花園大学情報セキュリティポリシー

2020（令和２）年４月１日　制定

第１章　情報セキュリティの基本方針

（目的）

第１条　花園大学（以下「本学」という。）において、情報資産は教育・研究活動を推進する上で重要な資産である。情報資産が守られなければ、本学の教育・研究活動の停滞、本学に対する社会的な信頼の喪失などの被害を受ける可能性が出てくる。したがって、「hunet（花園大学学術情報ネットワーク）」が提供するサービスを利用する者が、情報資産を適切且つ厳密に管理運用するため、情報セキュリティポリシー（以下「ポリシー」という。）を定め、情報セキュリティの重要性への理解を促進するものである。

（基本方針）

第２条　前条の目的を達成するため、本学情報システム（以下「情報システム」という。）は、円滑で効果的な情報流通を図るために、以下に定めるポリシーにより、優れた秩序と安全性をもって安定的且つ効率的に運用され、全学に供用される。

（定義）

第３条　本ポリシーにおいて、次の各号に掲げる用語の定義は、当該各号に定めるところによる。

（１）情報システム

情報処理および情報ネットワークにかかわるシステムで、本学により、所有または管理されているもの、本学との契約あるいは他の協定に従って提供されるものをいう。

（２）情報ネットワーク

本学により、所有または管理されている全ての情報ネットワークおよび、本学との契約あるいは他の協定に従って提供される全ての情報ネットワークをいう。

（３）情報資産

情報システム内部に記録された情報、情報システム外部の電磁的記録媒体に記録された情報、情報システムに関係がある書面に記載された情報をいう。

（４）情報機器

コンピュータ、タブレット端末、スマートフォン等をいう。

（５）要保護情報

機密情報や個人情報など、漏洩や滅失、毀損、改竄等によって個人の権利侵害や大学の信用の失墜などの問題が発生することが予想されることから、何らかの保護が必要とされる情報をいう。

（６）情報セキュリティ

情報資産の機密性、完全性および可用性を維持することをいう。

（７）各部署の管理対象情報システム

本学情報システムの内、各部署が運用責任を持つ情報システムをいう。

（８）利用者

本学の教職員（非常勤講師、派遣職員、委託職員、アルバイト等を含む。）（以下「教職員等」という。）、学部生、大学院生（以下「学生」という。）、研究員、研究生、研修生、科目等履修生、別科生、その他情報システムセンター長（以下、「センター長」という。）が許可したものをいう。

（９）アカウント

本学情報システムの利用に当たって用いる認証情報をいう。

（10）インシデント

情報セキュリティに関し、故障を含む意図的または偶発的に生じる事故や事件、本学規程または法令に反して発生させた事故あるいは事件をいう。

（対象範囲）

第４条　本ポリシーの対象は本学の情報システムの利用者、本学の情報システムを利用する委託業者、および本学が情報セキュリティの遵守が必要と認めた者とする。

第２章　組織体制

（総括情報責任者）

第５条　情報システムの運用に関する権限と責任を持ち、情報システムに関する業務を大学運営の面から意思決定・判断し、統括的に管理・執行するため、総括情報責任者を置き、学長をもって充てる。

２　学長が出張等により不在の場合および学長に事故がある場合は、事務局長が業務を代行する。

（管理運営部局）

第６条　本学における情報システムの運用および管理ならびに情報セキュリティ対策の推進に関して、その管理運営にあたる部署は、情報システムセンターとする。

２　情報システムセンターは、以下の各号に定める事務を行う。

（１）情報システムおよび情報ネットワークに対する管理、運用およびセキュリティ対策の実施

（２）情報システムの運用と利用におけるポリシーの実施状況の取りまとめ

（３）教育・研修計画、リスク管理および非常時行動計画等の実施状況の取りまとめ

（４）情報システムのセキュリティに関する連絡と通報

（５）情報化委員会の運営に関する事務

（運用実施管理責任者）

第７条　運用実施管理責任者（以下「実施管理責任者」という。）を置き、センター長をその任に充てる。

2　実施管理責任者は、大学全体の情報システムおよびセキュリティのあり方、情報システムの運用計画の立案、運用管理指標の設定等に関する業務を行い、学内情報ネットワークおよび、それに接続される情報システムおよび情報機器の管理・セキュリティに関する運用管理業務を行う。

（部局運用管理責任者）

第 8 条　部局に部局運用管理責任者を置き、実施管理責任者がこれを統括する。

2　部局運用管理責任者は、各部長をその任に充てる。

3　部局運用管理責任者は、各部局の管理対象範囲の情報システムおよび情報機器等のセキュリティを総括する。

（情報運用担当者）

第 9 条　情報運用担当者（以下「運用担当者という。）を置き、情報システムセンター課員をその任に充てる。

2　運用担当者は、本ポリシーに従い学内情報ネットワークおよび、それに接続される情報システムおよび情報機器の運用・セキュリティ対策を実施する責任を有する。

（部局情報運用担当者）

第 10 条　部局の各課に部局情報運用担当者を置き、各課長をその任に充てる。

2　部局情報運用担当者は本ポリシーに従い、当該課の利用者にその運用を守らせる責任を負うと共に、利用状況について点検を行う。また、管理対象範囲の情報システムおよび情報機器等のセキュリティを維持・管理する。

第 3 章　情報システム運用規則

（情報の格付けと取扱い）

第 11 条　教職員等は、情報システムに係る情報を作成または入手する場合は、本学の教育・研究、事務の遂行の目的に十分留意すること。

2　教職員等は、情報の作成時あるいは学外の者が作成した情報を入手し管理を開始する場合に、当該情報の機密性、完全性、可用性に応じて格付けを行ない、あわせて取扱制限の必要性の有無を検討すること。

3　教職員等は、情報の格付けを当該情報の参照が許されている者が認識できる方法を用いて明示すること。

4　前項において、取扱制限が必要な情報に関しては「回収資料」、「配布・送信禁止」、「複製禁止」、「印刷禁止」、「転送禁止」、「書換禁止」、「削除禁止」、「要暗号化」、「要アクセス制限」等の制限を明示すること。

5　教職員等は原則として要保護情報を電子メールで移送してはならない。移送が必要な場合には当該情報に暗号化やパスワード制限、書換制限などを設けること。

6　各部署は当該部署に関連する保存された要保護情報について、取扱制限および保護対策を明示し、それらを利用者に守らせること。

7　派遣社員等を含む非正規の教職員に対し、学外での要保護情報の処理を行うことを禁止する。なお、業務の遂行において止むを得ず必要な場合には、必要最小限の情報処理にとどめると共に、事前に当該部局運用管理責任者の許可を得ること。

8　実施管理責任者は、要保護情報である電磁的記録のバックアップまたは重要な設計書の複写の保管について、災害等への対策の必要性を検討し、必要があると認めたときは、同時被災等しないための適切な措置を講ずること。

（情報資産の管理）

第 12 条　実施管理責任者は、要保護情報を取り扱う情報システムについては、通信回線を用い送受信される要保護情報の暗号化を行う必要性の有無を検討し、必要があると認めたときは情報を暗号化すること。

2　実施管理責任者は情報システムの運用を終了する場合には、システムに保存されている全ての情報を復元が困難な状態にすること。

3　各部署がファイル共有のために利用する共有フォルダーには、共有が必要とされる情報のみを掲載し、利用者を限定する場合には情報ファイルにアクセス制限を設けること。

4　前項の共有フォルダー利用者は、フォルダー内情報の作成日時、作成者、バージョン等が利用者にわかるように明示し、不要となった情報は速やかに廃棄すること。

5　毎年、共有フォルダー内の情報に対してその必要性を検証し、保存が必要とされず、且つ原則 1 年間アクセスのない情報は廃棄すること。

（要保護情報）

第 13 条　情報の提供を求める場合は、求める情報の範囲、利用の目的、その情報が伝達される範囲を、あらかじめ相手方に示さなければならない。

2　前項が個人情報である場合には、当人より請求があった場合、開示、訂正または削除をしなければならない。また、そのための手続を示さなければならない。なお、訂正または削除において、その請求がその後の業務遂行に正当なものかどうか判断しなければならない。

3　個人情報などの要保護情報を学外コンピュータへ保存、もしくは可搬型メモリーに保存して持ち歩くことを禁止する。但し、業務上止むを得ない場合には、情報への暗号化、パスワード保護、あるいはアクセス制御が可能な可搬型メモリーの利用、外部での作業中の覗き見防止等を行うこと。

4　要保護情報を保存した電子媒体および印刷物の廃棄は、裁断などの方法により、情報の復元が困難な状態にすること。

5　利用者等が保有する情報は、ネットワーク運用に不可欠な範囲またはインシデント対応に不可欠な範囲において、閲覧、複製または提供することができる。

6　個人情報の取り扱いについては、別途「花園大学個人情報の保護に関する規程」に定める。

（アクセス制御）

第 14 条　実施管理責任者は、利用者が要保護情報を扱う情報システムにログインする場合、主体認証を

行えるようなシステムを構成すること。

2　実施管理責任者は、通信回線を経由してサーバ装置にアクセスして保守作業を行う場合は、暗号化を行う必要性の有無を検討し、必要があると認めたときには情報を暗号化すること。

3　各部署の管理対象情報システムにおけるアカウント管理は部局情報運用担当者が行い、利用者のアカウント管理が情報システムセンターで管理されているものにおいては、業務または業務上の責務に即してアカウントが必要と判断された場合には、その利用申請を情報システムセンターに文書で提出すること。また、アカウントに応じたアクセス制限が必要な場合には、その内容を情報システムセンターに依頼すること。

（アカウント管理）

第 15 条　実施管理責任者はアカウント管理を行う必要があると認めた情報システムにおいて、管理者権限を持つアカウントを、業務または業務上の責務に即した場合に限定して付与すること。

2　実施管理責任者は、セキュリティ侵害またはその可能性が認められる場合、利用者に主体認証情報（パスワード）の変更を求め、またはアカウントを失効させることができる。

3　実施管理責任者は、発行済のアカウントについて、次号に掲げる項目を随時確認し、停止が必要と判断されたときは、速やかにそのアカウントを停止すること。

(１)利用資格を失ったもの

(２)当該アカウントを必要とする情報システムの利用が必要なくなったもの

4　利用者は情報システムのアクセスに必要な自分の主体認証となるユーザ ID およびパスワードを第三者に貸与、譲渡、漏えいしてはならない。また、それらが容易に目に付く場所に表示するなどして、意図せずに使われることがないよう管理すること。

5　アカウントは利用者別に異なるものを付与すること。

6　全ての利用者は他者のアカウントを使って情報システムにアクセスしてはならない。

7　部局情報運用担当者は、当該部署が管理する利用者がポリシーに則ってアカウントを利用するよう管理する責任を有する。

8　部局情報運用担当者は、利用する教職員等に変更が生じた場合には、速やかに変更内容を情報システムセンターに文書で伝え、アカウントの抹消依頼、変更依頼、新規作成依頼等を行う。

9　部課メールなど、同じメールアドレスを複数の利用者が使っている場合には、利用者に変更があった時点で、当該課の部局情報運用担当者はメールアクセスのパスワードを変更しなければならない。

（アカウント交付申請）

第 16 条　利用希望者は、「hunet（花園大学学術情報ネットワーク）利用申請書」を情報システムセンターに提出し、実施管理責任者からアカウントの交付を得なければならない。

2　本学の教職員等、学生、研究員、研究生、研修生、科目等履修生、別科生は、就任時や入学時等にアカウントの交付を得る場合の申請を不要とする。

（アカウントの有効期限）

第 17 条　本学の教職員等、学生、研究員、研究生、研修生、科目等履修生、別科生のアカウントの有効

期限は、在職期間、委嘱期間または在学期間とする。

2　実施管理責任者が許可した者についてはその必要期間に限定するものとする。

（サーバ装置の対策）

第 18 条　情報システムセンターは、要保護情報を取り扱うサーバ装置に保存されている情報について、定期的にバックアップを取得すること。また、取得した情報を記録した媒体は、安全に管理すること。

2　情報システムセンターは、サーバ装置の運用管理について、作業日、作業を行なったサーバ装置、作業内容および作業者を含む内容を記録すること。

（セキュリティホール対策）

第 19 条　実施管理責任者は、情報システムに関する脆弱性の診断を定期的に実施し、セキュリティの維持に努めること。

2　実施管理責任者は、情報システムについて、セキュリティホール対策が必要となる機器情報を収集し、当該機器上で利用するソフトウェアに関連する公開されたセキュリティ対策を実施すること。

（不正プログラム対策）

第 20 条　実施管理責任者は、不正プログラムから情報システムを保護するため、アンチウイルスソフトウェアを導入する等の対策を実施すること。

2　学生が利用することを前提に学内に設置したコンピュータでは、プログラムのネットワークからのダウンロードやインストールにより、セキュリティの侵害が起こらないように、コンピュータにソフトウェアのインストール権限の設定を行うこと。

3　学生が利用することを前提に学内に設置したコンピュータでは、再起動することにより、利用開始時の初期状態に戻るように設定を行うこと。

4　教職員等は大学のネットワークに接続する情報機器にプログラムをダウンロードする場合には、セキュリティ面からプログラムの信頼性を確認し、情報システムセンターに申請の上、細心の注意を払って行うこと。

（証跡管理）

第 21 条　利用者等によるネットワークを通じて行われる通信の傍受を禁止する。但し、実施管理責任者は、セキュリティ確保のため、あらかじめ指定した者にネットワークを通じて行われる通信の監視（以下「監視」という。）を行わせることができる。なお「監視」を指定された者については、その者が判明できる情報を公表してはならない。

2　不正アクセス行為またはこれに類する重大なセキュリティ侵害に対処するために、特に必要と認められる場合、実施管理責任者は、セキュリティ侵害の緊急性、内容および程度に応じて、対処のために不可欠と認められる情報については、指定した者以外においても、監視を行うよう命ずることができる。

3　監視を行う者は、監視によって知り得た通信の内容は、実施管理責任者、および伝達を認められた

者以外に公表してはならない。

4　実施管理責任者は、監視を行う者に対して、監視記録を保存する期間をあらかじめ指示するものとする。監視を行う者は、指示された期間を経過した監視記録は直ちに破棄しなければならない。但し、監視記録から個人情報に係る部分を削除して、ネットワーク運用・管理のための資料とすることができる。資料は、体系的に整理し、常に活用できるよう保存することが望ましい。

5　監視を行う者および監視記録の報告を受けた者は、ネットワーク運用・管理のために必要な限りにおいて、これを閲覧且つ保存することができる。なお、上記以外の者については、実施管理責任者の許可なく閲覧してはならない。

6　不必要となった監視記録は、直ちに破棄しなければならない。監視記録の内容を、法令に基く場合等を除き、他の者に公表してはならない。

7　報告を受けた通信情報については、実施管理責任者は、総括情報責任者に報告すると同時に情報化委員会へ報告するものとする。

（学外の情報機器の学内への持込み）

第 22 条　利用者は学外の情報機器を本学ネットワークに接続する場合には、事前に実施管理責任者の許可を得なければならない。

2　前項の情報機器は、事前にアンチウイルス対策ソフトが最新の状態でインストールされていなければならない。

3　教職員等は、独自に学内に無線 LAN アクセスポイントを設ける場合には、回線速度への悪影響を及ぼすことがあることから、事前に実施管理責任者に設置許可を申請すること。

（インシデント対応）

第 23 条　実施管理責任者は、情報セキュリティに関するインシデントが発生した場合、被害の拡大を防ぐとともに、インシデントから復旧するための体制を整備すること。

2　実施管理責任者は、インシデントが発生した際の対応手順を整備すること。

3　実施管理責任者は、インシデントに備え本学の教育・研究、事務の遂行のため特に重要と認めた情報システムについて、各部署の部署長の緊急連絡先、連絡手段、連絡内容を含む緊急連絡網を整備すること。

4　実施管理責任者は、インシデントが発生した場合には、インシデントの原因を調査し再発防止策を策定し、その結果を報告書として総括情報責任者に報告すること。

（利用記録）

第 24 条　複数の者が利用する情報機器の管理者は、当該機器に係る利用記録をあらかじめ定めた目的の範囲でのみ採取することができる。当該目的との関連で必要性の認められない利用記録を採取することはできない。

（外部委託管理）

第 25 条　実施管理責任者は、情報システムの運用業務のすべてまたはその一部を第三者に委託する場合

には、当該第三者による情報セキュリティの確保が徹底されるよう必要な措置を講じるものとする。

2　外部委託契約を行う場合は、委託先に請け負わせる業務の情報セキュリティ対策、機密保持（情報の目的外利用の禁止を含む)、情報セキュリティ侵害発生時の対処手順および情報セキュリティ対策の履行が不十分である場合の対処手順を含み、それらを充分に確認した上で、委託契約を取り交わすこと。

3　原則として、委託先がその請負内容の全部または一部を第三者に再請負させることを禁止すること。但し、委託先からの申請を受け、再請負させることにより生ずる脅威に対し、情報セキュリティが十分に確保される措置が担保されると部局運用管理責任者が判断する場合は、その限りではない。

4　委託先に提供する情報を必要最低限とし、委託先が要保護情報を取り扱う場合、以下の実施手順に従うこと。

（１)委託先に情報を移送する場合は、不要部分のマスキングや暗号化等、安全な受渡方法により実施し、移送した記録を保存すること。

（２)外部委託の業務終了等により情報が不要になった場合には、直ちに返却させるか、廃棄させること。

（利用者管理）

第 26 条　情報システム利用者に変更が生じた場合には、当該利用者を管理する部局運用管理責任者は変更の内容を遅滞なく情報システムセンターに文書で連絡すること。

2　実施管理責任者は、情報システムの利用者を特定するための文書および利用者データベースに変更内容を反映すること。また、当該変更の記録を保存すること。

（ウェブの利用および公開）

第 27 条　利用者は、ウェブブラウザを利用したウェブサイトの閲覧、情報の受信、ファイルのダウンロード等を行う際には、不正プログラムの感染、情報の漏えい、誤った相手への情報の送信等に注意するだけでなく、業務時間中における私的目的でのウェブの閲覧、掲示板への無断書き込み、その他業務効率を低下させたり本学の社会的信用を失墜させることのないよう注意しなければならない。

2　利用者は、担当部局運用管理責任者に許可を得た場合に、ウェブページを作成し、公開することができる。ウェブページの公開にあたって、「花園大学ソーシャルメディアガイドライン」を遵守し、セキュリティや著作権等の問題および本学の社会的信用を失墜させることのないように配慮しなければならない。

3　教員は、研究室等でウェブサーバを運用しようとする場合は、事前に実施管理責任者に申請し、許可を得なければならない。ウェブでの公開に関しては前項に準じる。

（安全管理義務）

第28条　利用者は、自己の管理するコンピュータについて、情報ネットワークとの接続状況に関わらず、

安全性を維持する一次的な担当者となることに留意し、次の各号に定めるように、悪意あるプログラムを導入しないように注意しなければならない。

(1)アンチウイルス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せず、データファイルをアプリケーション等で読み込まないこと。

(2)アンチウイルスソフトウェア等にかかわるアプリケーションおよび不正プログラム定義ファイル等について、これを常に最新の状態に維持すること。

(3)アンチウイルスソフトウェア等による不正プログラムの自動検査機能を有効にしなければならない。

(4)アンチウイルスソフトウェア等により定期的にすべての電子ファイルに対して、不正プログラムの有無を確認すること。

(5)外部からデータやソフトウェアをコンピュータ等に取り込む場合または外部にデータやソフトウェアを提供する場合、不正プログラム感染の有無を確認すること。

(6)ソフトウェアのセキュリティ機能を活用し、不正プログラム感染の予防に努めること。

2　利用者は自己が管理する情報機器に不正プログラム感染が発見されたときには、すぐにネットワークから当該機器を切り離し、ネットワークを介した他のシステムへの影響を防ぐこと。

3　利用者は可搬型メモリー内の不正プログラム感染チェックを随時行い、セキュリティを維持すること。また感染が発見された場合にはそれを削除するか、当該メモリーの使用を止めること。

4　利用者は、本学情報ネットワークおよびシステムの利用に際して、インシデントを発見したときは、当該システムを管理する部局運用管理責任者もしくは実施管理責任者にその内容を報告しなければならない。

5　利用者は、本ポリシー、関連規程および各種内規等を遵守しなければならない。

（禁止事項）

第29条　利用者は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)当該情報システムおよび情報について定められた目的以外の利用

(2)差別、名誉毀損、侮辱、ハラスメントにあたる情報の発信

(3)個人情報やプライバシーを侵害する情報の発信

(4)守秘義務に違反する情報の発信

(5)著作権等の財産権を侵害する情報の発信

(6)通信の秘密を侵害する行為

(7)営業ないし商業を目的とした本学情報システムの利用

(8)部局管理運用責任者の許可（業務上の正当事由）なくネットワーク上の通信を監視し、または情報機器の利用情報を取得する行為

(9)「不正アクセス禁止法」に定められたアクセス制御を免れる行為、またはこれに類する行為

(10) 部局管理運用責任者の要請に基かずに管理権限のないシステムのセキュリティ上の脆弱性を検知する行為

(11)過度な負荷等により本学の円滑な情報システムの運用を妨げる行為

(12)その他法令に基く処罰の対象となりまたは損害賠償等の民事責任を発生させる情報の発信

(13)上記の行為を助長する行為
(14)実施管理責任者の許可をえずソフトウェアのインストールやコンピュータの設定の変更を行う行為
2　利用者は、ファイルの自動公衆送信機能を持った P2P ソフトウェア（ファイル共有ソフト）については、教育・研究目的以外にこれを利用してはならない。このような P2P ソフトウェアを教育・研究目的に利用する場合は実施管理責任者の許可を得なければならない。

（違反と例外措置）
第 30 条　利用が前条に掲げる事項に違反すると認められた場合、部局運用管理責任者は速やかに調査を行い、事実を確認するものとする。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しなければならない。
2　部局運用管理責任者は、上記の措置を講じたときは、遅滞無く実施管理責任者にその旨を報告しなければならない。
3　実施管理責任者は、調査によって違反行為が判明したときには、次の各号に掲げる措置を講ずることができる。
(1)行為者に対する当該行為の中止命令
(2)当該行為に係る情報発信の遮断命令
(3)当該行為者のアカウント停止命令、または抹消命令
(4)総括情報責任者への報告
(5)その他法令に基く措置
4　実施管理責任者は、前項第 1 号から第 3 号については、当該行為者の部局運用管理責任者を通じて同等の措置を依頼することができる。
5　実施管理責任者は、情報セキュリティ関係規程への重大な違反の報告を受けた場合および自らが重大な違反を知った場合および上記の措置を講じた場合は、遅滞無く総括情報責任者にその旨を報告すること。

（情報システムの利用制限）
第 31 条　実施管理責任者は、次の場合、情報システムの全部または一部の利用を制限することがある。
(1)保守・点検作業
(2)事故または障害発生時
(3)緊急の処理が必要な場合
(4)天災等やむを得ぬ事態が生じた場合
2　利用を制限する場合は、実施管理責任者が決裁し、システム上で事前に周知する。但し、緊急やむを得ない場合は、この限りではない。

（利用者に対する利用停止）
第 32 条　実施管理責任者は、利用者が次のいずれかに該当する場合には、当該利用者による情報システ

ムの利用の停止を行うことがある。

(1)本ポリシーに違反した場合

(2)前号の他、本ポリシーの義務を怠り、または怠る恐れがある場合

(3)適正利用のための指導に従わない場合

2　実施管理責任者は、前項の規定により情報システムの利用を停止する時は、あらかじめその理由、利用停止する日および期間または停止を解除する条件を利用者に通知する。但し、緊急やむを得ない場合は、この限りではない。

（他ネット接続）

第 33 条　情報システムの取扱いに関しては、外国の法令、国内外の電気通信事業者等が定める契約約款等により制限されることがある。

2　利用者が国内外の他のネットワークを経由して通信を行う場合、利用者は、経由するすべての国の法令等、通信業者の約款等およびすべてのネットワークの規則に従うものとする。

（情報システムの変更、追加または廃止）

第 34 条　実施管理責任者は、情報システムの全部または一部を変更、追加または廃止することがある。

2　変更、追加または廃止する場合、実施管理責任者が決裁し、システム上で事前に周知する。但し、緊急やむを得ない場合は、この限りではない。

（教育・研修）

第 35 条　実施管理責任者は、本ポリシーについて、利用者に教育すべき内容を検討し、教育のための資料を整備すること。

2　実施管理責任者は、利用者に対しての情報セキュリティ対策の教育に係る計画を企画、立案するとともに、その実施体制を整備すること。

3　情報システムセンターは利用者からの情報セキュリティ対策に関する相談に対応すること。

4　部局運用管理責任者は実施管理責任者の指示により、部局の構成員に対して、情報セキュリティ対策の教育を実施すること。

（本ポリシーの改廃）

第 36 条　本ポリシーの改廃は、学長が、情報化委員会および評議会の意見を聴き、これを行う。

附則

1　本ポリシーは、2020（令和 2）年 4 月 1 日から施行する。

1　1998（平成 10）年 4 月 1 日制定の「花園大学学術情報ネットワークシステム管理・運用・利用規程」および 2002（平成 14）年 3 月 7 日制定の「「花園大学学術情報ネットワーク（hunet)」利用上のガイドライン」は、本ポリシーの施行日をもって廃止する。