学校法人文化学園　情報システム運用基本規程

（目的）

第１条　本規程は、学校法人文化学園（以下「学園」という。）における情報システムの運用及び管理について必要な事項を定め、学園の保有する情報の保護と活用及び適切な情報セキュリティ対策を図ることを目的とする。

（適用範囲）

第２条　本規程は、学園情報システムを運用及び管理するすべての者、並びに利用者及び臨時利用者に適用する。

（定義）

第３条　本規程において、次の各号に掲げる用語は、それぞれ当該各号の定めるところによる。

(1)　情報システム

情報ネットワークに接続する機器を含む、情報処理及び情報ネットワークに係るシステムで、次のものをいう。

ア　学園により、所有又は管理されているもの

イ　学園との契約又は他の協定に従って提供されるもの

(2)　情報

情報には次のものを含む。

ア　情報システム内部に記録された情報

イ　情報システム外部の電磁的記録媒体に記録された情報

ウ　情報システムに関係がある書面に記載された情報

(3)　情報資産

情報システム並びに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及び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)　学校法人文化学園情報セキュリティポリシー（以下「ポリシー」という。）

学園が定める「情報システム運用基本方針」、「情報システム運用基本規程」及び「情報セキュリティインシデント対応チーム(CSIRT)運営規程」をいう。

(5)　実施規程

ポリシーに基づいて策定される規程、基準及び計画をいう。

(6)　手順

実施規程に基づいて策定される具体的な手順、マニュアル及びガイドラインをいう。

(7)　利用者

教職員等及び学生等で、許可を受けて学園情報システムを利用する者をいう。

(8)　教職員等

学園の役員及び学園に勤務する常勤又は非常勤の教職員（派遣職員を含む）その他部局総括責任者が認めた者をいう。

(9)　学生等

各校学則に定める学生、その他部局総括責任者が認めた者をいう。

(10)　臨時利用者

教職員等及び学生等以外の者で、許可を受けて学園情報システムを臨時に利用する者をいう。

(11)　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。

(12)　電磁的記録

電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、コンピュータによる情報処理の用に供されるものをいう。

(13)　情報セキュリティインシデント

情報セキュリティに関し、意図的又は偶発的に生じる、学園規程や法律に反する事故又は事件をいう。

(14)　CSIRT

学園において発生した情報セキュリティインシデントに対処するため、学園に設置された体制をいう。Computer Security Incident Response Team の略。

(15)　明示等

情報を取り扱うすべての者が当該情報の格付けについて共通の認識となるようにする措置をいう。明示等には、情報ごとに格付けを記載することによる明示のほか、当該情報の格付けに係る認識が共通となるその他の措置も含まれる。

(16)　部局

学園における各部門をいう。

(17)　部局長

前号に定める部局の長として、学部長、グループ長、部長又はそれに相当する者をいう。

（全学総括責任者）

第４条　学園情報システムの運用に責任を持つ者として、学園に全学総括責任者を置く。理事長がこれを任命する。

２　全学総括責任者は、ポリシー及びそれに基づく規程の決定や情報システム上での各種問題に対する処置を行う。

３　全学総括責任者は、全学の情報基盤として供される学園情報システムのうち情報セキュリティが侵害された場合の影響が特に大きいと評価される情報システムを指定することができる。この指定

された情報システムを「全学情報システム」という。

4　全学総括責任者は、全学向け教育及び全学情報システムを担当する部局技術担当者向け教育を統括する。

5　全学総括責任者に事故があるときは、全学総括責任者があらかじめ指名する者が、その職務を代行する。

6　全学総括責任者は、原則として、情報セキュリティに関する専門的な知識及び経験を有した専門家を情報セキュリティアドバイザーとして置く。

（情報セキュリティ委員会）

第５条　学園情報システムの円滑な運用のための最終決定機関として、学園に情報セキュリティ委員会を置く。

2　情報セキュリティ委員会は以下を実施する。

(1)　ポリシー及び全学向け教育の実施ガイドラインの改廃

(2)　情報システムの運用と利用及び教育に係る規程及び手順の制定及び改廃

(3)　情報システムの運用と利用に関する教育の年度講習計画の制定及び改廃、並びにその計画の実施状況の把握

(4)　情報システム運用リスク管理規程の制定及び改廃、並びにその実施状況の把握

(5)　情報セキュリティ監査規程の制定及び改廃、並びにその実施

(6)　情報システム非常時行動計画の制定及び改廃、並びにその実施

(7)　情報セキュリティインシデントの再発防止策の検討及び実施

（情報セキュリティ委員会の構成員）

第６条　情報セキュリティ委員会は、全学実施責任者が必要と認める者で構成する。

（情報セキュリティ委員会の委員長）

第７条　情報セキュリティ委員会の委員長は、全学実施責任者をもって充てる。

2　委員長は、会務を総理する。

（全学実施責任者）

第８条　学園に全学実施責任者を置き、IT 戦略室室長をもって充てる。

2　全学実施責任者は、全学総括責任者の指示により、学園情報システムの整備及び運用に関し、ポリシー及びそれに基づく規程並びに手順等の実施を行う。

3　全学実施責任者は、情報システムの運用に携わる者及び利用者に対して、情報システムの運用及び利用並びに情報システムのセキュリティに関する教育を企画し、ポリシー及びそれに基づく規程並びに手順等の遵守を確実にするための教育を実施する。

４　全学実施責任者は、学園情報システムのセキュリティに関する監視と通報において学園を代表する。

（情報セキュリティ監査責任者）

第９条　全学総括責任者は、情報セキュリティ監査責任者を置くことができる。

２　情報セキュリティ監査責任者は、全学総括責任者の指示に基づき、監査に関する事務を統括する。

（管理運営部局）

第１０条　情報セキュリティ委員会は、IT 戦略室を学園情報システムの管理運営部局として定める。

（管理運営部局が行う業務）

第１１条　管理運営部局は、全学実施責任者の指示により、次に掲げる業務を行う。

⑴　情報セキュリティ委員会の運営に関する事務

⑵　学園情報システムの運用及び利用におけるポリシーの実施状況の取りまとめ

⑶　講習計画、リスク管理及び非常時行動計画等の実施状況の取りまとめ

⑷　学園情報システムのセキュリティに関する監視と通報

（部局総括責任者）

第１２条　情報セキュリティ委員会は、各部局に部局総括責任者を置き、部局長をもって充てる。

２　部局総括責任者は、情報セキュリティ委員会の指示に従い、部局における運用方針の決定や情報システム上での各種問題に対する処置を担当する。

（部局技術責任者）

第１３条　部局に部局技術責任者を置き、部局長が任命する。

２　部局技術責任者は、部局情報システムの構成の決定や技術的問題に対する処置を担当する。

３　部局技術責任者は、部局技術担当者に対して、ポリシー及びそれに基づく規程並びに手順等の遵守を確実にするための教育を実施する。

（部局技術担当者）

第１４条　部局技術責任者は、当該部局の情報システムの管理業務において必要な単位ごとに、部局技術担当者を置く。部局技術担当者は部局技術責任者が推挙し部局長が任命する。なお、部局技術責任者自ら部局技術担当者を兼務することができる。

２　部局技術担当者は、部局技術責任者の指示により、部局の情報システムの運用の技術的実務を担当し、利用者への教育を実施する。

（全学情報セキュリティアドバイザーの設置）

第１５条　全学総括責任者は、情報セキュリティについて専門的な知識及び経験を有する者を全学情報セキュリティアドバイザーとして置く。

２　全学情報セキュリティアドバイザーは、情報セキュリティ対策に係る助言又は支援を行う。

（情報セキュリティインシデントに備えた体制の整備）

第１６条　全学総括責任者は、情報セキュリティインシデントの発生時に迅速かつ円滑な対応を図るため、別途定める規程により CSIRT を設置する。

２　全学総括責任者は、情報セキュリティインシデントが発生した際、直ちに自らへの報告が行われる体制を整備する。

（役割の分離）

第１７条　情報セキュリティ対策の運用において、以下の役割を同じ者が兼務しないこと。

(1)　承認又は許可事案の申請者とその承認又は許可を行う者（以下、「承認権限者等」という。）

(2)　監査を受ける者とその監査を実施する者

２　前項の定めに係らず、教職員等は、承認権限者等が有する職務上の権限等から、当該承認権限者等が承認又は許可（以下「承認等」という。）の可否の判断を行うことが不適切と認められる場合は、当該承認権限者等の上司に承認等の申請をする。この場合において、当該承認権限者等の上司の承認等を得たときは、当該承認権限者等の承認等を得ることを要しない。

３　教職員等は、前項の場合において承認等を与えたときは、承認権限者等に係る遵守事項に準じて、措置を講ずる。

（情報の格付け）

第１８条　情報セキュリティ委員会は、情報システムで取り扱う情報について、電磁的記録については機密性、完全性及び可用性の観点から、書面については機密性の観点から当該情報の格付け及び取扱制限の指定並びに明示等の規程等を整備する。

（学外の情報セキュリティ水準の低下を招く行為の防止）

第１９条　全学実施責任者は、学外の情報セキュリティ水準の低下を招く行為の防止に関する措置についての規程等を整備する。

２　学園情報システムを運用及び管理する者、並びに利用者及び臨時利用者は、学外の情報セキュリティ水準の低下を招く行為の防止に関する措置を講ずる。

（情報システム運用の外部委託管理）

第２０条　全学総括責任者は、学園情報システムの運用業務のすべて又はその一部を第三者に委託す

る場合は、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。

（情報セキュリティ監査）

第２１条　情報セキュリティ監査責任者は、情報システムのセキュリティ対策がポリシーに基づく手順に従って実施されていることを監査する。情報セキュリティ監査に際しては、別途定める規程に従う。

（見直し）

第２２条　ポリシー、実施規程及び手順を整備した者は、見直しを行う必要性の有無を適時検討し、必要があると認めた場合は、その見直しを行う。

２　学園情報システムを運用及び管理する者、並びに利用者及び臨時利用者は、自らが実施した情報セキュリティ対策に関連する事項に課題及び問題点が認められる場合は、当該事項の見直しを行う。

（改廃）

第２３条　本規程の改廃は、所管部署に諮り、理事長が定める。

附　則

本規程は、平成 30 年 6 月 1 日から施行する。