

○情報機器取扱内規

(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。）に関連する情報機器（ハードウェアおよびソフトウェア）の有効活用および資産の保全を目的とする。

(適用範囲)

第2条 本内規で取り扱う情報機器とは情報システム部（以下「システム部」という。）が設置した以下のもの、および本学情報ネットワークに接続することのできる個人の以下の(1)～(4)のものをいう。

- (1) パソコン（メモリー，ディスク，各種ボードを含む。）
- (2) パソコン用ソフトウェア（ワープロ，表計算など）
- (3) プリンタ
- (4) ネットワーク関連機器
- (5) サーバ

(標準機種)

第3条 システム部は設置する情報機器，および本学情報ネットワークに接続することのできる個人の情報機器の標準機種を定める。

(標準外機種の導入)

第4条 本学の情報システムを利用する通常業務を行なうことを目的として，前条で定めた以外の機種を導入する場合，情報システム部と相談の上，運用管理責任者の承認を必要とする。

(ソフトウェアの標準設定基準)

第5条 情報システム部が設置した情報機器，および本学情報ネットワークに接続することのできる個人の情報機器の各種ソフトウェアの環境設定については可能な限り統一するものとし，情報システム部はOS，ソフトウェアごとに「標準設定基準」を定める。利用者は，本設定を変更してはならない。

- 2 情報システム部が提供した各種ソフトウェアの複製については情報システム部の許可を必要とする。個人目的などで本学のソフトウェアを複製することは禁止する。

(遵守事項)

第6条 利用者は，本学が所有または管理する情報機器，または本学情報システムに接続する情報機器の利用に関して，次の各号を遵守しなければならない。

- (1) ネットワークを経由して，不特定多数の第三者が情報機器にアクセスできないようにしなければならない。
- (2) 当該情報機器にアカウントを有さない者に情報機器を使用させてはならない。但し，教育・研究上必要な場合など，運用管理責任者が特に認める場合を除く。
- (3) 当該情報機器の紛失または盗難が発生した場合は，すみやかにシステム部に届け出なければならない。また，個人情報が含まれる場合は総務課へ届け出

なければならない。

- (4) 当該情報機器を廃棄，あるいは譲渡する場合は，内部ハードディスクや不揮発性メモリに，個人情報等重要な情報が残留することのないように，専用ツールを用いて完全に消去するか，物理的に破壊しなければならない。
- (5) 当該情報機器の OS，アプリケーションを定期的に最新の状態にアップデートしなければならない（自動で最新の状態に更新されるように設定することが望ましい）。
- (6) 当該情報機器にアンチウイルス対策ソフトをインストールしなければならない。ライセンスの有効期間に注意し，ウイルス情報データベースは常に最新に保っておかなければならない。
- (7) 出所の定かでないソフトウェアをインストールし，使用してはならない。

（外部記憶媒体）

第7条 利用者は，外部記憶媒体（CD-ROM，USB メモリ，SDHC カード等）の利用に際して，次の各号を遵守しなければならない。

- (1) 利用者のファイルを保存した外部記憶媒体を放置してはならない。
 - (2) 放置してある，または出所が定かでない外部記憶媒体をパソコン等に挿入しアクセスしてはならない。そのような媒体を発見した場合は，情報システム部に届け出なければならない。
 - (3) 使用前にアンチウイルス対策ソフトのパターンファイルを最新の状態にし，外部記憶媒体のウイルスチェックを行ってから使用しなければならない。
 - (4) 使用済みの外部記憶媒体を譲渡，または廃棄する場合には，記録されていたデータが復元されることのないように，専用ツールを用いて消去するか，外部記憶媒体を物理的に破壊しなければならない。
- 2 学内の情報を外部記憶媒体や持ち運び可能な個人のパソコン，およびオンラインストレージサービスに記録する場合は，別表1の定めに基づかなければならない。

（改廃）

第8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，「ユーザ端末利用細則」（平成12年4月1日施行）は，廃止する。

別表1 データ分類

データ分類	情報資産分類・重要度	定義	該当データの例	情報漏洩時の影響	対応		
					オンラインストレージ		CD-ROM、USBメモリ等
					個人領域に格納	他者と共有	個人領域に格納
禁止データ (最重要情報)	レベル4	原則として外部記憶媒体上に格納してはいけない(格納することが極めて推奨されない)データ。	<ul style="list-style-type: none"> ・マイナンバー、住民票コード ・健康保険証番号、免許証番号 ・クレジットカード情報(カード番号、有効期限、セキュリティコード、氏名等) ・金融機関の各種口座番号 ・パスポート番号、ビザ番号 ・外為法の規制対象(輸出規制対象)となる情報 ・相談事項(法律、心理、健康など) ・医療情報(カルテ、健康診断結果、保険料請求など) 	<ul style="list-style-type: none"> ・学外関係者および学内への影響は深刻かつ重大である。 ・大学の評判・信用に重大な影響を与える。 ・コンプライアンス上の問題が生じる。 	フォルダ内に格納しない。		格納しない。
制限データ (重要情報)	レベル3	外部記憶媒体上に格納することについて、制約があるデータ。データ所有者からの許諾、権利関係の確認、公開範囲の制限、暗号化などを考慮すべきデータ。	<ul style="list-style-type: none"> ・個人情報とみなされるものまたは個人のプライバシーに関わるもの 学籍番号、教職員番号、学生生徒記録、人事情報、出願書類、サークル名簿 ・学外非公開情報 非公開の経営情報、非公開の財務情報、非公開の企画情報、非公開の規則・手順書、非公開の寄付情報、非公開の契約情報 	<ul style="list-style-type: none"> ・学内全箇所および学内関係者に重大な影響がある。 ・大学の経営および事業の運営に重大な影響がある。 	必ずファイルにパスワードを設定しなければならない。	必ず共有用パスワードを設定しなければならない(共有期限設定を併用することが望ましい)。	格納しない。
制限データ (取扱注意情報)	レベル2	外部記憶媒体上に格納することについて、制約があるデータ。公開範囲の制限などを考慮すべきデータ。	<ul style="list-style-type: none"> ・研究情報 公表出版前の論文 ・危険物情報、経営財務情報、企画情報 規則・手順書、寄付者情報および寄付内容、学内情報、契約情報 ・公開予定情報、資料 	<ul style="list-style-type: none"> ・学内の特定の箇所または大学の特定の機能に影響がある。 	ファイルにパスワードを設定しなくてもよい。	共有用パスワード・共有期限設定を行うことが望ましい。	必ず外部記憶媒体にパスワードを設定しなければならない。
許可データ (一般情報)	レベル1	外部記憶媒体上に格納することに関して、制限のないデータ。	<ul style="list-style-type: none"> ・佛教大学の公式webサイトで、一般に公開されているコンテンツ ・一般公開されている大学規則、方針 ・一般公開されている公募情報 ・一般公開されている大学の公式な連絡先 ・公表出版済の論文、研究データ ・パブリックドメイン状態にある著作物 	支障が出ない。	データの格納にあたり制限はない。		