員の遵守事項

大学等構成員は、次の事項を遵守しなければならない。

（ア）　情報機器において、コンピュータウイルス等対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更しない。

（イ）　外部ネットワーク及び電磁的記録媒体からデータ又はソフトウェアを取り入れる際には、必ずコンピュータウイルス等対策ソフトウェアによるチェックを行う。

（ウ）　外部ネットワーク及び電磁的記録媒体へデータ又はソフトウェアを送信・書き込みする際には、必ずコンピュータウイルス等対策ソフトウェアによるチェックを行う。

（エ）　差出人が不明な電子メール又は不自然なファイルが添付された電子メールを受信した場合は速やかに削除する。

（オ）　情報機器に対して、コンピュータウイルス等対策ソフトウェアによる完全スキャンを定期的に行い、スキャンの実行を途中で止めない。

（カ） 情報セキュリティ管理者が提供するコンピュータウイルス等の情報を常に確認する。

（キ） 添付ファイルのあるメールを送受信する場合は、コンピュータウイルス等対策ソフトウェアでチェックを行う。

（ク） コンピュータウイルス等に感染したおそれがある場合は、速やかに情報管理者へ報告すると共に、その指示に従い、ＬＡＮケーブルの即時取り外し、情報機器の通信機能の停止や電源遮断等、他への感染を防止する措置を講じる。

（ケ） ウイルス対策ソフトウェア等により不正プログラムとして検知される実行ファイルを実行しない。

（コ） 外部からデータやソフトウェアを物理資産に取り込む場合又は外部にデータやソフトウェアを提供する場合には、不正プログラム感染の予防に努める。

（サ） 常に最新のセキュリティ情報に注意し、不正プログラム感染の予防に努める。

（シ） 情報基盤管理者及び業務システム管理者等権限のある者より不正プログラム対策の指示があった場合には、それに従って当該情報システムに対して対策を実施する。

エ 専門家の支援体制

部門情報統括責任者は、実施しているコンピュータウイルス等対策では不十分な事態が発生した場合に備え、外部の専門家の支援を受けられるようにしておかなければならない。

(5) 不正アクセス対策

ア 使用されていないポートの閉鎖等

情報基盤管理者及び業務システム管理者は、不正なアクセスによる影響を防止するための必要な措置を講じなければならない。

（ア） 使用されていないポートを閉鎖する。

（イ） 不正アクセスに関する情報の収集に努め、当該情報について必要な措置を講ずるものとする。

（ウ） ソフトウェアにセキュリティホールが発見された場合は、速やかに修正プログラムを適用する。

イ 攻撃の対処

情報基盤管理者及び業務システム管理者は、所管するシステムへの攻撃の予告等サーバ等に不正アクセスを受けることが明白な場合には、システムの停止、他のネットワークとの切断などの必要な措置を講じなければならない。

また、各関係機関との連絡を密にして情報の収集に努めなければならない。

ウ　記録の保存

情報セキュリティ最高責任者及び部門情報統括責任者は、不正アクセス行為の禁止等に関する法律に違反等犯罪の可能性がある不正アクセスを受けた場合は、不正アクセスの記録の保存に努めるとともに、警察・関係機関との緊密な連携に努めなければならない。

エ　内部からの攻撃

情報基盤管理者及び業務システム管理者は、大学等構成員が使用している端末からの学内のサーバ等に対する不正アクセスや外部のサイトに対する不正アクセスを監視しなければならない。

オ　大学等構成員による不正アクセス時の措置

大学等構成員による不正アクセスがあった場合は、情報基盤管理者及び業務システム管理者は、当該大学等構成員が所属するグループの情報管理者に通知し、適切な措置を求めなければならない。

(6)　セキュリティ情報の収集

情報基盤管理者は、セキュリティホール等のセキュリティに関する情報を収集し、必要に応じ関係者間で情報を共有しなければならない。

9　運用面のセキュリティ

(1)　情報システムの監視

ア　事象の検知

情報基盤管理者及び業務システム管理者は、セキュリティに関する事象を検知するため、情報システムの監視を行わなければならない。

イ　時刻同期

情報基盤管理者及び業務システム管理者は、重要なアクセスログ等を取得するサーバの正確な時刻設定又はサーバ間の時刻同期ができる措置を施さなければならない。

ウ　常時監視

情報基盤管理者及び業務システム管理者は、外部と接続するシステムを稼働中、常時監視しなければならない。

(2)　情報セキュリティポリシー等の遵守状況の確認及び対処

情報基盤管理者、業務システム管理者及び情報管理者は、所管の範囲において情報セキュリティポリシー及びこれに基づく文書の遵守状況について常に確認を行い、問題を認めた場合には速やかに部門情報統括責任者に報告しなければならない。部門情報統括責任者は、発生した問題について、適切かつ速やかに対処しなければならない。

(3)　運用管理における留意点

ア　調査権限のある大学等構成員の指名

部門情報統括責任者は、情報漏えい、不正アクセス、コンピュータウイルス等の調査のために、情物理資産、アクセス記録及びメール等の情報を調査する権限を有する大学等構成員を指名する。

イ　セキュリティポリシー等の閲覧

情報基盤管理者、業務システム管理者及び情報管理者は、大学等構成員、人材派遣職員及び非常勤嘱託職員が常に情報セキュリティポリシー及びこれに基づく文書を参照できるよう配慮しなければならない。

ウ　管理者権限

情報基盤管理者、業務システム管理者及び情報管理者の権限を代行する者は、それぞれが指名する。

エ　大学等構成員の報告義務

（ア）　大学等構成員は、情報セキュリティポリシーに対する違反行為を発見した場合、直ちに情報基盤管理者及び情報管理者に報告を行わなければならない。

（イ）　違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると部門情報統括責任者が判断した場合は、緊急時対応計画に従って適切に対処しなければならない。

(4)　緊急時の対応

ア　緊急時対応計画の策定

部門情報統括責任者及び業務システム管理者は、情報資産への重大な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において、連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適切に実施するために、緊急時対応計画を策定しなければならない。

イ　緊急時対応計画に盛り込むべき内容

緊急時対応計画には、次の内容を定めなければならない。

（ア）　関係者の連絡先

（イ）　意思決定の所在

（ウ）　発生した事象に係る報告すべき事項

（エ）　発生した事象への対応措置

（オ）　再発防止措置の策定

ウ　緊急時対応計画の見直し

部門情報統括責任者及び業務システム管理者は、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて緊急時対応計画を見直さなければならない。

(5)　例外措置

ア　例外措置の許可

情報基盤管理者、業務システム管理者及び情報管理者は、情報セキュリティポ

リシーを遵守することが困難な状況で、大学等の事務の適正な遂行を継続するため、遵守事項とは異なる方法を採用し、又は遵守事項を実施しないことについて合理的な理由がある場合には、情報セキュリティ最高責任者の許可を得て、例外措置を取ることができる。

イ　緊急時の例外措置

情報基盤管理者、業務システム管理者及び情報管理者は、前項に該当する場合であって、大学等の事務の遂行に緊急を要し、情報セキュリティ最高責任者の許可を得る時間的な猶予のないときは、例外措置を実施し、実施後速やかに部門情報統括責任者に報告しなければならない。

ウ　例外措置の申請書等の管理

情報セキュリティ最高責任者は、例外措置の申請書、報告書及び審査結果を適切に保管しなければならない。

１０　情報セキュリティ個別基準の策定

部門情報統括責任者は、情報セキュリティポリシーを補完するために必要な事項に関して、具体的な内容を定めた情報セキュリティ個別基準を策定する。

１１　情報セキュリティ実施手順の策定

部門情報統括責任者及び業務システム管理者は、情報セキュリティポリシーに基づき、所管するシステム等に対する情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定する。

１２　情報セキュリティに関する違反に対する対応

(1)　懲戒処分

情報セキュリティポリシー及びこれに基づく文書に違反した大学等構成員及びその監督責任者は、その重大性、発生した事象の状況等に応じて、神戸市公立大学法人職員就業規則等による懲戒処分の対象となる。

(2)　再発防止の指導等

大学等構成員に情報セキュリティポリシー及びこれに基づく文書に違反する行為がみられた場合には、情報基盤管理者、業務システム管理者及び情報管理者は、速やかに次の措置を講じなければならない。

ア　当該大学等構成員に対して速やかに調査を行い、事実を確認する。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。

イ　当該大学等構成員に対して違反する行為の事実を通知し、再発防止の指導その他適切な措置を行う。

ウ　指導等によっても改善されない場合、当該大学等構成員の情報資産の使用権を停止あるいは剥奪する。

エ　違反する行為が生じた場合、違反する行為の内容、指導内容その他措置の状況について情報セキュリティ最高責任者に報告する。

１３　評価・改善・見直し

(1)　監査

ア　実施方法

情報セキュリティ最高責任者は、情報監査統括責任者に命じ、情報セキュリティ対策状況について、定期的及び必要に応じて監査を行わせなければならない。

イ　監査を行う者の要件

（ア）　情報監査統括責任者は、監査を実施する場合には、被監査部門から独立した者に対して監査の実施を依頼しなければならない。

（イ）　監査を行う者は、監査及び情報セキュリティに関する専門知識を有するものでなければならない。

ウ　監査実施計画の策定及び実施への協力

（ア）　情報監査統括責任者は、監査を行うに当たって監査実施計画を策定し、情報管理委員会に報告しなければならない。

（イ）　被監査部門は、監査の実施に協力しなければならない。

エ　外部委託業者に対する監査

情報監査統括責任者は、外部委託業者に対して外部委託業者からの再委託の事業者も含めて、情報セキュリティポリシーの遵守について監査を定期的及び必要に応じて行わなければならない。

オ　監査結果の報告

情報監査統括責任者は、監査結果を取りまとめ、情報管理委員会に報告する。

カ　監査調書等の保管

情報監査統括責任者は、監査の実施を通して収集した監査証拠及び監査報告書の作成のための監査調書を、紛失等が発生しないように適切に保管しなければならない。

キ　指摘事項への対処

部門情報統括責任者は、監査結果を踏まえ、指摘事項に関係する情報管理者等に対し、当該事項への対処を指示しなければならない。また、指摘事項に関係しない情報管理者等に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。

ク　監査結果の活用

情報セキュリティ最高責任者は、情報セキュリティポリシー等情報セキュリティ対策の見直し時に監査結果を活用しなければならない。

(2)　自己点検

ア　実施方法

（ア）　情報基盤管理者及び業務システム管理者は、所管するネットワーク及び情報システムの情報セキュリティ対策状況について、定期的及び必要に応じて

自己点検を実施しなければならない。

（イ） 情報管理者は、所管する所属の情報セキュリティ対策状況について、定期的及び必要に応じて自己点検を行なわなければならない。

イ 自己点検結果等の報告

（ア） 情報基盤管理者、業務システム管理者及び情報管理者は、自己点検結果と自己点検結果に基づく改善策を取りまとめ、部門情報統括責任者に報告しなければならない。

（イ） 部門情報統括責任者は、報告を受けた点検結果及び改善策を情報管理委員会に報告しなければならない。

ウ 自己点検結果の活用

（ア） 大学等構成員は、自己点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。

（イ） 情報セキュリティ最高責任者は、情報セキュリティポリシー等情報セキュリティ対策の見直し時に点検結果を活用しなければならない。

(3) 改善

ア 是正措置

情報基盤管理者、業務システム管理者及び情報管理者は、業務上発見された問題、外部からの指摘による問題、監査及び自己点検において指摘された問題等に対する再発防止のため、その原因を除去するための措置を施さなければならない。

イ 予防措置

情報基盤管理者、業務システム管理者及び情報管理者は、業務上予見される問題、他の組織で発生したものと同種の情報セキュリティインシデント、監査及び自己点検において指摘されうる問題等の発生を未然に防止するため、その原因を除去するための措置を施さなければならない。

(4) 情報セキュリティポリシーの見直し

情報セキュリティ最高責任者は、監査及び自己点検の結果、改善の状況、残留リスク、情報セキュリティに関する状況の変化等を踏まえ、情報セキュリティポリシーに対して必要があると認めた場合は、その見直しを行う。

第２節　高等専門学校

１　目的

本節セキュリティ対策基準とは、神戸市立公立大学法人セキュリティ基本方針に基づき、高等専門学校の情報セキュリティ対策等を実施するために適用範囲における具体的な遵守事項及び判断基準を定めたものである。

２　適用範囲

高等専門学校における情報資産及び情報資産に接する、学生及び教職員など高等

専門学校において情報資産を取り扱うすべての者（以下「高等専門学校構成員」という。）とする。

3　情報セキュリティ管理体制

高等専門学校の情報資産について、適切に情報セキュリティ対策を推進・管理するための体制を確立するものとする。

そのため次に掲げるものを置く。

(1)　情報セキュリティ最高責任者

法人事務局長を情報セキュリティ最高責任者とする。

(2)　部門情報統括責任者

校長を部門情報統括責任者とする。

(3)　情報基盤管理者

総合情報センター長を情報基盤管理者とする。

(4)　情報管理者

教務主事、学生主事、事務室長、各学科の学科長及び学校長の指名する者を情報管理者とする。

(5)　業務システム管理者

各業務システムを所管するグループの長を当該業務システムに関する業務システム管理者とする。

(6)　情報監査統括責任者

校長の指名する主事及び事務室長を情報監査統括責任者とする。

(7)　高専情報セキュリティ委員会

次に掲げる事項を審議し、その内容を情報管理委員会を経て情報セキュリティ最高責任者に報告する。組織等については、別途定める。

①　高等専門学校の情報セキュリティに関する重要事項の審議・決定

②　情報セキュリティポリシー遵守状況の把握と必要な措置の検討

③　前２号に掲げるもののほか、高等専門学校における情報セキュリティの確保に資する事項

4　権限と責任

情報セキュリティ基本方針で定めた情報セキュリティ管理体制における権限と責任については次のとおりとする。

(1)　情報セキュリティ最高責任者

ア　情報セキュリティ最高責任者は、法人における全てのネットワーク、情報システム、データ等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。

イ　情報セキュリティ最高責任者は、必要に応じ、情報セキュリティに関する専門的な知識及び経験を有する専門家をアドバイザーとして置くことができる。

(2)　部門情報統括責任者

ア　部門情報統括責任者は、情報セキュリティ最高責任者を補佐しなければならない。

イ　部門情報統括責任者は、管轄する部門全てのネットワーク、情報システム、データ等の情報資産における開発、設定の変更、運用、見直し等を行う統括的な権限及び責任を有する。

ウ　部門情報統括責任者は、管轄する全ての情報資産における情報セキュリティ対策に関する統括的な権限及び責任を有する。

エ　部門情報統括責任者は、情報基盤管理者、情報管理者及び業務システム管理者に対して、情報セキュリティに関する指導及び助言を行う権限を有する。

オ　部門情報統括責任者は、所管する部門の情報資産に対するインシデントが発生した場合又は発生のおそれがある場合に、情報セキュリティ最高責任者の指示に従い、情報セキュリティ最高責任者が不在の場合には自らの判断に基づき、必要かつ十分な措置を行う権限及び責任を有する。

カ　部門情報統括責任者は、緊急時等の円滑な情報提供を図るため、情報セキュリティ最高責任者、部門情報統括責任者、情報基盤管理者、情報管理者及び業務システム管理者を網羅する連絡体制を整備しなければならない。

(3)　情報基盤管理者

ア　情報基盤管理者は部門情報統括責任者を補佐し、その実務を担当する。

イ　情報基盤管理者は、高等専門学校のネットワーク、情報システム、データ等の情報資産における開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

ウ　情報基盤管理者は、高等専門学校のネットワーク、情報システム、データ等の情報資産の情報セキュリティ対策に関する権限及び責任を有する。

エ　情報基盤管理者は、高等専門学校のネットワーク、情報システム、データ等の情報資産に関する情報セキュリティ実施手順を策定し、その維持・管理を行う。

オ　情報基盤管理者は、高等専門学校の情報資産に対するインシデントが発生した場合又は発生のおそれがある場合に、部門情報統括責任者及び情報セキュリティ最高責任者へ速やかに報告を行い、指示を仰がなければならない。

カ　情報基盤管理者は、高等専門学校のネットワーク、情報システム、データ等の情報資産のうち情報機器についての物理的セキュリティに関する管理を情報管理者に行わせることができる。

(4)　情報管理者

ア　情報管理者は、高等専門学校の校内（以下「学校内」という。）におけるデータ等の情報資産の情報セキュリティ対策に関する権限及び責任を有する。

イ　情報管理者は、情報基盤管理者の指示に従い高等専門学校のネットワーク、情

報システム、データ等の情報資産のうち高等専門学校の情報機器についての物理的セキュリティに関する管理を行う。

ウ　情報管理者は、高等専門学校の情報資産に対するインシデントが発生した場合又は発生のおそれがある場合には、情報基盤管理者、業務システム管理者へ速やかに報告を行い、指示を仰がなければならない。

(5)　業務システム管理者

ア　業務システム管理者は、当該業務システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

イ　業務システム管理者は、当該業務システムの情報セキュリティ対策に関する権限及び責任を有する。

ウ　業務システム管理者は、当該業務システムに関する情報セキュリティ実施手順を策定し、その維持・管理を行う。

エ　業務システム管理者は、当該業務システムにおいて情報資産に対するインシデントが発生した場合又は発生のおそれがある場合には、情報基盤管理者へ速やかに報告を行い、指示を仰がなければならない。

オ　業務システム管理者は、当該業務システムにおける開発、設定の変更、運用等についての作業を業務システム管理者が指名する者に行わせることができる。

(6)　情報監査統括責任者

情報監査統括責任者は、情報セキュリティ監査の計画、実施、報告等を行う権限及び責任を有する。

(7)　兼務の禁止

ア　情報セキュリティ対策の実施において、やむを得ない場合を除き、承認又は許可の申請を行う者とその承認者又は許可者は、同じ者が兼務してはならない。

イ　監査を受ける者とその監査を実施する者は、同じ者が兼務してはならない。

5　情報資産の分類と管理

(1)　情報資産の管理責任

ア　管理責任

情報資産は、情報基盤管理者、業務システム管理者及び情報管理者等権限のある者(以下「情報資産管理責任者」という)がそれぞれ所管する情報資産についての管理責任を有する。また、情報資産管理責任者は、当該情報資産の利用範囲を定めなければならない。

イ　高等専門学校構成員の責任

高等専門学校構成員は、情報資産の作成・入手・利用等に際しては、十分にその責任を自覚したうえで行わなければならない。

ウ　複製等の管理

データが複製又は送信された場合には、当該複製等も原本と同様に管理しなけ

ればならない。

(2)　情報資産の分類と管理方法

ア　情報資産の分類

（ア）　対象となる情報資産は、各々の情報資産の機密性、完全性及び可用性を踏まえ、次の重要性分類に従って分類する。

機密性

3	高等専門学校で取り扱う情報資産のうち、特に機密性を要するもの ・個人情報に関するもの ・法令の規定により秘密を守る義務を課されているもの ・部外に知られることが適当でない法人その他団体に関するもの ・部外に漏れた場合に法人事務局及び高等専門学校の信頼を著しく害するおそれのあるもの ・公開することでセキュリティ侵害が生じるおそれがあるもの
2	直ちに一般に公表することを前提としていないもの （機密性３には当てはまらないが、広報などは行っていないもの）
1	機密性２又は機密性３の情報資産以外のもの

完全性

3	高等専門学校で取り扱う情報資産のうち、特に完全性を要するもの （改ざんあるいは誤りがあると学生等の権利が侵害される、又は法人事務局及び高等専門学校運営の適確な遂行に支障を及ぼす可能性があるもの） ・個人情報に関するもの ・法令の規定により秘密を守る義務を課されているもの ・部外に知られることが適当でない法人その他団体に関するもの ・部外に漏れた場合に法人事務局及び高等専門学校の信頼を著しく害するおそれのあるもの
2	改ざんあるいは誤りがあると組織に軽微な影響が発生する可能性があるもの
1	完全性２又は完全性３の情報資産以外のもの

可用性

3	高等専門学校で取り扱う情報資産のうち、特に可用性を要するもの （利用できないと学生等の権利が侵害される、又は法人事務局及び高等専門学校事務の安定的な遂行に支障を及ぼす可能性があるもの） ・滅失し又は損傷した場合その復元が著しく困難であるため法人事務局及び高等専門学校の円滑な運営が妨げられるおそれのあるもの
2	利用できないことが一定時間以上継続すると学生等の権利が侵害される、

	又は法人事務局及び高等専門学校の事務の安定的な遂行に支障を及ぼす可能性があるもの
1	可用性２又は可用性３の情報資産以外のもの

（イ） 情報資産の機密性、完全性、可用性のいずれかの重要性分類２以上に分類される情報資産をこの対策基準の対象とする。

また、重要性分類１の情報資産も、必要なものはできる限りこの対策基準に準じた対応を講じるものとする。

イ　情報資産に関するリスク分析の実施

（ア） 高等専門学校が保有する情報資産に対して、あらかじめ定められた方法に従い、リスク分析を行わなければならない。

（イ） 情報セキュリティ最高責任者は、リスクを受容するための基準を作成し、受容可能なリスクの水準を定めなければならない。

（ウ） リスク分析の結果、リスクの大きさが受容可能なリスクの水準を上回る場合、リスク対応計画書を作成し、情報セキュリティ最高責任者の承認を得たうえで、適切なリスク管理を行わなければならない。リスク対応計画書には、リスク対応を施すための活動内容、資源、責任体制及び優先順位等を記載すること。

（エ） リスク分析及び受容可能なリスクの水準等は、情報セキュリティに関する状況の変化等を踏まえ、定期的に見直しを行うものとする。

ウ　情報資産の管理方法

（ア） 情報資産の管理

① 情報資産について、第三者が重要性の識別を容易に認識できないよう適切な管理を行わなければならない。

② すべての情報資産を明確に識別し、重要な情報資産に対しては必要に応じて目録を作成して管理しなければならない。

（イ） データの作成

① 次のデータを作成してはならない。

a 差別、名誉毀損、侮辱、ハラスメントにあたる情報

b 個人情報やプライバシーを侵害する情報

c 守秘義務に違反する情報

d 著作権等の財産権を侵害する情報

e 業務に必要のない情報

f 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

② データの作成時に重要性分類に基づき、当該データの分類を定めなけ

ればならない。

③　作成途上のデータについても、紛失や流出等を防止しなければならない。また、データの作成途上で不要になった場合は、当該データを消去しなければならない。

（ウ）　情報資産の入手

①　学校内の者が作成した情報資産を入手した者は、入手元の情報資産の分類に基づいた取扱いをしなければならない。

②　高等専門学校構成員以外の者が作成した情報資産を入手した者は、重要性分類に基づき、当該情報の分類を定めなければならない。

③　情報資産を入手した者は、入手した情報資産の分類が不明な場合、情報資産管理責任者に判断を仰がなければならない。

（エ）　情報資産の利用

①　情報資産を利用する者は、情報資産を業務上の目的以外に利用してはならない。

②　情報資産の利用においては、情報資産の分類に応じ、利用者及びアクセス権限を定めなければならない。

③　機密性３のデータは、情報資産管理責任者の許可を得た場合、複写、複製、送付又は送信を行うことができる。ただし、暗号化等による情報漏えい対策を施さなければならない。

④　電子メールにより機密性２のデータを送信する者は、必要に応じ暗号化等による情報漏えい対策を施さなければならない。

⑤　情報資産を利用する者は、物理資産に情報資産の分類が異なるデータが複数記録されている場合、最高度の分類に従って、当該物理資産を取り扱わなければならない。

（オ）　情報資産の保管・運搬

①　情報資産管理責任者は、情報資産の重要性分類に従って、情報資産の保管を適切に行わなければならない。

②　最終的に確定したデータを記録した物理資産は、書込禁止措置を行ったうえで保管しなければならない。

③　情報資産管理責任者は、持ち運び可能な物理資産を耐火、耐熱、耐水及び耐湿対策を講じたうえ施錠可能な場所への保管等適切な管理を行わなければならない。

④　情報資産管理責任者は、情報システムのバックアップで取得したデータを記録する物理資産を長期保管する場合は、自然災害を被る可能性が低い地域への保管を考慮しなければならない。

⑤　機密性２以上の情報資産が保管された物理資産の搬送にあたっては、

必要に応じ鍵付きのケース等に格納し、暗号化の設定を行う等、情報資産の不正利用を防止するための措置を施さなければならない。

⑥　機密性２以上の情報資産が保管された物理資産を運搬する者は、情報資産管理責任者に許可を得なければならない。

（カ）　情報資産の提供・公開

①　機密性３の情報資産を外部に提供する場合は、次の措置を行わなければならない。

a　事前に情報管理者の許可を得る。

b　提出日時・提出者及び提供概要を記録する。

c　必要に応じ暗号化の設定を行う。

②　情報資産管理責任者は、公開する情報資産について、完全性を確保しなければならない。

（キ）　情報資産の廃棄

①　情報資産の廃棄を行う場合、次の措置を行わなければならない。

a　事前に情報基盤管理者の許可を得る。

b　廃棄処理の日時、担当者及び処理内容を記録する。

②　電磁的記録媒体が不要となった場合は、当該媒体に含まれるデータの消去を行ったうえで裁断、溶解等により物理的に破壊し、復元不可能な状態にして廃棄しなければならない。紙媒体が不要となった場合は、焼却、裁断又は溶解等により廃棄しなければならない。

エ　文書の管理

（ア）　情報セキュリティ対策基準を実施していくうえで必要とされる文書は、神戸市立公立大学法人文書管理規程（2007年４月規程第96号）等の定めに従い管理しなければならない。

（イ）　情報セキュリティに係る文書（以下「文書」という）を作成又は更新する場合は、あらかじめ定められた者による承認を受けなければならない。

（ウ）　文書は、定期的に見直しを行い、必要に応じて更新しなければならない。

（エ）　文書を廃棄する場合は、廃棄文書が誤って使用されないようにしなければならない。ただし、廃棄文書を保持する必要がある場合には、廃棄文書と分かるように適切な識別を施さなければならない。

オ　記録の管理

情報セキュリティ対策基準の効果的運用の証拠を示すために、記録を作成し、適切な管理をしなければならない。

(3)　情報セキュリティに関する統一的な窓口の設置（ＣＳＩＲＴ）

ア　ＣＳＩＲＴ の設置

情報セキュリティ最高責任者は、情報セキュリティに関する事件・事故、シス

テム上の欠陥及び誤動作（以下、「情報セキュリティに関する事件・事故等」という。）に対処する組織としてＣＳＩＲＴを設置し、総合情報センターが、その役割を担う。

イ　ＣＳＩＲＴの役割

ＣＳＩＲＴは、情報セキュリティに関する事件・事故等に対処し、被害拡大防止、復旧、再発防止等に向けた対応を、迅速かつ的確に実施する。

ウ　ＣＳＩＲＴの連絡体制

ＣＳＩＲＴの統一窓口は、情報管理者とする。情報管理者は、情報セキュリティに関する事件・事故等が発生したときは、その内容に応じて、業務システム管理者等と適宜連絡し、国や県等の関係機関との情報共有を行う。

6　物理的セキュリティ

(1)　サーバ等の管理

ア　入退室の管理

情報資産管理責任者は、重要性分類３のデータを取扱う執務区域については、許可された者以外の立入を制限するなどの適正な入退室管理を行わなければならない。なお、ネットワークの基幹機器及び重要な情報システムを設置し、当該機器の管理及び運用を行う部屋（以下「管理区域」という）については、さらに次の事項に従い厳重な管理を行わなければならない。

（ア）　外部からの侵入が容易にできないようにしなければならない。

（イ）　施設管理部門と連携して、管理区域から外部に通ずるドアは必要最小限とし、鍵、監視機能、警報装置等によって許可されていない者の立ち入りを防止しなければならない。

（ウ）　管理区域への入退室は、許可された者のみに制限し、IDカード等による認証及び入退室管理簿の記載による入退室管理を行わなければならない。

（エ）　高等専門学校構成員は、管理区域に入室する場合、身分証明素等を携帯し、求めにより提示しなければならない。

（オ）　外部からの訪問者が管理区域に入室する場合には、必要に応じて立ち入り区域を制限したうえで、管理区域への入退室を許可された教職員が付き添うものとし、外見上教職員と区別できる措置を施さなければならない。

（カ）　管理区域については、当該システムに関連しない情報機器等を持ち込ませないようにしなければならない。

イ　装置の取付け等

（ア）　情報基盤管理者及び業務システム管理者は、ネットワーク機器及び情報システム機器の取付けを行う場合、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適切な固定を行う等必要な措置を施さなければならない。

（イ） 情報基盤管理者及び業務システム管理者は、システムの停止により、高等専門学校業務の遂行等に重大な影響を及ぼすおそれがあるものについて二重化等を行い、同一データを保持し、システムの運用が停止しないように努めなければならない。

（ウ） 権限のある者以外の者が容易に操作できないように、情報基盤管理者及び業務システム管理者は、利用者のクレデンシャルを設定する等の措置を施さなければならない。

ウ　電源

（ア） 情報基盤管理者及び業務システム管理者は、サーバ等の機器の電源については、当該機器を適切に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。

（イ） 情報基盤管理者及び業務システム管理者は、落雷等による過電流に対してサーバ等の機器を保護するための措置を施さなければならない。

エ　配線

（ア） 配線の変更、追加については、情報基盤管理者及び業務システム管理者等限られた者の権限とする。

（イ） 情報基盤管理者及び業務システム管理者は、施設管理部門と連携し、通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用する等必要な措置を施さなければならない。

（ウ） 情報基盤管理者及び業務システム管理者は、主要な箇所の通信ケーブル及び電源ケーブルについて、施設管理部門から損傷等の報告があった場合、連携して対応しなければならない。

（エ） 情報基盤管理者及び業務システム管理者は、ネットワーク接続口（ハブのポート等）を他者が容易に接続できない場所に設置する等適切に管理しなければならない。

オ　機器等の定期保守及び修理

（ア） 情報基盤管理者及び業務システム管理者は、可用性３のサーバ等の機器は、定期保守を実施しなければならない。

（イ） 情報基盤管理者、業務システム管理者及び情報管理者は、記憶装置を内蔵する機器を外部の業者に修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合、外部の業者に故障を修理させるにあたり、修理を委託する事業者との間で、守秘義務契約を締結するほか、秘密保持体制の確認等を行わなければならない。

カ　消火薬剤及び消防設備

消火薬剤及び消防用設備等は、機器及び電子記録媒体に影響を与えるものであってはならない。

キ　敷地外への機器の設置

情報基盤管理者及び業務システム管理者は、高等専門学校の敷地外にサーバ等の機器を設置する場合、部門情報統括責任者の許可を得なければならない。また、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

ク　物理資産の廃棄等

情報基盤管理者、業務システム管理者及び情報管理者は、物理資産を廃棄、リース返却等をする場合、物理資産内部の記憶装置から、すべてのデータを消去の上、復元不可能な状態にする措置を施さなければならない。

ケ　物理資産等の搬入出

（ア）　情報基盤管理者及び業務システム管理者は、物理資産等を搬入する場合、あらかじめ当該機器等の既存情報システムに与える影響について、教職員に確認を行わせなければならない。

（イ）　物理資産等の搬入出には教職員が同行する等の必要な措置を施さなければならない。

(2)　ネットワークの管理

ア　情報基盤管理者及び業務システム管理者は、学校内の通信回線及び通信回線装置を施設管理部門と連携し、適切に管理しなければならない。また、通信回線及び通信回線装置に関する文書を適切に保管しなければならない。

イ　情報基盤管理者及び業務システム管理者は、通信回線による外部ネットワークへの接続は必要最低限のものに限定し、できる限り接続ポイントを減らさなければならない。

ウ　部門情報統括責任者は、所管する情報システムにおいて機密性３の情報資産を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適切な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。

エ　ネットワークに使用する回線は送信途上においてデータの破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策が実施されたものでなければならない。

(3)　情報機器の管理

ア　情報基盤管理者、業務システム管理者及び情報管理者は、学校内の端末等について、必要に応じてワイヤーによる固定等盗難防止のための措置を講じなければならない。

イ　情報基盤管理者及び業務システム管理者は、情報システムにアクセスする場合いは、利用者を識別するためのクレデンシャルの入力による認証を必要とするように設定しなければならない。また、必要に応じてＢＩＯＳ認証、ハードディス

ク認証を併用しなければならない。

ウ　情報基盤管理者及び業務システム管理者は、取り扱う情報の重要度に応じて、パスワード以外にＩＤカード、生体認証等を導入し、二要素認証を行うものとする。

エ　情報基盤管理者及び業務システム管理者は、端末の暗号化等の機能を有効に利用しなければならない。また、電子記録媒体等についても、取り扱う情報の重要度に応じて、データ暗号化機能を備える媒体を使用しなければならない。

オ　モバイル端末を学校外で業務利用する場合は、端末の紛失・盗難対策として、普段からパスワードによる端末ロックを設定しておかなければならない。また、紛失・盗難に遭った際の対応として、遠隔消去（リモートワイプ）や自己消去機能などを活用できるときは、それらの機能を活用し、モバイル端末内のデータを消去しなければならない。

7　人的セキュリティ

(1)　高等専門学校構成員の責務

ア　情報セキュリティポリシー等の遵守義務

高等専門学校構成員は、情報セキュリティポリシー及びこれに基づく文書に定められている事項を遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点がある場合には、情報管理者等権限のある者に相談し、指示を仰がなければならない。

イ　法令等の遵守義務

高等専門学校構成員は、職務の遂行において使用する情報資産を保護するために、法令等を遵守しこれに従わなければならない。

- 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）
- 著作権法（昭和45年法律第48号）
- 個人情報の保護に関する法律（平成15年法律第57号）
- サイバーセキュリティ基本法（平成26年法律第104号）
- 神戸市個人情報保護法の施行に関する条例（令和４年12月条例第17号）
- 神戸市公立大学法人職員就業規則（2023年４月規則第28号）
- 神戸市公立大学法人再雇用職員就業規則（2023年４月規則第29号）
- 神戸市公立大学法人契約職員就業規則（2023年４月規則第30号）
- 神戸市公立大学法人パート職員就業規則（2023年４月規則第31号）
- 神戸市公立大学法人留学生担当嘱託講師就業規則（2023年４月規則第32号）
- 神戸市公立大学法人非常勤講師就業規則（2023年４月規則第33号）
- 神戸市公立大学法人特任教員就業規則（2023年４月規則第34号）
- 神戸市公立大学法人文書管理規程

ウ　指示に基づいた情報資産の利用等

高等専門学校構成員は、情報管理者等権限のある者の指示に従い、物理資産を利用するとともに、開発、設定の変更、運用、更新等の作業を行う。

エ　情報資産利用上の注意事項

高等専門学校構成員は、様々な情報の作成、利用、保存等のため情報機器の利用に際して、以下の事項を遵守しなければならない。

（ア）　高等専門学校の管理するネットワークに新規かつ固定的に物理資産を接続する場合、又は新たに物理資産を使用する場合は、事前に情報基盤管理者及び業務システム管理者の許可を得なければならない。

物理資産の持込みについては、別途定める手順に従うものとする。

（イ）　物理資産のソフトウェアに関するセキュリティ機能の設定を情報基盤管理者又は業務システム管理者の許可なく変更してはならない。

（ウ）　物理資産は脆弱性を持たないよう可能な限り最新の状態でなければならない。

（エ）　許可を受けた物理資産の利用を取りやめる場合には、物理資産内にデータが残留した状態とならないよう、すべてのデータを復元できないよう措置を施し、情報基盤管理者又は業務システム管理者に届け出なければならない。

（オ）　物理資産やデータ資産について、第三者に使用されないこと、また、情報管理者等管理権限のある者の許可なく情報を閲覧されることがないように、離席時の端末のロックやデータ資産を容易に閲覧されない場所への保管等適切な措置を講じなければならない。

（カ）　物理資産の紛失及び盗難を発生させないように注意しなければならない。

（キ）　学外のインターネットカフェなどに設置されているような不特定多数の人が操作（利用）可能な情報機器を用いての情報システムへのアクセスを行ってはならない。

オ　情報資産の学外利用

教職員は、情報資産の学外の利用にあたっては、以下の手順を遵守しなければならない。

①　情報資産で機密性、完全性、可用性分類２以上の情報を取り扱う場合、暗号化等による情報漏えい対策や作業中ののぞき見防止等を行わなければならない。

②　情報資産は可能な限り強固な認証システムを備え、ログ機能を持っており、それらの機能が設定され動作していなければならない。

またコンピュータウイルス等対策ソフトウェア及び定義ファイルは常に最新のものに保ち、システムを保護可能でなければならない。

③　情報資産の画面を他者から見える状態で利用してはならない。また当該

システムを他者が支配操作可能な状態にしてはならない。（不正操作、情報漏洩及び盗難防止）

④　情報資産を高等専門学校の情報システムに再接続する場合、接続に先だってコンピュータウイルス等対策ソフトウェアでチェックをしなければならない。

カ　学校外の情報システムからの利用

教職員は、学校外の情報システムから高等専門学校の管理するネットワークへ接続する場合、以下の手順を遵守しなければならない。

①　学校外の情報システムを用いて、公開のウェブ以外の高等専門学校の管理するネットワークの接続にあたって、事前に情報基盤管理者の許可を得なければならない。

②　本条の目的に利用する学校外の情報システムは可能な限り強固な認証システムを備え、ログ機能を持っており、それらの機能が設定され動作していなければならない。

またコンピュータウイルス等対策ソフトウェア及び定義ファイルは常に最新のものに保ち、システムを保護可能でなければならない。

③　これらの情報システムを許可された者以外に利用させてはならない。また当該システムを他者が支配操作可能な状態にしてはならない。（不正操作、情報漏洩及び盗難防止）

④　部門情報統括責任者の許可なく、これらの情報システムに機密性、完全性、可用性分類２以上の情報を複製保持してはならない。

⑤　これらの情報システムで動作するソフトウェアは正規のライセンスを受けたものでなければならない。

キ　情報資産の学校外への持ち出し

高等専門学校構成員は、情報管理者等管理権限のある者の許可を得た場合に限り、その指示に従って、 学校外へ情報資産を持ち出すことができる。

ク　業務目的外の利用禁止

教職員は、業務目的外でのパーソナルコンピュータ等の利用、情報システムへのアクセス、電子メールの利用及びインターネットへのアクセス等を行ってはならない。

ケ　端末等の利用

（ア）　教職員は、端末のソフトウェアに関するセキュリティ機能の設定を情報基盤管理者及び業務システム管理者の許可なく変更してはならない。

（イ）　教職員は、端末や電子記録媒体、データが印刷された文書等について、第三者に使用されること、又は情報管理者等管理権限のある者の許可なく情報を閲覧されることがないように、離席時の端末のロックや電子記録媒体、文

書等の容易に閲覧されない場所への保管等、適切な措置を講じなければならない。

コ　学校外における情報処理作業の制限

（ア）　部門情報統括責任者は、機密性２以上、可用性３、完全性３の情報資産を学校外で処理する場合における安全管理措置を定めなければならない。

（イ）　教職員は、学校外で情報処理作業を行う場合には、情報管理者等管理権限のある者の許可を得なければならない。また、その際、部門情報統括責任者の定める事項を遵守しなければならない。

サ　異動、退職時等の遵守事項

高等専門学校構成員は、異動、退職等により高等専門学校を離れる場合には、利用していた情報資産を返却しなければならない。また、その後も業務上知り得た情報を漏らしてはならない。

シ　人材派遣職員等

人材派遣職員及び非常勤嘱託職員が情報資産を取り扱う必要が生じた場合は、情報管理者等管理権限のある者は従事させる事務の範囲を指定する。また、人材派遣職員及び非常勤嘱託職員は「７．人的セキュリティ　(1) 高等専門学校構成員の責務」のア～サに定める事項を遵守しなければならない。

ス　学生等

学生等が高等専門学校の情報機器及びネットワークを利用する場合、教職員は情報セキュリティに関連する規定の趣旨に則り、教育的配慮の下、学生等を指導するものとする。授業以外の利用に関しては、総合情報センターの利用講習会を受講し、部門情報統括責任者の利用許可を得た後に、教職員の指導の下で利用するものとする。ただし、利用講習会は総合情報センター長の指定する授業科目の受講で代えることができる。

セ　臨時的利用者

学校外からの訪問者等が臨時的に高等専門学校の情報機器及びネットワークを利用する場合、教職員は部門情報統括責任者の許可を得たうえで、利用者に対し、情報セキュリティに関連する規定の趣旨に則り安全に利用できるよう指示する。

(2)　研修・訓練

ア　教職員に対する研修・訓練の実施

情報セキュリティ最高責任者は、定期的に教職員等情報取扱者に対する情報セキュリティに関する研修・訓練を実施させなければならない。

イ　研修計画の策定及び実施

（ア）　部門情報統括責任者は、教職員等情報取扱者に対する情報セキュリティに関する研修計画を定期的に策定し、情報管理委員会に報告しなければならな

い。

（イ） 教職員等情報取扱者を対象とする情報セキュリティに関する研修を毎年度最低１回実施しなければならない。

（ウ） 新規採用の教職員等を対象とする情報セキュリティに関する研修を実施しなければならない。

（エ） 研修は、部門情報統括責任者、情報基盤管理者、情報管理者、業務システム管理者及び教職員等情報取扱者に対して、それぞれの役割、情報セキュリティに関する理解度等に応じたものにしなければならない。

（オ） 部門情報統括責任者は、毎年度１回、情報管理委員会に対して、情報セキュリティに関する研修の実施状況について報告しなければならない。

(3) インシデントの報告・分析等

ア インシデントの報告

（ア） 高等専門学校構成員は、情報セキュリティに関するインシデント若しくはシステム上の欠陥及び誤動作を発見した場合、又は外部から報告を受けた場合は、速やかに情報管理者又は業務システム管理者等権限のある者に報告しなければならない。

（イ） 報告を受けた情報管理者又は業務システム管理者等権限のある者は、速やかに部門情報統括責任者に報告しなければならない。また、当該インシデントが高等専門学校にかかるネットワークに関連する場合は、情報基盤管理者に対しても報告しなければならない。

（ウ） 情報管理者は、報告のあったインシデントについて、部門情報統括責任者及び情報セキュリティ最高責任者に報告しなければならない。

イ インシデントの原因調査と再発防止策

（ア） インシデントを引き起こした部門の情報管理者又は業務システム管理者は、情報基盤管理者と連携し、インシデントの原因を調査し、再発防止策を策定し、その結果を部門情報統括責任者及び情報セキュリティ最高責任者に報告しなければならない。

（イ） 情報セキュリティ最高責任者は、情報基盤管理者からインシデントについての報告を受けた場合には、その内容を検討し、再発防止策を実施するために必要な措置を講じなければならない。

（ウ） インシデントを引き起こした部門の情報管理者又は業務システム管理者は、インシデントの再発防止策の記録を保存しなければならない。

(4) アカウントの発行と管理

高等専門学校構成員である情報システムの利用者に付与された識別符号及び主体認証情報の組合せ、又はそれらのいずれかを指して「アカウント」と言う。

ア アカウントの発行

（ア） 高等専門学校構成員である情報システムの利用者は、情報基盤管理者及び業務システム管理者等権限のある者からアカウントの交付を受ける。

（イ） 情報基盤管理者及び業務システム管理者等権限のある者は、利用者等からのアカウント発行申請を受理した場合は、遅滞なくアカウントを発行するものとする。

（ウ） 利用する高等専門学校構成員に姓名の変更等識別コードの変更、停止及び廃止が生じた場合には、速やかに所定の申請書により情報基盤管理者及び業務システム管理者等権限のある者に申請し、アカウントの変更、停止及び廃止を受ける。

（エ） 契約により操作を認められた外部委託業者等臨時的に利用させることを目的としてアカウントの交付を受ける場合、申請者は外部委託業者等にこの規則を遵守させなければならない。

（オ） アカウントを発行するに当たって、暫定主体認証情報で発行する。

イ　アカウントの管理

（ア） 情報基盤管理者及び業務システム管理者等権限のある者はアカウントの適正な管理を行わなければならない。

（イ） 高等専門学校構成員は、次の事項を遵守しなければならない。

① アカウントを適切に管理しなければならない。

② アカウントを利用して、学校外から高等専門学校の情報システムにアクセスする場合には、定められた手順に従ってアクセスしなければならない。

③ 自分のユーザーアカウントを他者に使用させたり、他のユーザーアカウントを使用したり、又他者に開示してはならない。

④ 他の者の主体認証情報を聞き出したり使用したり、またその行為を助ける行為をしてはならない。

⑤ アカウントは、高等専門学校構成員間で共有しない。ただし、所属等ごとに配布されたアカウントについては除く。

⑥ 共用アカウントを利用する場合は、共用アカウントの利用者以外に利用させてはならない。

⑦ アカウントを他者に使用され又はその危険が発生した場合には、直ちに情報基盤管理者及び業務システム管理者等権限のある者にその旨を報告しなければならない。

⑧ アカウントを紛失した場合には、速やかに情報基盤管理者及び業務システム管理者等権限のある者に通報し、指示を仰ぐ。

（ウ） 情報基盤管理者及び業務システム管理者は、利用されていないアカウントが放置されないよう、点検しなければならない。

（エ） 情報基盤管理者及び業務システム管理者等権限のある者は、次の場合アカウントを停止する。

① 高等専門学校の情報システムの利用者資格を喪失した場合

② 臨時的に利用させる期間を超過した場合

③ アカウントの紛失通報があった場合

ウ 特権アカウントの管理

（ア） 情報基盤管理者及び業務システム管理者は、管理者権限等の特権を付与されたアカウントを利用する者を必要最小限にし、当該アカウントの漏えい等が発生しないよう、当該アカウントを厳重に管理しなければならない。

（イ） 情報基盤管理者及び業務システム管理者の特権を代行する者は、当該管理者が指名し、部門情報統括責任者が認めた者でなければならない。

（ウ） 情報基盤管理者及び業務システム管理者は、特権を付与されたアカウントの変更について、原則として外部委託事業者に行わせてはならない。

（エ） 情報基盤管理者及び業務システム管理者は、特権を付与されたアカウントについて高等専門学校構成員の情報機器のアカウントと同等あるいはそれ以上のセキュリティ強化を実施しなければならない。

（オ） 情報基盤管理者及び業務システム管理者は、特権によるネットワーク及び情報システムへの接続時間を必要最小限に制限しなければならない。

（カ） 管理者権限を持つアカウントを付与された者は、管理者としての業務遂行時に限定して、当該アカウントを利用しなければならない。

エ 主体認証の管理

（ア） 高等専門学校構成員は、自己の主体認証に関し、次の事項を遵守しなければならない。

① 主体認証は秘密にし、主体認証の照会等には一切応じない。

② 情報システム又は主体認証に対する危険のおそれがある場合には、情報基盤管理者及び業務システム管理者等権限のある者に速やかに報告し、主体認証を速やかに変更する。

③ 原則として、主体認証情報を記載したメモを作成しない。やむを得ず作成する場合は、他人に分からない場所に保管する。

④ 主体認証は定期的（教職員については概ね半年以内ごと）又はアクセス回数に基づいて変更する。

⑤ 複数の情報システムを扱う場合は、同一の主体認証を複数のシステムで用いない。

⑥ 暫定の主体認証は、最初のログイン時に変更する。

⑦ 情報機器の主体認証の記憶機能を利用しない。

⑧ 高等専門学校構成員の間で主体認証を共有しない。

（イ） 情報基盤管理者及び業務システム管理者は、主体認証の照会等には一切応じてはならない。

(5) 外部委託に関する管理

ア 契約書の記載事項

（ア） ネットワーク及び情報システムの開発・保守及びデータ処理その他情報処理に係る業務を外部委託する場合は、当該委託先事業者との間で、下記事項を明記した契約を締結しなければならない。

① データその他業務上知り得た情報（以下「データ等」という）の秘密の保持に関する事項

② 第三者への委託の禁止又は制限に関する事項

③ データ等の目的以外の目的のための使用及び第三者への提供の禁止に関する事項

④ データ等の複写及び複製の禁止に関する事項

⑤ データ等の取扱いに関する事故の発生時における報告義務に関する事項

⑥ データ等の取扱いに関する検査の実施に関する事項

⑦ 契約に違反した場合における契約の解除及び損害賠償に関する事項

⑧ 委託業務終了時の情報資産の返還及び廃棄等に関する事項

⑨ 情報セキュリティポリシー及びこれに基づく文書の遵守に関する事項

⑩ インシデント発生時の公表に関する事項

⑪ 委託先の責任者、委託内容、従事者、作業場所の特定に関する事項

（イ） 前項に加えて、次に掲げる事項を必要に応じて契約書等に明記するよう努めるものとする。

① 提供されるサービスレベルの保証に関する事項

② 委託業務の定期報告及び緊急時報告義務に関する事項

③ 外部施設等への情報資産の搬送時における紛失、盗聴、不正コピー等の防止に関する事項

イ 情報セキュリティ確保への取組みの実施状況等の調査

情報基盤管理者及び業務システム管理者は、契約締結後においても、当該委託先事業者の情報セキュリティ確保への取組みの実施状況について定期的又は随時、調査を行い、安全を確保しなければならない。部門情報統括責任者から内容の報告を求められた場合には、報告を行わなければならない。

ウ 再委託等

再委託を受ける事業者がある場合、「７．人的セキュリティ (5)外部委託に関する管理」のア、イに定める事項は再委託を受ける事業者にも適用する。

エ　クラウドサービスの利用

教職員がクラウドサービスを利用する場合は、別途定める手順に従うものとする。

8　技術的セキュリティ

(1)　情報機器及びネットワークの管理

ア　データの保存

データの保存については、情報基盤管理者等管理権限のある者の定める方法により保存を行わなければならない。

イ　ファイルサーバの設定等

情報基盤管理者がデータを共有するためのファイルサーバを設置する場合には、次の事項を守らなければならない。

（ア）　教職員、人材派遣職員及び非常勤嘱託職員が使用できるファイルサーバの容量を必要に応じて設定し、人材派遣職員及び非常勤嘱託職員に周知しなければならない。

（イ）　特定の教職員、特定の人材派遣職員及び非常勤嘱託職員のみが取り扱う権限を持つデータについては、権限のない者が閲覧及び使用できないよう設定しなければならない。

ウ　アクセス記録の取得等

（ア）　情報基盤管理者及び業務システム管理者は、所管するシステムにおいて、アクセス記録及び情報セキュリティの確保に必要な記録を取得し、窃取、改ざん、誤消去等を防止する措置を施したうえで一定期間保存する。また、不正アクセスの兆候を発見するために定期的にそれらを分析することとする。

（イ）　情報基盤管理者及び業務システム管理者は、システムから自動出力したアクセス記録等について、必要に応じ、外部記録媒体にバックアップしなければならない。

エ　仕様書等の保管

情報基盤管理者及び業務システム管理者は、所管するシステムのネットワーク構成図、情報システム仕様書等に関し、記録媒体の形態に関わらず、業務上必要とする者以外の者が閲覧したり、紛失したりすることがないよう、適切な保管をしなければならない。

オ　情報資産のバックアップ

情報基盤管理者及び業務システム管理者は、所管するシステムにおいて、必要なものはサーバの二重化対策実施の有無に関わらず、定期的に情報資産のバックアップのための対応を行うものとする。

カ　他団体との情報システムに関する情報等の交換

情報基盤管理者及び業務システム管理者は、他の団体と情報システムに関す

る情報及びソフトウェアを交換する場合、その取扱いに関する事項をあらかじめ定め、部門情報統括責任者及び業務システム責任者の許可を得なければならない。

キ　外部の者が利用するシステム

情報基盤管理者及び業務システム管理者は、インターネット等により外部の者が利用できるシステムにおいては、必要に応じ他のネットワーク及び情報システムと物理的に分ける等、情報セキュリティ対策について特に強固に対策をとらなければならない。

ク　Ｗｅｂサイトでの情報公開時の注意事項

情報基盤管理者及び業務システム管理者は、Ｗｅｂサイトにより情報を公開・提供する場合に、所管するサイトに係るシステムにおいて情報の漏えい・改ざん・消去、踏み台、Ｄｏｓ攻撃等を防止しなければならない。また、メールシステムを含め各業務システムにおいても、他のシステムに対する攻撃の踏み台とならないようにコンピュータウイルス対策等適切な管理をしなければならない。

ケ　無線ＬＡＮの利用

高等専門学校構成員は、適用範囲内のネットワーク（以下「内部ネットワーク」という）において、無線ＬＡＮを利用した接続又は端末等の無線機能を利用した端末間通信を行ってはならない。ただし、情報基盤管理者が特に必要と認める場合には、接続の機密性・安全性等について総合情報センターが審査を行い、情報基盤管理者の許可を得て、無線ＬＡＮを利用した接続等を行うことができる。

コ　無許可ソフトウェアの導入等の禁止

（ア）　高等専門学校構成員は、各自に供与された端末に対して、情報基盤管理者が定めるもの以外のソフトウェアの導入を行ってはならない。

（イ）　ただし、業務を円滑に遂行するため又は教育・研究のために必要なソフトウェアがある場合、情報基盤管理者の定める手続きを行い、必要な許可を得て利用することができる。

（ウ）　高等専門学校構成員は、不正にコピーしたソフトウェア、不正に入手したソフトウェア、及び高等専門学校に利用権の無いソフトウェアを導入又は使用してはならない。

サ　ネットワーク機器構成の変更の禁止

高等専門学校構成員は、ネットワークに関する物理資産の増設又は改造を行ってはならない。軽微な情報機器の増設や変更の場合は、情報基盤管理者等権限のある者の許可を必要とする。

シ　電子メール

（ア） 電子メールの利用を希望する場合は、情報基盤管理者が利用者を特定し、メールアドレスを発行するものとする。

（イ） 情報基盤管理者は、電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能にしなければならない。

（ウ） 情報基盤管理者は、電子メールに添付されるファイルについて、セキュリティ上問題があると思われるファイルについては、送受信を制限できるようにしなければならない。

（エ） メールアドレス保有者は、業務上必要のない送信先に電子メールを送信してはならない。

（オ） メールアドレス保有者は、複数の宛先に電子メールを送信する場合、必要がある場合を除き他の送信先の電子メールアドレスがわからないようにしなければならない。

（カ） メールアドレス保有者は、重要な電子メールを誤送信した場合、情報管理者及び情報基盤管理者に報告しなければならない。

（キ） メールアドレス保有者は、情報基盤管理者の許可なく自動転送機能を用いて、電子メールを転送してはならない。

ス 電子署名・暗号化

（ア） 高等専門学校構成員は、情報資産の分類により定めた取扱制限に従い、外部に送るデータの機密性又は完全性を確保することが必要な場合には、部門情報統括責任者が定める電子署名、暗号化又はパスワード設定等の方法を用いて、送信しなければならない。

（イ） 高等専門学校構成員は、暗号化を行う場合に部門情報統括責任者が定める以外の方法を用いてはならない。また、部門情報統括責任者が定める方法で暗号のための鍵を管理しなければならない。

（ウ） 部門情報統括責任者は、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全に提供しなければならない。

セ 利用可能なネットワークプロトコル

高等専門学校構成員が利用できるネットワークプロトコルは、セキュリティ等の必要に応じて情報基盤管理者が制限を設定する。

ソ 障害記録

情報基盤管理者及び業務システム管理者は、所管するシステムにおいて、高等専門学校構成員からのシステム障害の報告、システム障害に対する処理結果又は問題等を障害記録として体系的に記録し、適切に保存しなければならない。

(2) アクセス制御

ア 利用者の識別及び認証

情報基盤管理者及び業務システム管理者は、所管するネットワーク又は情報

システムに権限がない者がアクセスすることが不可能となるように、利用者の識別及び認証等適切な対応を行わなければならない。

イ　利用者の点検

情報基盤管理者及び業務システム管理者は、アカウントに割り当てているアクセス権の正当性を確保するために、定められた方法に従って点検しなければならない。

ウ　ネットワークにおけるアクセス制御

情報基盤管理者及び業務システム管理者は、アクセス可能なネットワーク又はネットワーク上のサービス毎にアクセスできる者を定めなければならない。また、ネットワークサービスを利用する権限を有しない者が当該サービスを利用できるようにしてはならない。

エ　強制的な接続制御、経路制御

（ア）　情報基盤管理者及び業務システム管理者は、不正アクセスを防止するため、適切なネットワーク経路制御を施さなければならない。

（イ）　情報基盤管理者及び業務システム管理者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等に搭載されている通信ソフトウェア等を設定しなければならない。

オ　無人状態にある装置の管理

情報基盤管理者及び業務システム管理者は、サーバ又は端末等の装置が無人の状態になる場合、適切なセキュリティ対策を施さなければならない。

カ　外部からのアクセス

（ア）　情報基盤管理者及び業務システム管理者は、外部からのアクセスを許可する場合、合理的理由を有する必要最低限のものに限定しなければならない。

（イ）　内部ネットワーク及び情報システムへのアクセス方法及び利用方法等は、通信途上の機密性及び利用者の真正性が確保できるものでなければならない。

（ウ）　高等専門学校構成員は、学校外で利用する物理資産について、セキュリティ確保のために必要な措置を講じなければならない。

キ　外部ネットワークとの接続

（ア）　情報基盤管理者及び業務システム管理者は、外部ネットワークとの接続にあたり当該外部ネットワークのネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、高等専門学校の情報資産に影響が生じないことを確認したうえで、部門情報統括責任者の許可に基づき接続しなければならない。

（イ）　情報基盤管理者及び業務システム管理者は、接続に際して情報セキュリティの確保できるネットワーク構成を採らなければならない。情報基盤管理者及び業務システム管理者は、当該外部ネットワークの瑕疵により高等専門学

校のデータの漏えい、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対応するため、必要に応じて当該外部ネットワークの管理責任者による損害賠償責任を契約上担保するよう努めなければならない。

（ウ） 接続した外部ネットワークのセキュリティに問題が認められ、高等専門学校の情報資産に脅威が生じるおそれがある場合には、情報基盤管理者及び業務システム管理者は当該外部ネットワークとの接続を物理的に遮断することができるものとする。

ク ネットワーク機器の自動識別

情報基盤管理者及び業務システム管理者は、高等専門学校のネットワークで使用される機器について、機器固有情報等によって端末とネットワークとのアクセスの可否が自動的に識別されるよう必要に応じてシステムを設定しなければならない。

ケ ログイン試行回数の制限等

情報基盤管理者及び業務システム管理者は、ログイン試行回数の制限及びアクセスタイムアウトの設定等により、正当なアクセス権を持たない者が利用できないようにシステムを設定するよう考慮しなければならない。

コ 主体認証情報の管理

（ア） 情報基盤管理者及び業務システム管理者は、高等専門学校構成員を識別するためのクレデンシャルを設定した情報を厳重に管理しなければならない。

（イ） 情報基盤管理者及び業務システム管理者は、暫定主体認証も含めアカウントを発行する場合は他者が想像しにくいものとする。

(3) システム開発、導入、保守等

ア 情報システムの調達

（ア） 情報基盤管理者及び業務システム管理者は、情報システムの調達にあたっては、一般に公開する調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

（イ） 情報基盤管理者及び業務システム管理者は、物理資産及びソフトウェアの調達にあたっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

（ウ） 部門情報統括責任者は、適切に情報セキュリティ対策を推進・管理するための基礎資料として、情報システム台帳を作成し、整理する。業務システム管理者は、情報システムを新たに調達したり、既にある情報システムを廃止したりしたときは、部門情報統括責任者からの求めに応じて、報告しなければならない。

イ 情報システムの開発等

（ア） 情報基盤管理者及び業務システム管理者は、ネットワーク及び情報システ

ムの開発、導入、更新及び運用保守にあたっては、次の事項を定める。

① 責任者及び監督者
② 従事者及び作業範囲
③ 開発するシステムと運用中のシステムとの分離
④ 開発・保守に関する設計仕様等の成果物の提出
⑤ セキュリティ上問題となり得るおそれのあるハードウェア及びソフトウェアの使用禁止
⑥ アクセス制限
⑦ 物理資産の搬入出の際の許可及び確認
⑧ 記録の提出義務
⑨ 仕様書・マニュアル等の定められた場所への保管
⑩ 情報システムに係るソースコードの適切な方法での保管
⑪ 開発・保守を行った者の利用者ＩＤ、パスワード等の当該開発・保守終了後に不要となった時点での速やかな抹消

（イ） 情報基盤管理者及び業務システム管理者は、ネットワーク及び情報システムの開発、導入、更新及び運用保守にあたって、不正にコピーしたソフトウェア及び個人所有のソフトウェアを導入又は使用等、問題のある行為が発生しないようにしなければならない。

（ウ） 情報基盤管理者及び業務システム管理者は、ネットワーク及び情報システムの開発、導入、更新及び運用保守にあたって、コンピュータウイルス等対策ソフトウェアを導入する等、ウイルス感染による情報漏えい等が発生しないようにしなければならない。

ウ 情報システムの移行

（ア） 情報基盤管理者及び業務システム管理者は、システム開発・保守計画の策定時に情報システムの移行手順を明確にしなければならない。また、移行の際、情報システムに記録されているデータの保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。

（イ） 情報基盤管理者及び業務システム管理者は、新たに情報システムを導入する際には、既に稼働している情報システムに接続する前に、十分な試験を行わなければならない。また、既存の情報システムを更新する際には、既に稼働している情報システムとの連携において、十分な試験を行わなければならない。

（ウ） 情報基盤管理者及び業務システム管理者は、擬似環境による動作確認後に情報システムの移行を行わなければならない。また、作業については、作業経過を確認しながら実施するとともに、作業内容を記録しなければならない。

（エ） 情報基盤管理者及び業務システム管理者は、原則として個人情報及び機密

性の高い生データを試験データに使用してはならない。ただし、合理的な理由がある場合で、部門情報統括責任者が許可した場合は、この限りではない。

（オ） 情報基盤管理者及び業務システム管理者は、試験に使用したデータ及びその結果を５年間厳重に管理しなければならない。

エ 情報システムの入出力データ

（ア） 情報基盤管理者及び業務システム管理者は、情報システムに入力されるデータについて、範囲、妥当性のチェック機能及び不正な文字列等の入力を除去する機能を必要に応じて組み込むように情報システムを設計しなければならない。

（イ） 情報基盤管理者及び業務システム管理者は、内部処理において誤ったデータに書き換えられる等の可能性がある場合に、書き換え等を検出するチェック機能を組み込むように情報システムを設計しなければならない。

（ウ） 情報基盤管理者及び業務システム管理者は、情報システムから出力されるデータは、保存された情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。

オ ソフトウェアの保守及び更新

情報基盤管理者及び業務システム管理者は、ソフトウェア等を更新、又は修正プログラムを導入する場合、不具合及び他のシステムとの相性の確認を行い、計画的に更新し又は導入しなければならない。また、情報セキュリティに重大な影響を及ぼす不具合に対する修正プログラムについては、情報基盤管理者及び業務システム管理者は、速やかに対応を行わなければならない。

カ 委託業務等従事者の身分確認

情報基盤管理者及び業務システム管理者は、作業前に委託業務等従事者に対して身分証明書の提示を求め、契約で定められた資格を有するものが作業に従事しているか確認をすることができるようにしておかなければならない。

キ 作業の確認

契約により操作を認められた委託業務等従事者が重要なシステム変更等の作業を行う場合は、２名以上で作業しその作業を相互確認又は教職員の立ち合い確認の元で作業を行わなければならない。

ク 作業管理記録

情報基盤管理者及び業務システム管理者は、担当するシステムにおいて行ったシステム変更等の作業については、作業記録を作成しなければならない。作成した作業記録は、窃取、改ざん等をされないように適切に管理を行わなければならない。

(4) コンピュータウイルス等不正プログラム対策

ア 情報基盤管理者の実施事項

情報基盤管理者は、次の事項を実施しなければならない。

（ア） コンピュータウイルス等の情報について高等専門学校構成員に対する注意喚起を行う。

（イ） 常時コンピュータウイルス等に関する情報収集に努める。

（ウ） コンピュータウイルス等対策ソフトウェア及び定義ファイルは常に最新のものに保たせるよう指導等を行う。

イ 情報基盤管理者等の実施事項

情報基盤管理者、業務システム管理者及び情報管理者は、次の事項を実施しなければならない。

（ア） 所管するサーバ及び端末に、コンピュータウイルス等対策ソフトウェアを常駐させる。再起動により環境復元する等対策が施されている場合はこの限りではない。

（イ） 情報システムにおいて電子記録媒体を使用する場合、高等専門学校構成員にウイルスチェックを行わせる。

（ウ） コンピュータウイルス等対策ソフトウェア及び定義ファイルは常に最新のものに保つ。

ウ 高等専門学校構成員の遵守事項

高等専門学校構成員は、次の事項を遵守しなければならない。

（ア） 端末において、コンピュータウイルス等対策ソフトウェアが導入されている場合は、情報セキュリティ最高責任者の指示に従い設定する。

（イ） 外部ネットワーク及び電子記録媒体からデータ又はソフトウェアを取り入れる際には、必ずコンピュータウイルス等対策ソフトウェアによるチェックを行う。

（ウ） 外部ネットワーク及び電子記録媒体へデータ又はソフトウェアを送信・書き込みする際には、必ずコンピュータウイルス等対策ソフトウェアによるチェックを行う。

（エ） 差出人が不明な電子メール又は不自然なファイルが添付された電子メールを受信した場合は速やかに削除する。

（オ） 情報機器に対して、コンピュータウイルス等対策ソフトウェアによる完全スキャンを定期的に行い、スキャンの実行を途中で止めない。

（カ） 情報基盤管理者が提供するコンピュータウイルス等の情報を常に確認する。

（キ） 添付ファイルのあるメールを送受信する場合は、コンピュータウイルス等対策ソフトウェアでチェックを行う。

（ク） コンピュータウイルス等に感染したおそれがある場合は、速やかに情報管理者等権限のある者に報告するとともに、その指示に従い、ＬＡＮケーブル

の即時取り外しや端末の通信機能の停止等、他への感染を防止する措置を講じる。

（ケ） ウイルス対策ソフトウェア等により不正プログラムとして検知される実行ファイルを実行しない。

（コ） 外部からデータやソフトウェアを物理資産に取り込む場合又は外部にデータやソフトウェアを提供する場合には、不正プログラム感染の予防に努める。

（サ） 常に最新のセキュリティ情報に注意し、不正プログラム感染の予防に努める。

（シ） 情報基盤管理者及び業務システム管理者等権限のある者より不正プログラム対策の指示があった場合には、それに従って当該情報システムに対して対策を実施する。

エ 専門家の支援体制

部門情報統括責任者は、実施しているコンピュータウイルス等対策では不十分な事態が発生した場合に備え、外部の専門家の支援を受けられるようにしておかなければならない。

(5) 不正アクセス対策

ア 使用されていないポートの閉鎖等

情報基盤管理者及び業務システム管理者は、不正なアクセスによる影響を防止するための必要な措置を講じなければならない。

（ア） 使用されていないポートを閉鎖する。

（イ） サーバ上の不要なサービスを停止する。

（ウ） 不正アクセスに関する情報の収集に努め、当該情報について必要な措置を講ずるものとする。

（エ） ソフトウェアにセキュリティホールが発見された場合は、速やかに修正プログラムを適用する。

イ 攻撃の対処

情報基盤管理者及び業務システム管理者は、所管するシステムへの攻撃の予告等サーバ等に不正アクセスを受けることが明白な場合には、システムの停止、他のネットワークとの切断等の必要な措置を講じなければならない。

また、関係機関との連絡を密にして情報の収集に努めなければならない。

ウ 記録の保存

情報セキュリティ最高責任者及び部門情報統括責任者は、不正アクセス行為の禁止等に関する法律違反等犯罪の可能性がある不正アクセスを受けた場合、不正アクセスの記録の保存に努めるとともに、関係機関との緊密な連携に努めなければならない。

エ　内部からの不正アクセスの監視

情報基盤管理者及び業務システム管理者は、学校内の情報機器からの、学校内のサーバ等に対する不正アクセスや外部のサイトに対する不正アクセスを監視しなければならない。

オ　高等専門学校構成員による不正アクセス時の措置

高等専門学校構成員による不正アクセスがあった場合、情報基盤管理者及び業務システム管理者は適切な措置をとらなければならない。

(6)　セキュリティ情報の収集

情報基盤管理者は、セキュリティホール等のセキュリティに関する情報を収集し、必要に応じ関係者間で情報を共有しなければならない。

9　運用面のセキュリティ

(1)　情報システムの監視

ア　事象の検知

情報基盤管理者及び業務システム管理者は、セキュリティに関する事象を検知するため、情報システムの監視を行わなければならない。

イ　時刻同期

情報基盤管理者及び業務システム管理者は、重要なアクセスログ等を取得するサーバの正確な時刻設定又はサーバ間の時刻同期ができる措置を施さなければならない。

ウ　常時監視

情報基盤管理者及び業務システム管理者は、外部と接続するシステムを稼働中、常時監視しなければならない。

(2)　情報セキュリティポリシー等の遵守状況の確認及び対処

情報基盤管理者、業務システム管理者及び情報管理者は、所管の範囲において情報セキュリティポリシー及びこれに基づく文書の遵守状況について常に確認を行い、問題を認めた場合には速やかに部門情報統括責任者に報告しなければならない。部門情報統括責任者は、発生した問題について、適切かつ速やかに対処しなければならない。

(3)　運用管理における留意点

ア　調査権限のある高等専門学校構成員の指名

部門情報統括責任者は、情報漏えい、不正アクセス、コンピュータウイルス等の調査のために、物理資産、アクセス記録及びメール等の情報を調査する権限を有する高等専門学校構成員を指名する。

イ　情報セキュリティポリシー等の閲覧

情報基盤管理者、業務システム管理者及び情報管理者は、高等専門学校構成員、人材派遣職員及び非常勤嘱託職員が常に情報セキュリティポリシー及びこれに

基づく文書を参照できるよう配慮しなければならない。

ウ　管理者権限

情報基盤管理者、業務システム管理者及び情報管理者の権限を代行する者は、それぞれが指名する。

エ　高等専門学校構成員の報告義務

（ア）　高等専門学校構成員は、情報セキュリティポリシーに対する違反行為を発見した場合、直ちに情報基盤管理者及び情報管理者に報告を行わなければならない。

（イ）　違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると部門情報統括責任者が判断した場合は、緊急時対応計画に従って適切に対処しなければならない。

(4)　緊急時の対応

ア　緊急時対応計画の策定

情報基盤管理者及び業務システム管理者は、情報資産への重大な侵害が発生した場合又は発生するおそれがある場合において、連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適切に実施するために、緊急時対応計画を策定しなければならない。

イ　緊急時対応計画に盛り込むべき内容

緊急時対応計画には、次の内容を定めなければならない。

（ア）　関係者の連絡先

（イ）　意思決定の所在

（ウ）　発生した事象に係る報告すべき事項

（エ）　発生した事象への対応措置

（オ）　再発防止措置の策定

ウ　緊急時対応計画の見直し

情報基盤管理者及び業務システム管理者は、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて緊急時対応計画を見直さなければならない。

(5)　例外措置

ア　例外措置の許可

情報基盤管理者、業務システム管理者及び情報管理者は、情報セキュリティポリシーを遵守することが困難な状況で、学校業務の適正な遂行を継続するため、遵守事項とは異なる方法を採用し、又は遵守事項を実施しないことについて合理的な理由がある場合には、情報セキュリティ最高責任者の許可を得て、例外措置を取ることができる。なお、情報セキュリティ最高責任者が、軽微な例外措置と判断したものについては、当該責任者の許可により、例外措置を取ることができ

る。

イ　緊急時の例外措置

情報基盤管理者、業務システム管理者及び情報管理者は、前項に該当する場合であって、学校業務の遂行に緊急を要し、前項に定める許可を得る時間的な猶予のないときは、例外措置を実施し、実施後速やかに情報セキュリティ最高責任者及び部門情報統括責任者に報告しなければならない。

ウ　例外措置の申請書等の管理

情報セキュリティ最高責任者は、例外措置の申請書、報告書及び審査結果を適切に保管させなければならない。

１０　情報セキュリティ個別基準の策定

部門情報統括責任者は、情報セキュリティポリシーを補完するために必要な事項に関して、具体的な内容を定めた情報セキュリティ個別基準を策定する。

１１　情報セキュリティ実施手順の策定

部門情報統括責任者及び業務システム管理者は、情報セキュリティポリシーに基づき、所管するシステム等に対する情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定する。

１２　情報セキュリティに関する違反に対する対応

(1)　懲戒処分

情報セキュリティポリシー及びこれに基づく文書に違反した高等専門学校構成員及びその監督責任者は、その重大性、発生した事象の状況等に応じて、神戸市公立大学法人職員就業規則等による懲戒処分の対象となる。

(2)　再発防止の指導等

高等専門学校構成員に情報セキュリティポリシー及びこれに基づく文書に違反する行為がみられた場合には、情報基盤管理者、業務システム管理者及び情報管理者は、速やかに次の措置を講じなければならない。

ア　当該高等専門学校構成員に対して速やかに調査を行い、事実を確認する。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。

イ　当該高等専門学校構成員に対して違反する行為の事実を通知し、再発防止の指導その他適切な措置を行う。

ウ　指導等によっても改善されない場合、当該高等専門学校構成員の情報資産の使用権を停止あるいは剥奪する。

エ　違反する行為が生じた場合、違反する行為の内容、指導内容その他措置の状況について情報セキュリティ最高責任者に報告する。

１３　評価・改善・見直し

(1)　監査

ア　実施方法

情報セキュリティ最高責任者は、情報監査統括責任者に命じ、情報セキュリティ対策状況について、定期的及び必要に応じて監査を行わせなければならない。

イ　監査を行う者の要件

（ア）　情報監査統括責任者は、 監査を実施する場合には、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。

（イ）　監査を行う者は、監査及び情報セキュリティに関する専門知識を有する者でなければならない。

ウ　監査実施計画の策定及び実施への協力

（ア）　情報監査統括責任者は、監査を行うに当たって監査実施計画を策定し、情報管理委員会に報告しなければならない。

（イ）　被監査部門は、監査の実施に協力しなければならない。

エ　委託先事業者に対する監査

情報監査統括責任者は、委託先事業者に対して委託先事業者からの再委託の事業者も含めて、情報セキュリティポリシーの遵守について監査を定期的及び必要に応じて行わなければならない。

オ　監査結果の報告

情報監査統括責任者は、監査結果を取りまとめ、情報管理委員会に報告する。

カ　監査調書等の保管

情報監査統括責任者は、監査の実施を通して収集した監査証拠及び監査報告書の作成のための監査調書を紛失等が発生しないように適切に保管しなければならない。

キ　指摘事項への対処

部門情報統括責任者は、監査結果を踏まえ、指摘事項に関係する情報管理者等に対し、当該事項への対処を指示しなければならない。また、指摘事項に関係しない情報管理者等に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。

ク　監査結果の活用

情報セキュリティ最高責任者は、情報セキュリティポリシー等情報セキュリティ対策の見直し時に監査結果を活用しなければならない。

(2)　自己点検

ア　実施方法

（ア）　情報基盤管理者及び業務システム管理者は、所管するネットワーク及び情報システムの情報セキュリティ対策状況について、定期的及び必要に応じて自己点検を実施しなければならない。

（イ）　情報管理者は、所管する部門の情報セキュリティ対策状況について、定期的及び必要に応じて自己点検を行わなければならない。

イ　自己点検結果等の報告

（ア）　情報基盤管理者、業務システム管理者及び情報管理者は、自己点検結果と自己点検結果に基づく改善策を取りまとめ、部門情報統括責任者に報告しなければならない。

（イ）　部門情報統括責任者は、報告を受けた点検結果及び改善策を情報管理委員会に報告しなければならない。

ウ　自己点検結果の活用

（ア）　高等専門学校構成員は、自己点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。

（イ）　情報セキュリティ最高責任者は、情報セキュリティポリシー等情報セキュリティ対策の見直し時に点検結果を活用しなければならない。

(3)　改善

ア　是正措置

情報基盤管理者、業務システム管理者及び情報管理者は、業務上発見された問題、外部からの指摘による問題、監査及び自己点検において指摘された問題等に対する再発防止のため、その原因を除去するための措置を施さなければならない。

イ　予防措置

情報基盤管理者、業務システム管理者及び情報管理者は、業務上予見される問題、他の組織で発生したものと同種の情報セキュリティインシデント、監査及び自己点検において指摘されうる問題等の発生を未然に防止するため、その原因を除去するための措置を施さなければならない。

(4)　情報セキュリティポリシーの見直し

情報セキュリティ最高責任者は、監査及び自己点検の結果、改善の状況、残留リスク、情報セキュリティに関する状況の変化等を踏まえ、必要があると認めた場合、情報セキュリティポリシー等情報セキュリティ関連文書の見直しを行う。

附　則

1　この規則は、2023年４月１日から施行する。

2　公立大学法人神戸市外国語大学　情報セキュリティポリシー（2008年11月規程第14号）は、廃止する。