◯佛教大学情報ネットワーク利用・運用内規

第１章　総則

（目的）

第１条　本内規は，「佛教大学情報セキュリティポリシー」に基づき，佛教大学情報ネットワーク（以下「情報ネットワーク」という。）の利用および管理・運用に関する事項を定め，情報ネットワークの保護と活用ならびに情報セキュリティの確保に資することを目的とする。

（定義）

第２条　本内規における用語については，「佛教大学情報セキュリティポリシー」に定めるところによる。その他の用語については，当該各号に定めるところによる。

(1)　接続機器
　　情報ネットワークに接続した情報機器等をいう。

(2)　周辺機器
　　プリンター，スキャナ等の接続機器に接続して使用する機器をいう。

（利用資格）

第３条　情報ネットワークを利用できる者は，「佛教大学セキュリティポリシー」に準ずる者とする。

（接続機器管理者）

第４条　接続機器については，当該接続者をもって接続機器管理者とする。

２　接続機器管理者は，当該接続機器による情報ネットワークの利用について，その管理および運用に責任を負うものとする。

３　接続機器管理者は，当該接続機器の利用に伴って生じた情報ネットワークの障害および損害について責任を負うものとする。

（接続機器に伴う費用負担）

第５条　情報ネットワークに個人の接続機器を接続するために必要な費用は，原則として接続機器管理者の負担とする。

（情報ネットワークへの接続方式）

第６条　個人の情報機器やスマートフォン等による情報ネットワークへの接続については，有線形式の DHCP 情報コンセントおよび無線形式の無線 LAN の２方式とする。

２　教員研究室が管理する無線 LAN 経由でアクセスする場合は，当該の教員が管理する無線 LAN 用 SSID ならびに暗号化キーを用いるものとする。

（遵守事項）

第７条　接続機器管理者は，以下の事項を遵守しなければならない。

(1) 機密情報（試験問題・成績データ・個人データなど）を有する端末は極力接続しないようにすること。

(2) 通信路の暗号化を行なわないまま，他のサーバへのログインや機密情報へのアクセスを行なわないこと。

(3) 機密情報を有する端末を接続する場合は，機密情報を有するドライブ・フォルダ・ファイルは共有設定を行なわないこと。

(4) 機密情報を有さないドライブ・フォルダ・ファイルについても，むやみに共有設定しないこと。

(5) 共有設定を行なう場合は，必ずアクセス権の設定，パスワードの設定，暗号化などによりデータの保護を個人の責任において行なうこと。

（障害対応）

第８条　接続機器管理者は，接続機器およびその周辺機器に障害が生じたときは，速やかに運用管理責任者（以下「管理責任者」という。）に障害に至った経緯を報告しなければならない。

２　管理責任者は，前項の規定により連絡を受けたとき，または自ら障害を発見したときは，速やかに機能回復のため所要の措置を講じなければならない。

第２章　ネットワーク認証・検疫

（認証・検疫システムの設置）

第９条　情報ネットワークの保護と情報セキュリティの確保のために，認証・検疫システムを設置する。

（認証対象）

第１０条　情報ネットワークの利用者をネットワーク認証（以下「認証」という。）の対象者とする。

（認証義務）

第１１条　セキュリティ確保のため，情報ネットワークへ接続する際に認証対象者は認証・検疫システムに登録されているアカウントとパスワード，または主体認証情報格納装置(以下「IC カード等」という。)を使用して認証を行なわなければならない。

２　学外から情報ネットワークへ接続する際に認証対象者は，認証・検疫システムに登録されているアカウントとパスワード，および本学が指定する方法を利用して認証を行なわなければならない。

（識別コードによる認証）

第１２条　認証対象者は，アカウントとパスワードを使用して認証を行なう場合において，アカウント名とパスワードの管理に際して次の各号を遵守しなければならない。

(1) 自分のアカウントを他の者に使用させたり，他の者のアカウントを使用したりしてはならない。
(2) セキュリティを確保するためのパスワードの定期的な変更を怠ってはならない。
(3) 他の者の認証情報を聞き出したりしてはならない。
(4) 自己のパスワードを厳重に管理しなければならない。
(5) 他の者にパスワードを教えたり，不注意でパスワードが他の者に知られることがないよう最大限の注意を払わなければならない。
(6) 使用中の機器をロックあるいはログアウト(ログオフ)せずに長時間離席してはならない。
(7) 学外に設置されている不特定多数の人が操作または利用可能な端末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。但し，当該端末が信頼できるサイトの証明書を得ている場合または ssh 等で暗号化された通信を行なう場合はこの限りではない。
(8) アカウントを他者に使用され，またはその危険が発生した場合には，直ちに情報システム部にその旨を報告しなければならない。

（IC カード等を用いた認証）
第１３条　IC カード等を用いた認証を行なう場合は，IC カード等の管理を次の各号のように徹底しなければならない。
(1) IC カード等を本人が意図せずに使われることのないように安全措置を講じて管理しなければならない。
(2) IC カード等を他者に付与および貸与してはならない。
(3) IC カード等を紛失しないように管理しなければならない。
(4) IC カード等使用時に利用する PIN は，他に漏らしたりしてはならない。

（検疫対象）
第１４条　情報ネットワークに接続し，利用する端末（以下「検疫対象端末」という。）をネットワーク検疫（以下「検疫」という。）対象とする。

（検疫義務）
第１５条　セキュリティ確保のため，情報ネットワークへ接続する際に検疫対象端末は，定められた安全策を実施されていることが認証・検疫システムで確認されなければならない。

（検疫の内容）
第１６条　検疫対象端末の安全性確保のため，次の項目について検査を実施できるものとする。
(1)　指定された OS および定義ファイルの更新
(2)　指定されたウィルス対策ソフトの稼働および定義ファイルの更新

（接続許可）
第１７条　認証・検疫システムは，認証による正当性および検疫による端末の安全策の確認ができない場合は，対象端末の本学の情報ネットワークへの接続を認めない。

（認証・検疫除外機器）
第１８条　次の機器については，ネットワーク認証および検疫の除外対象とする。
(1)　運用上認証対象者が介在しない機器（プリンタ，ネットワークスキャナ等）
(2)　情報ネットワークへの接続時に認証および検疫が行えない機器（サーバ等）

第３章　ファイアーウォール

（ファイアーウォールの設置）
第１９条　情報ネットワークの保護と活用および情報セキュリティの確保のために，ファイアーウォールを設置する。

（通過を禁止する通信）
第２０条　学外ネットワークとの接続の必要性が極めて低く危険性が見込まれる通信については一律にフィルタリング(遮断)を行なう。

（情報ネットワークから学外ネットワークへの接続）
第２１条　情報ネットワークから学外ネットワークへの接続については，第２０条の場合を除いて，http および https についてはプロキシサーバを経由することにより可能とする。但し，学外ネットワークのサーバ等への接続を保証するものではない。

（学外ネットワークから情報ネットワークへの接続）
第２２条　学外ネットワークからの情報ネットワークのサーバ等への接続については，以下の各号に従わなければならない。

（１） 管理責任者の許可を得なければならない。
（２） 本学の認証・検疫システムにおいて指定された認証を受けなければならない。

（IPS・IDS）

第２３条 管理責任者は，情報ネットワークのセキュリティ確保のため，ファイアーウォールには IPS(不正侵入防御システム)・IDS（不正侵入検知システム）を導入し，不正な通信の監視を行なう。

第２４条 管理責任者は，IPS・IDS により不正な通信が検出された場合は，通信を機械的に遮断することができる。

（利用の停止）

第２５条 管理責任者は，接続端末等に脆弱性や不正な通信が発見された場合，「佛教大学セキュリティポリシー」に基づき，利用の停止を行なうことがある。

第４章 無線アクセスポイント

（無線アクセスポイントの設置）

第２６条 学術研究および教育を目的に，利用者が利用することのできる無線アクセスポイントを設置する。但し，学校管理・運営および利用者の福利厚生に資するための利用については認めるものとする。

（設置基準）

第２７条 本学の無線アクセスポイント設置にあたり，２通りの設置基準を設ける。なお，無線アクセスポイントから本学情報ネットワークへのアクセスは，「第２章 ネットワーク認証・検疫」に従うものとする。

(1) 情報システム部管理の無線アクセスポイント
「オープンスペース，教室，その他複数の学部学科で利用が見込める場所」
これらの場所への設置計画および設置は，情報システム部が行なうものとし，個人の無線アクセスポイントの設置を認めない。

(2) 教員研究室管理の無線アクセスポイント
「教員の個人研究室」
教員の個人研究室に無線アクセスポイントを設置する場合は，設置申請手続きを行い，管理責任者の承認を得なければならない。
なお，教員の個人研究室の無線アクセスポイントの運用にあたり，申請した教員を研究室無線管理者とする。

（設置申請）

第２８条 本内規第２７条第２号の無線アクセスポイントを設置申請し，設置することができる者は本学専任教員とする。

第２９条 本内規第２７条第２号の無線アクセスポイントの設置を希望する者は「無線アクセスポイント(無線 LAN)設置申請書」（別紙様式 1 号）を管理責任者に提出し承認を得なければならない。

第３０条 研究室無線管理者は，次の号に掲げる責任を負わなければならない。

(1) 無線アクセスポイントの設置および運用の責任を負わなければならない。
(2) 無線アクセスポイントの設置内容を変更・廃止する場合，管理責任者に届出を行なわなければならない。
(3) セキュリティに対する適切な対策を施さなければならない。
(4) 情報ネットワークに影響を及ぼすことのないよう注意を払わなければならない。

（アクセスポイントの利用者）
第３１条　設置された無線アクセスポイントを利用できる者は，「佛教大学情報セキュリティポリシー」に準ずる者とする。
（電波干渉）
第３２条　情報システム部が管理する無線アクセスポイントと，教員が新規申請または運用する無線アクセスポイントが電波干渉する場合は，情報システム部が管理する無線アクセスポイントを優先するものとする。
第３３条　研究室無線管理者は，自らが運用する無線アクセスポイントが他の研究室無線管理者が運用する無線アクセスポイントと電波干渉する場合には情報システム部に報告し，情報システム部は各々の研究室無線管理者に設定変更を依頼することがある。
（セキュリティ）
第３４条　研究室無線管理者は，以下の事項について理解し，利用者の特定とセキュリティの確保に努めなければならない。
(1) 本学の認証・検疫に関すこと。
(2) 不十分な設定のまま使用しないこと。
(3) 利用者情報について，申請書に記載し，利用者のセキュリティに関する指導を行なうこと。
(4) WPA2 等の暗号化通信を提供すること。
（接続の停止および承認の取消）
第３５条　管理責任者は，研究室無線管理者が本内規に違反した時および違反する恐れがあるときは，無線アクセスポイントを一定期間停止し，または当該接続の承認を取り消すことができる。
２　管理責任者は，無線アクセスポイントの利用が情報ネットワークの管理または運用に重大な支障を及ぼすものであり，その利用を直ちに停止する必要があると認めた場合には，その接続を停止することができる。

第５章　ネットワークディスク

（ネットワークディスクの設置）
第３６条　学術研究および教育を目的に，情報ネットワーク上に，利用者が利用することのできるディスクを設置する。但し，学校管理・運営および利用者の福利厚生に資するための利用については認めるものとする。
（ディスクの容量）
第３７条　情報ネットワーク上にあるディスクの容量は，別表１で定める。利用者は，この値を超えてディスクスペースを使用することはできない。
（ファイルの取り扱い）
第３８条　利用者が，ディスクに格納したファイルおよびその内容に関する全責任は，利用者が負うものとする。
２　利用者は，本サービス上に格納するファイルに関して，その内容に応じて，自己の責任において，暗号化など適切な処理を行なわなければならない。
３　データ分類については，別表２で定める。
（改廃）
第３９条　本内規の改廃は，情報システム委員会の議を経て，運用実施責任者が決定する。

附則

第１条　本内規は，平成 29 年 4 月 1 日から施行する。

第２条　本内規の施行に伴い，「学内情報システム（B-COM-NET,SSTnet）利用規程（平成 7 年 4 月 1 日施行），「学内無線 LAN 利用規程」（平成 23 年 10 月 1 日施行），ネットワーク利用細則（平成 12 年 4 月 1 日施行），情報コンセント利用内規（平成 15 年 4 月 1 日施行）は，廃止する。

別表1　ネットワークディスクの容量制限

対象者	ホームディレクトリ
専任教員	5GB
専任職員	3GB
大学院生	3GB
学部生（通学課程）	1GB
学部生（通信教育課程）	1GB
研究員・研究生	3GB
科目等履修生（通学課程）	1GB