旭川医科大学情報セキュリティ対策実施要項の一部を改正する要項を次のように定める。

（令和６年６月１９日学長裁定）

旭川医科大学情報セキュリティ対策実施要項の一部を改正する要項

旭川医科大学情報セキュリティ対策実施要項（平成24年学長裁定）の一部について，下表右欄（「現行」欄）を，同表左欄（「改正後」欄）のように改正する。

※下線部分は改正箇所を示す。

改正後	現行
（略） （定義） 第2　1～2（略） 3　この要項において，「部局」とは，旭川医科大学情報セキュリティ管理規程（平成24年旭医大達第38号。以下「セキュリティ規程」という。）第2条に定めるものをいう。 4～10（略） （略） （据付型クライアント機器の盗難対策） 第11　旭川医科大学情報システム運用基本規程（令和6年旭医大達第84号。以下「システム運用基本規程」という。）第7条に定める部局情報システム管理者は，据付型クライアント機器が盗難等により学外に持ち出されないよう何らかの対策を講じなければならない。 （ネットワークへの接続） 第12　部局情報システム管理者は，ネットワークケーブルを使用する場合には，過失によるネットワークケーブルの切断を防ぐための措置を講じなければならない。 2　システム運用基本規程第6条に定める情報システム管理者は，有	（略） （定義） 第2　1～2（略） 3　この要項において，「部局」とは，情報セキュリティ管理規程（以下「セキュリティ規程」という。）第2条に定めるものをいう。 4～10（略） （略） （据付型クライアント機器の盗難対策） 第11　セキュリティ規程第6条に定める部局情報セキュリティ管理者（以下「部局セキュリティ管理者」という。）は，据付型クライアント機器が盗難等により学外に持ち出されないよう何らかの対策を講じなければならない。 （ネットワークへの接続） 第12　部局セキュリティ管理者は，ネットワークケーブルを使用する場合には，過失によるネットワークケーブルの切断を防ぐための措置を講じなければならない。 2　セキュリティ規程第4条に定める部門情報セキュリティ責任者（以

線，無線どちらの場合においても，ネットワークの盗聴に対する対策を講じなければならない。	下「部門セキュリティ責任者」という。）は，有線，無線どちらの場合においても，ネットワークの盗聴に対する対策を講じなければならない。
3　部局情報システム管理者は，クライアント機器接続用のネットワークケーブルに違うコンピュータが接続されないよう，物理アドレスとIPアドレスの定期的な監視に努めなければならない。	3　部局セキュリティ管理者は，クライアント機器接続用のネットワークケーブルに違うコンピュータが接続されないよう，物理アドレスとIPアドレスの定期的な監視に努めなければならない。
（貸出型クライアント機器の備品管理）	（貸出型クライアント機器の備品管理）
第13　部局情報システム管理者は，当該部局の構成員がクライアント機器を学外へ持ち出す場合においては，貸し出しの事実について管理しなければならない。	第13　部局セキュリティ管理者は，当該部局の構成員がクライアント機器を学外へ持ち出す場合においては，貸し出しの事実について管理しなければならない。
2　部局情報システム管理者は，当該部局の構成員が個人で所有する機器を学内に持ち込みクライアント機器として使用する場合及びこれを学外へ持ち出す場合においては，この事実について管理しなければならない。	2　部局セキュリティ管理者は，当該部局の構成員が個人で所有する機器を学内に持ち込みクライアント機器として使用する場合及びこれを学外へ持ち出す場合においては，この事実について管理しなければならない。
3～4（略）	3～4（略）
（管理区域の設置）	（管理区域の設置）
第14　1～4（略）	第14　1～4（略）
5　管理区域の物理的な場所は，当該サーバのシステム管理者以外には非公開とする。	5　管理区域の物理的な場所は，当該サーバのシステム管理者以外には非公開とする。
6　部局情報システム管理者は，当該部局内のサーバを把握しなければならない。	6　部局セキュリティ管理者は，当該部局内のサーバを把握しなければならない。
（電源）	（電源）
第15　部局情報システム管理者は，電源を供給する際には，電圧の流動や突発的な停電，過電流に対応する装置を経由するよう努めなければならない。	第15　部局セキュリティ管理者は，電源を供給する際には，電圧の流動や突発的な停電，過電流に対応する装置を経由するよう努めなければならない。
（略）	（略）
（サーバ盗難への対策）	（サーバ盗難への対策）
第18　部局情報システム管理者は，サーバが管理区域から持ち出され	第18　部局セキュリティ管理者は，サーバが管理区域から持ち出され

ないよう何らかの対策を講じなければならない。 （略） （コンソールポートの隔離） 第20　ルータ，インテリジェントスイッチは，コンソールポート，管理ポートが許可された特定のシステム管理者以外は使用できないように電子的認証等を用いるものとする。 2　ルータ，インテリジェントスイッチは，施錠などによって物理的に隔離された区域に設置するよう努めるものとする。 （設置場所の秘匿） 第21　部門情報システム（情報システム管理者が管理する情報システムをいう。以下同じ。）を構成する機器をはじめ，重要と思われるネットワーク機器については，その設置場所を限られたシステム管理者以外に非公開とする。 （略） （ネットワーク設計，機器導入及び設定） 第26　大学での新たなネットワークの設計及び構築にあたっては，教育，研究，医療及び管理事務といった目的の異なるネットワーク上の情報を物理的又は論理的に混在させないようにしなければならない。 2　ネットワークの改変を行う場合は，情報セキュリティ委員会（以下「セキュリティ委員会」という。）の許可を得なければならない。 （ネットワーク機器） 第27　部局情報システム管理者は，ルータ，ソフトウェア，設定可能なハブ等が機器障害や権限のないアクセスによって機器の構成や制御機能が損なわれないように管理しなければならない。また，これらの機能を常に最新のものとするように努めなければならない。 （ネットワークの無許可利用等） 第28　ネットワークに接続する装置は，共同利用端末を除き，不特定	ないよう何らかの対策を講じなければならない。 （略） （コンソールポートの隔離） 第20　ルータ，インテリジェントスイッチは，コンソールポート，管理ポートが許可された特定の情報システム管理者以外は使用できないように電子的認証等を用いるものとする。 2　ルータ，インテリジェントスイッチは，施錠などによって物理的に隔離された区域に設置するよう努めるものとする。 （設置場所の秘匿） 第21　部門情報システム（部門情報セキュリティ責任者が管理する情報システムをいう。以下同じ。）を構成する機器をはじめ，重要と思われるネットワーク機器については，その設置場所を限られた情報システム管理者以外に非公開とする。 （略） （ネットワーク設計，機器導入及び設定） 第26　大学での新たなネットワークの設計及び構築にあたっては，教育，研究，医療及び管理事務といった目的の異なるネットワーク上の情報を物理的又は論理的に混在させないようにしなければならない。 2　ネットワークの改変を行う場合は，情報セキュリティ委員会（以下「セキュリティ委員会」という。）の許可を得なければならない。 （ネットワーク機器） 第27　部局セキュリティ管理者は，ルータ，ソフトウェア，設定可能なハブ等が機器障害や権限のないアクセスによって機器の構成や制御機能が損なわれないように管理しなければならない。また，これらの機能を常に最新のものとするように努めなければならない。 （ネットワークの無許可利用等） 第28　ネットワークに接続する装置は，共同利用端末を除き，不特定

多数の手に触れさせてはならない。 2　ネットワークのセキュリティ機能の管理を回避する目的でのバックドア（PPPサーバ，コンピュータに接続する公衆回線，VPN装置及びソフトウェア等をいう。）の設置を原則禁止する。 3　独自のハードウェア回線等を設置する場合には，情報セキュリティ委員会の許可を受けなければならない。また，情報セキュリティ委員会の求めに応じて運用状況を報告しなければならない。 （ネットワークの日常運用） 第29　情報システム管理者は，ファイアウォールや侵入検知システムのログを一定期間保存しなければならない。 2　情報システム管理者は，情報システムへのアクセス記録を取得し一定期間保存しなければならない。また，定期的にそれらのログを分析し，侵入の試みがなされていないかなどをチェックしなければならない。 3　情報システム管理者は，ネットワークに対して不正な接続の監視を行わなければならない。 （略） 附　則 この要項は，令和6年6月19日から実施する。 【改正理由】 本学の情報システム体制の見直しに伴い，所要の改正を行うものである。	多数の手に触れさせてはならない。 2　ネットワークのセキュリティ機能の管理を回避する目的でのバックドア（PPPサーバ，コンピュータに接続する公衆回線，VPN装置及びソフトウェア等をいう。）の設置を原則禁止する。 3　独自のハードウェア回線等を設置する場合には，情報セキュリティ委員会の許可を受けなければならない。また，情報セキュリティ委員会の求めに応じて運用状況を報告しなければならない。 （ネットワークの日常運用） 第29　部門セキュリティ責任者は，ファイアウォールや侵入検知システムのログを一定期間保存しなければならない。 2　部門セキュリティ責任者は，情報システムへのアクセス記録を取得し一定期間保存しなければならない。また，定期的にそれらのログを分析し，侵入の試みがなされていないかなどをチェックしなければならない。 3　部門セキュリティ責任者は，ネットワークに対して不正な接続の監視を行わなければならない。 （略）