XXXX-XX-0XXX

公立大学法人
神戸市看護大学情報セキュリティ対策基準

制定日：2019 年 4 月 1 日

公立大学法人神戸市看護大学

施行年月日	版番号	改訂理由・内容
2019年4月1日	第1.0版	

目次

1　目的

公立大学法人神戸市看護大学情報セキュリティ対策基準とは，公立大学法人神戸市看護大学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

公立大学法人神戸市看護大学（以下「法人」という。）を適用範囲とし，対象者は，役員，職員，派遣労働者，学生及び委託業務等従事者（以下「役職員等情報取扱者」という。）とする。

3　情報セキュリティ管理体制

3.1　体制

適切に情報セキュリティ対策を推進・管理するため，次の者を置く。

3.1.1　情報セキュリティ最高責任者

理事長を情報セキュリティ最高責任者とする。

3.1.2　情報セキュリティ責任者

学長を情報セキュリティ責任者とする。

3.1.3　情報基盤管理者

図書情報センター長を情報基盤管理者とする。

3.1.4　情報責任者

事務局長を情報責任者とする。

3.1.5　情報管理者

各常設委員会委員長及び経営管理課長を情報管理者とする。

3.1.6　業務システム責任者

図書情報センター長及び経営管理課長を業務システム責任者とする。

3.1.7　業務システム管理者

図書情報センター副センター長及び経営管理課総務係長を業務システム管理者とする。

3.1.8　情報セキュリティ監査統括責任者

学長を情報セキュリティ監査統括責任者とする。

3.2　権限と責任

公立大学法人神戸市看護大学情報セキュリティ基本方針及び前項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。

3.2.1　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ものとする。

3.2.2 情報セキュリティ責任者

ア　情報セキュリティ責任者は情報セキュリティ最高責任者を補佐する。

イ　情報セキュリティ責任者は，法人にかか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　情報セキュリティ責任者は，法人にかか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　情報セキュリティ責任者は，情報基盤管理者，情報責任者，情報管理者，業務システム責任者，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　情報セキュリティ責任者は，法人にかかる情報資産に対する情報セキュリティ侵害が発生した場合又は侵害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　情報セキュリティ責任者は，法人にかかるネットワーク，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の維持・管理を行う統括的な権限及び責任を有する。

キ　情報セキュリティ責任者は，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，情報基盤管理者，情報責任者，情報管理者，業務システム責任者，情報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。

3.2.3 情報基盤管理者

ア　情報基盤管理者は，法人にかかるネットワーク，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。

イ　情報基盤管理者は，法人にかかるネットワーク，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。

ウ　情報基盤管理者は，法人にかかるネットワーク，情報システム，データ等の情報資産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　情報基盤管理者は，法人にかかるネットワーク，情報システム，データ等の情報資産に対する侵害が発生した場合又は侵害のおそれがある場合には，情報セキュリティ責任者，情報セキュリティ最高責任者へ速やかに報告を行い，指示を仰がねばならない。

オ　情報基盤管理者は，法人にかかるネットワーク，情報システム，データ等の情報資産のうちパーソナルコンピュータ等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。

3.2.4　情報責任者

ア　情報責任者は，法人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。

イ　情報責任者は，情報管理者を監督し，法人における緊急時等の連絡体制の整備並びに役職員等情報取扱者に対する助言及び指示を行う。

3.2.5　情報管理者

ア　情報管理者は，法人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法人にかかるネットワーク，情報システム，データ等の情報資産のうち法人内のパーソナルコンピュータ等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，法人内におけるデータ等の情報資産に対する情報セキュリティ侵害が発生した場合又は侵害のおそれがある場合には，情報セキュリティ責任者，情報基盤管理者，業務システム管理者，情報責任者へ速やかに報告を行い，指示を仰がねばならない。

3.2.6　業務システム責任者

ア　業務システム責任者は，当該業務システムにおける開発，設定の変更，運用，見直し等を行う統括的な権限及び責任を有する。

イ　業務システム責任者は，当該業務システムの情報セキュリティ対策に関する統括的な権限及び責任を有する。

ウ　業務システム責任者は，当該業務システムに関する情報セキュリティ実施手順の維持・管理を行う統括的な権限及び責任を有する。

エ　業務システム責任者は，当該業務システムについて，緊急時等の連絡体制の整備，情報セキュリティポリシーの遵守に関する意見の集約及び役職員等情報取扱者に対する助言及び指示を行う。

3.2.7　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情報セキュリティ侵害が発生した場合又は侵害のおそれがある場合には，情報セキュリティ責任者，情報基盤管理者，業務システム責任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。

3.2.8　情報セキュリティ監査統括責任者

情報セキュリティ監査統括責任者は，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。

3.2.9　情報管理委員会

情報管理委員会において，情報セキュリティに関する重要な事項を審議し，その内容を情報セキュリティ最高責任者に報告する。

3.2.10　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。

3.3 情報セキュリティに関する統一的な窓口の設置（CSIRT）

3.3.1　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（Computer Security Incident Response Team）を設置し，図書情報センターが，その役割を担う。

3.3.2　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。

3.3.3　CSIRT の連絡体制

CSIRT の統一窓口は，情報基盤管理者とする。情報セキュリティ責任者は，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，神戸市等の関係機関との情報共有を行う。

4　情報資産の分類と管理

4.1 情報資産の管理責任

4.1.1　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。

4.1.2　情報取扱者の責任

役職員等情報取扱者は，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。

4.1.3　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。

4.2 情報資産の分類と管理方法

4.2.1　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

分類	分類基準	主な取扱制限等
3	法人業務で取り扱う情報資産のうち，特に機密性を要するもの （次のデータだけではなくそれらが含まれる電子記録媒体，パーソナルコンピュータ，システム等も同様） ・ 特定個人情報に関するデータ ・ 個人情報に関するデータ ・ 法令の規定により秘密を守る義務を課されているデータ ・ 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データ ・ 部外に漏れた場合に本学の信頼を著しく害する可能性があるデータ ・ 公開することでセキュリティ侵害が生じる可能性があるデータ	【機密性３】 ・ 情報資産管理責任者の許可を得た場合，複製・送付・送信を行うことができる。また，権限のある者だけがアクセスできる環境で，保存・利用をしなければならない。複数の権限ある者でデータを共有したり，学外にデータを送付・送信したりするときも，パスワード等による情報漏えい対策を施さなければならない（4.2.3 エ(3)）。 ・ 外部に提供する者は，必要に応じ暗号化又はパスワードの設定を行わなければならない（4.2.3 カ(1)） ・ 外部に提供する者は，情報資産管理責任者に事前に許可を得たうえで，日時・担当者及び提供概要を記録しなければならない。ただし，情報セキュリティ責任者又は情報責任者が特に指示した場合にはその指示に従うこととする。（4.2.3 カ(2)）。 【機密性３・２共通】 ・ 電子記録媒体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，暗号化又はパスワードの設定を行う等，情報資産の不正利用を防止するための措置を施すものとする（4.2.3 オ（4））。 ・ 権限のある者の許可を得た場合に限り，記録
2	機密性３には当てはまらないが，直ちに一般に公表することを前提としていない情報資産	

		を作成したうえで，学外へ持ち出すことができる(6.1.5)。 ・ 異動，退職等により業務を離れる場合には，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（6.1.9)。 ・パート職員及びアルバイト職員（以下「パート職員等」という。）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，パート職員等は 6.1.1～6.1.9 に定める事項を守らなければならない。(6.1.10)。 【機密性２】 ・ 電子メールによりデータを送信する者は，必要に応じパスワード等による情報漏えい対策を施すものとする（4.2.3エ(4)）。
1	機密性２又は機密性３以外の情報資産	

完全性

分類	分類基準
2	法人業務で取り扱う情報資産のうち，改ざん，誤びゅう又は破損により，学生，保護者，法人役職員及び法人関係者[受験生，業務連携先]の権利が侵害される又は法人業務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産
1	完全性２以外の情報資産

可用性

分類	分類基準
2	法人業務で取り扱う情報資産のうち，滅失，紛失又は当該情報資産が利用不可能であることにより，学生，保護者，大学及び法人関係者[受験生，業務連携先]の権利が侵害される又は法人業務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産
1	可用性２以外の情報資産

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。

4.2.2　情報資産に対するリスク分析の実施

ア　法人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。

4.2.3　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) 業務上必要のない機密性 2 以上のデータを作成してはならない。

(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) 法人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) 法人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，情報管理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，利用者並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，送信を行うことができる。ただし，パスワード等による情報漏えい対策を施さなければ電子メールによる送信を行ってはならない。

(4) 電子メールにより機密性２のデータを送信する者は，必要に応じパスワード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，記録媒体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，当該記録媒体を取り扱わなければならない。

オ　情報資産の保管

(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記録媒体は，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，持ち運び可能な記録媒体を，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) 機密性２以上の情報資産が保管された記録媒体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，暗号化又はパスワードの設定を行う等，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。

(5) 機密性２以上の情報資産が保管された記録媒体を運搬する者は，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者は，必要に応じ暗号化又はパスワードの設定を行わなければならない。

(2) 機密性３の情報資産を外部に提供する者は，情報セキュリティ責任者又は情報責任者に事前に許可を得たうえで，日時・担当者及び提供概要を記録しなければならない。ただし，情報セキュリティ責任者又は情報責任者が特に指示した場合にはその指示に従うこととする。

(3) 情報資産管理責任者は，学生，保護者及び法人関係者に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) 電子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，溶解等により廃棄しなければならない。

(2) 情報資産の廃棄を行う者は，行った処理について，日時，担当者及び処理内容を記録しなければならない。

(3) 情報資産の廃棄を行う者は，情報資産管理責任者の許可を得なければならない。

4.2.4 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，文書管理規程及び情報セキュリティに係る文書管理基準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。

4.2.5 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。

5 物理的セキュリティ

5.1 サーバ等の管理

5.1.1 入退室の管理

情報資産管理責任者は，重要性分類２以上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 管理区域を新設する場合は，管理区域を地階又は１階に設けてはならない。また，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　役職員等情報取扱者は，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等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すものとする。

カ　管理区域については，当該システムに関連しないコンピュータ，通信回線装置，記録媒体等を持ち込ませないようにしなければならない。

5.1.2　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ＩＤ，パスワードの設定等の措置を施さなければならない。

5.1.3　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。

5.1.4　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。

5.1.5　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２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他，秘密保持体制の確認などを行わなければならない。

5.1.6　消火薬剤及び消防用設備

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

5.1.7　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，本学の敷地外にサーバ等の機器を設置する場合，情報セキュリティ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。

5.1.8　機器の廃棄等

情報基盤管理者，業務システム管理者及び情報管理者は，機器を廃棄，リース返却等をする場合，機器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。

5.1.9　機器等の搬入出

ア　情報基盤管理者及び業務システム管理者は，機器等を搬入する場合，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　機器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。

5.2 ネットワークの管理

5.2.1　法人内の通信回線等の管理

情報基盤管理者及び業務システム管理者は，法人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。

5.2.2　外部ネットワークへの接続

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。

5.2.3　機密を要する情報システムで使用する回線

情報基盤管理者及び業務システム管理者は，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。

5.2.4　ネットワークで使用する回線

ア　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。

イ　情報基盤管理者及び業務システム管理者は，ネットワークで使用する回線を選択するにあたって，必要な可用性を考慮しなければならない。

5.3 端末等の管理

5.3.1　端末等の盗難防止策

情報基盤管理者，業務システム管理者及び情報管理者は，法人内の端末等について，盗難防止のため，必要に応じて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。

5.3.2　ログインパスワード

情報基盤管理者及び業務システム管理者は，情報システムへのログインパスワードの入力を必要とするように設定しなければならない。また，必要に応じて電源起動時のパスワード（BIOS パスワード，ハードディスクパスワード等）を併用するものとする。

5.3.3　認証の併用

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，生体認証等の二要素認証を行うものとする。

5.3.4　暗号化機能の利用

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。

5.3.5　タブレット端末等の持ち運び可能な端末（モバイル端末）のセキュリティ

モバイル端末を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。

6 人的セキュリティ

6.1 役職員等情報取扱者の責務

6.1.1 情報セキュリティポリシー等の遵守義務

役職員等情報取扱者は，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。

6.1.2 法令等の遵守義務

役職員等情報取扱者は，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）
・神戸市個人情報保護条例（平成 9 年 10 月条例第 40 号）
・職員就業規則（平成 31 年 4 月規程第～号）
・文書管理規程（平成 31 年 4 月規程第～号）

6.1.3 指示に基づいた情報資産の利用等

役職員等情報取扱者は，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。

6.1.4 個人所有の情報資産の持ち込み

役職員等情報取扱者は，個人の所有するパーソナルコンピュータ及び記録媒体等の持ち込みをする場合は，大学情報管理者権限のある者の許可のもと，自らの責任で本対策基準に則った管理・使用を行わなければならない。

6.1.5 情報資産の持ち出し禁止

役職員等情報取扱者は，機密性２以上の情報資産について，情報管理者等管理権限のある者の許可を得たうえで，持ち出すことができる。また，持ち出しにあたってはその記録を作成しなければならない。

6.1.6 業務目的外の利用禁止

役職員等情報取扱者は，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。

6.1.7 端末等の利用

ア　役職員等情報取扱者は，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。

イ　役職員等情報取扱者は，端末や記録媒体，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。

6.1.8　法人外における情報処理作業の制限

ア　情報セキュリティ責任者は，機密性２以上，可用性２，完全性２の情報資産を法人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　役職員等情報取扱者は，法人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，情報セキュリティ責任者の定める事項を遵守しなければならない。

6.1.9　異動，退職時等の遵守事項

役職員等情報取扱者は，異動，退職等により業務を離れる場合には，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。

6.1.10　パート職員等

パート職員等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，パート職員等は 6.1.1～6.1.9 に定める事項を守らなければならない。

6.1.11　学生等

学生等が大学の情報機器及びネットワークを利用する場合，教職員等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，情報セキュリティ責任者の指定する授業科目等を受講し，利用許可を得た後に，教職員等の指導の下で利用するものとする。

6.1.12　臨時的利用者

学外からの訪問者等が臨時的に法人の情報機器及びネットワークを利用する場合，役職員等は情報セキュリティ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。

6.2 研修・訓練

6.2.1　役職員等に対する研修・訓練の実施

情報セキュリティ最高責任者は，役職員等情報取扱者に対して定期的に情報セキュリティに関する研修・訓練を実施しなければならない。

6.2.2　研修計画の策定及び実施

ア　情報セキュリティ責任者は，役職員等情報取扱者に対して情報セキュリティに関する研修計画を定期的に策定し，情報管理委員会を経て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　役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　新規採用の役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，情報セキュリティ責任者，情報基盤管理者，情報責任者，情報管理者，業務システム責任者，業務システム管理者及び役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　情報セキュリティ責任者は，毎年度１回，情報管理委員会を経て情報セキュリティ最高責任者に対して，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。

6.2.3　緊急時対応訓練

情報セキュリティ最高責任者は，緊急時対応を想定した訓練を定期的に実施させなければならない。訓練計画は，ネットワーク及び各情報システムの規模等を考慮し，訓練実施の内容等を定め，また，効果的に実施できるようにしなければならない。

6.2.4　研修等への参加

すべての役職員等情報取扱者は，情報セキュリティに関する意識を深め情報セキュリティ上の問題が生じないようにするため，定められた研修・訓練に参加しなければならない。

6.3 情報セキュリティに関する事件・事故等の報告・分析等

6.3.1　情報セキュリティに関する事件・事故等の報告

ア　役職員等情報取扱者は，情報セキュリティに関する事件・事故等を発見した場合，若しくは保護者及び法人関係者等外部から報告を受けた場合，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，速やかに情報セキュリティ責任者に報告しなければならない。また，当該情報セキュリティに関する事件・事故等が法人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，報告のあった情報セキュリティに関する事件・事故等について，神戸市等の関係機関に必要な連絡を行うとともに，情報責任者に報告しなければならない。

エ　業務システム管理者は，報告のあった情報セキュリティに関する事件・事故等について，必要に応じて，業務システム責任者に報告しなければならない。

オ　情報セキュリティ責任者は，報告のあった情報セキュリティに関する事件・事故等について，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。

6.3.2　事故等の分析・記録等

ア　情報セキュリティに関する事件・事故等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，基盤情報管理者と連携し，当該情報セキュリティに関する事件・事故等を分析し，記録を保存しなければならない。また，情報セキュリティに関する事件・事故等の原因究明の結果から，再発防止策を検討し，必要に応じて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，情報セキュリティに関する事件・事故等の再発防止策について報告を受けたときは，その内容を確認し，再発防止策を実施するために必要な措置を指示しなければならない。

6.4 アクセスのための認証情報及びパスワードの管理

6.4.1　ＩＤカード等の管理

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ＩＤカード等の適正な管理を行わなければならない。

イ　役職員等情報取扱者は，次の事項を遵守しなければならない。

(1) ＩＤカード等は，役職員等情報取扱者間で共有しない。ただし，共有使用を目的に配布されたＩＤカード等については除く。

(2) ＩＤカード等は，カードリーダ若しくは端末のスロット等に必要な時以外は挿入しない。

(3) ＩＤカード等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等権限のある者は，通報があり次第速やかに当該ＩＤカード等を使用したアクセス等を停止する。

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，ＩＤカード等を切り替える場合，切り替え前のＩＤカード等を回収し，破砕する等復元不可能な処理を行ったうえで廃棄しなければならない。

6.4.2　ＩＤの管理

ア　役職員等情報取扱者は，他人に自己が利用しているＩＤを利用させてはならない。

イ　共用ＩＤを利用する場合は，共用ＩＤの利用者以外に利用させてはならない。

6.4.3　パスワードの管理

ア　役職員等情報取扱者は，自己のパスワードに関し，次の事項を遵守しなければならない。

(1) パスワードは秘密にし，パスワードの照会等には一切応じない。

(2) 情報システム又はパスワード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，パスワー

ドを速やかに変更する。

(3) パスワードを記載したメモを作成する場合は，特定の場所に施錠して保存する等により，他人が容易に見ることができない措置をする。

(4) パスワードは十分な長さ（原則として８文字以上）とし，文字列は想像しにくいもの（英数字（大文字・小文字区別有），記号を組み合わせたものなど）とする。

(5) 複数の情報システムを扱う場合は，同一のパスワードを複数のシステムで用いない。

(6) 仮のパスワードは，最初のログイン時点で変更する。

(7) パーソナルコンピュータ等のパスワードの記憶機能を利用しない。

(8) 役職員等情報取扱者の間で共有利用の場合を除いてパスワードを共有しない。

イ　情報基盤管理者及び業務システム管理者は，パスワードの照会等には一切応じてはならない。

6.5 外部委託に関する管理

6.5.1　委託先事業者の選定

特定個人情報を扱う業務又はネットワーク及び情報システムの開発・保守並びに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，委託先の選定にあたり，委託内容に応じた情報セキュリティ対策の実施が確保されることを確認しなければならない。

6.5.2　契約書の記載事項

ア　特定個人情報を扱う業務又はネットワーク及び情報システムの開発・保守並びに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) 委託業務終了時の資産の返還，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) 事故時等の公表に関する事項

(11) 委託先の責任者，委託内容，作業者，作業場所の特定に関する事項

(12) 委託先の責任者及び従事者に対する研修の実施に関する事項

(13) 情報セキュリティ確保への取り組みの実施状況に係る報告義務に関する事項

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，盗難，不正コピー等の防止に関する事項

6.5.3　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，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等について定期的若しくは随時，調査を行い，安全を確保しなければならない。情報セキュリティ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。

6.5.4　再委託等

再委託（再々委託を含む）を受ける事業者がある場合，6.5.2 及び 6.5.3 に定める事項は再委託（再々委託を含む）を受ける事業者にも適用する。

7　技術的セキュリティ

7.1 コンピュータ及びネットワークの管理

7.1.1　データの保存

対策基準の対象となるデータの保存については，暗号化などの措置を施して保存を行わなければならない。

7.1.2　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　役員，職員及び派遣労働者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，役員，職員及び派遣労働者に周知しなければならない。

イ　特定の役員，特定の職員及び派遣労働者のみが取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。

7.1.3　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。

7.1.4　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。

7.1.5　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。

7.1.6　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，情報セキュリティ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。

7.1.7　通信回線によるデータの送信

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，送信するデータを必要最小限にする等データの保護のために適切な措置を講じなければならない。

7.1.8　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・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。

7.1.9　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，なりすまし防止などの観点から，可能な限り「ac. jp」ドメインを利用したり，ドメイン変更時に旧ドメインを一定期間保有したりするなど，ドメインを適切に設定し，管理しなければならない。

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など適切な管理をしなければならない。

7.1.10　無線ＬＡＮの利用

役職員等情報取扱者は，法人にかかるネットワーク（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う場合は，接続の機密性，安全性等について強固に対策を施すものとし，情報基盤管理者が事前にその機密性，安全性について十分に行われていることの確認をとらなければならない。

7.1.11　無許可ソフトウェアの導入等の禁止

ア　役職員等情報取扱者は，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。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については，情報基盤管理者の許可を得た場合に限り，利用することができる。

イ　役職員等情報取扱者は，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本学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。

7.1.12　ネットワーク機器構成の変更の禁止

役職員等情報取扱者は，ネットワークに関する機器の接続，増設又は改造を行ってはならない。軽微な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。

7.1.13　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セキュリティ責任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，情報セキュリティ責任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。

7.1.14　電子署名・暗号化

ア　役職員等情報取扱者は，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，情報基盤管理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　役職員等情報取扱者は，暗号化を行う場合に情報基盤管理者が定める以外の方法を用いてはならない。また，情報基盤管理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　情報基盤管理者は，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。

7.1.15　無許可端末の接続禁止

役職員等情報取扱者は，情報基盤管理者等権限のある者の許可なく端末等をネットワークに接続してはならない。

7.1.16　利用可能なネットワークプロトコル

役職員等情報取扱者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。

7.1.17　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，役職員等情報取扱者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。

7.2 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，所管するネットワーク又はシステムにおいて，次の事項を実施しなければならない。

7.2.1　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。

7.2.2　利用者登録

ア　情報基盤管理者及び業務システム管理者は，以下に記す行為等について，定められた方法に従って行わなければならない。

(1) 利用者の登録，変更，抹消

(2) 登録した情報資産の管理

(3) 異動，出向，退職時における利用者ＩＤの取扱い

必要な利用者登録・変更・抹消は，情報基盤管理者及び業務システム管理者に対する申請により行う。ただし，共有使用を目的に配布されたＩＤ等については除く。

イ　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ＩＤが放置されないよう，点検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，ＩＤ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。

7.2.3　特権管理等

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ＩＤを利用する者を必要最小限にし，当該ＩＤのパスワードの漏えい等が発生しないよう，当該ＩＤ及びパスワード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，情報セキュリティ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ＩＤ及びパスワードの変更について，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ＩＤ及びパスワードについて，役職員等情報取扱者の端末等のパスワード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。

7.2.4　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。

7.2.5　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。

7.2.6　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。

7.2.7　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，必要最低限のものかつ接続の機密性，安全性等について強固に対策を施した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　情報基盤管理者及び業務システム管理者は，学外で利用する端末を役職員等情報取扱者に貸与する場合，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。

7.2.8　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，あらかじめ接続先の内部ネットワークの管理者と協議し，以下の内容を確認したうえで，接続しなければならない。

ア　接続によりそれぞれの情報資産に影響が生じないこと

イ　接続した場合のそれぞれの情報システムの責任範囲

ウ　障害発生時の対応体制

7.2.9　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，本学の情報資産に影響が生じないことを確認したうえで，情報セキュリティ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本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。

7.2.10　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。

7.2.11　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。

7.2.12　パスワードに関する情報の管理

ア　情報基盤管理者及び業務システム管理者は，役職員等情報取扱者のパスワード

に関する情報を厳重に管理しなければならない。また，役職員等情報取扱者のパスワードを発行する場合において，仮のパスワードを発行する場合，ログイン後直ちに仮のパスワードを変更させなければならない。

イ　情報基盤管理者及び業務システム管理者は，パスワードファイルを不正利用から保護するため，オペレーティングシステム等でパスワード設定のセキュリティ強化機能がある場合は，必要に応じこれを活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，仮のパスワードも含めパスワードを発行する場合，パスワードは十分な長さ（原則として８文字以上）とし，文字列は想像しにくいもの（英数字（大文字・小文字区別有），記号を組み合わせたものなど）としなければならない。

7.3 システム開発，導入，保守等

7.3.1 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，機器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　情報責任者は，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，法人情報システム台帳を作成し，整理する。

エ　業務システム管理者は，法人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，情報セキュリティ責任者からの求めに応じて，報告しなければならない。

7.3.2 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責任者は，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) 機器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

(12) 情報システムセキュリティ実施手順書等の整備

イ　情報基盤管理者及び業務システム責任者は，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。

7.3.3　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，情報セキュリティ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一定期間厳重に管理しなければならない。

7.3.4　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。

7.3.5　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。

7.3.6　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。

7.3.7　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，互いにその作業を確認する，又は法人職員の立ち会い確認のもとで作業を行わなければならない。

7.3.8　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。

7.4 コンピュータウイルス等不正プログラム対策

7.4.1　情報セキュリティ責任者の実施事項

情報セキュリティ責任者は，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役職員等情報取扱者に対する注意喚起を行う。

イ　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。

7.4.2　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，必要に応じて，次の事項を実施するものとする。

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，役職員等情報取扱者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。インターネットに接続していないシステムにおいても，定期的に当該ソフトウェア及び定義ファイルの更新を行う。

7.4.3　役職員等情報取扱者の遵守事項

役職員等情報取扱者は，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，情報基盤管理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　端末に対して，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恐れがある場合は，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　端末には，業務に必要なソフトウェアのみをインストールするとともに，端末に導入されているソフトウェアについて，情報基盤管理者等から最新版へのアップデートの指示等があったときは，速やかにその指示に従う。

7.4.4　専門家の支援体制

情報セキュリティ責任者は，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，コンピュータウイルス等対策ソフトのサポート契約を締結する等，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。

7.5 不正アクセス対策

7.5.1 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，所管するシステムにおいて，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　不正アクセスによるデータの書換えを検出する等，Ｗｅｂサイトの改ざんを防止する。

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。

7.5.2 攻撃の予告等への措置

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，警察・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。

7.5.3 記録の保存

情報セキュリティ最高責任者および情報セキュリティ責任者は，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，警察・関係機関との緊密な連携に努めなければならない。

7.5.4 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，学内の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。

7.5.5 役職員等による不正アクセス時の措置

役職員等情報取扱者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求めなければならない。

7.5.6 サービス不能攻撃

情報基盤管理者及び業務システム管理者は，外部からアクセスできる情報システムに対して，第三者からサービス不能攻撃を受け，利用者がサービスを利用でなくなることを防止するため,情報システムの可用性を確保する対策に努めなければならない。

7.5.7 標的型攻撃

情報基盤管理者及び業務システム管理者は，情報システムにおいて，標的型攻撃による内部への侵入を防止するために，研修・啓発や自動再生無効化等の人的対策・入口対策を講じたり，内部に侵入した攻撃を早期検知して対処するために，通信をチェックするなどの内部対策を講じたりするよう，努めなければならない。

7.6 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。

8 運用面のセキュリティ

8.1 情報システムの監視

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，次の事項を実施しなければならない。

8.1.1 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。

8.1.2 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。

8.1.3 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。

8.2 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情報セキュリティ責任者に報告しなければならない。情報セキュリティ責任者は，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。

8.3 運用管理における留意点

8.3.1 調査権限

情報セキュリティ責任者は，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，パーソナルコンピュータ，記録媒体，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教職員を指名する。

8.3.2 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，役職員等情報取扱者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。

8.3.3 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。

8.3.4　役職員等の報告義務

ア　役職員等情報取扱者は，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，直ちに情報セキュリティ責任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情報セキュリティ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。

8.4 緊急時の対応

8.4.1　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責任者は，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。

8.4.2　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

8.4.3　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責任者は，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。

8.5 例外措置

8.5.1　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，法人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，情報セキュリティ責任者が，軽微な例外措置と判断したものについては，情報セキュリティ責任者の許可をもって，例外措置を取ることができる。

8.5.2　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，法人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情報セキュリティ責任者に報告しなければならない。

8.5.3　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。

9　情報セキュリティ個別基準の策定

情報セキュリティ責任者は，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。

10 情報セキュリティ実施手順の策定

情報セキュリティ責任者及び業務システム責任者は，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策定しなければならない。

11 情報セキュリティポリシー等に関する違反に対する対応

11.1 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役員，職員及びパート職員等並びにその監督責任者は，その重大性，発生した事象の状況等に応じて，法人の懲戒規程による懲戒処分の対象となる。

11.2 再発防止の指導等

役職員等情報取扱者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。

11.2.1　再発防止の指導その他適切な措置

当該役職員等情報取扱者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。

11.2.2　使用権の停止・剥奪

指導等によっても改善されない場合，当該役職員等情報取扱者の情報資産の使用権を停止あるいは剥奪する。

11.2.3　報告

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責任者に報告する。

12 評価・改善

12.1 自己点検

12.1.1　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。

12.1.2　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，情報セキュリティ責任者に報告しなければならない。

イ　情報セキュリティ責任者は，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，情報管理委員会はこれを審議したうえで，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。

12.1.3　自己点検結果の活用

ア　役職員等情報取扱者は，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。

12.2 監査

12.2.1　実施方法

情報セキュリティ最高責任者は，情報セキュリティ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自己点検を行ったうえで，定期的および必要に応じて監査を行わせなければならない。

12.2.2　監査を行う者の要件

ア　情報セキュリティ監査統括責任者は，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。

12.2.3　監査実施計画の策定及び実施への協力

ア　情報セキュリティ監査統括責任者は，監査を行うに当たって，監査実施計画を策定し，情報管理委員会はこれを審議したうえで，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　被監査部門は，監査の実施に協力しなければならない。

12.2.4　委託先事業者に対する監査

情報セキュリティ監査統括責任者は，委託先事業者に対して，委託先事業者からの再委託（再々委託を含む）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。

12.2.5　監査結果の報告

情報セキュリティ監査統括責任者は，監査結果を取りまとめ，情報管理委員会はこれを審議したうえで，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。

12.2.6　監査調書等の保管

情報セキュリティ監査統括責任者は，監査の実施を通して収集した監査証拠，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。

12.2.7　指摘事項への対処

情報セキュリティ責任者は，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。

12.2.8　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。

12.3 改善

12.3.1　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，学生，保護者及び法人関係者等からの指摘による問題，自己点検及び監査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。

12.3.2　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事件・事故，自己点検及び監査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。

12.4 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，自己点検及び監査の結果，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。