

「2025年2月25日」

「理事会制定」

1. 目的

学校法人東北文化学園大学（以下「本法人」という。）は、情報セキュリティの重要性を認識し、本法人の教育活動、研究、地域貢献及び事業運営（以下「本法人の活動」という。）における情報資産の安全な運用と適正な活用を図り、情報セキュリティの維持と向上を図ることを目的として、本基本方針を定める。

2. 定義

本基本方針における用語の定義は、別表に定めるとおりとする。

3. 義務

本法人の情報資産を利用する者、管理及び運用の業務に携わる者は、本基本方針、対策基本規程、その他関連規程を遵守するとともに、本法人外の組織又は個人に対する情報セキュリティ水準の低下を招く行為をしてはならない。

4. 情報セキュリティ対策推進体制の整備

情報セキュリティ対策を推進するために必要な組織体制を整備し、継続的に見直す。

5. 情報の格付け

本法人が取扱う情報について、その重要度と公開性に応じた情報の取扱い方法やアクセス権限を定め、適切に管理する。

6. 情報セキュリティインシデント即応体制の整備

本法人において情報セキュリティインシデント又は事象が発生した場合に、迅速に対応するための体制を整備する。

7. 教育・啓発活動の推進

本法人の情報セキュリティの向上を目的とした教育・啓発活動を推進する。

8. 点検と評価

情報システムの変更や新たな脅威の発生等に対応するため、本基本方針、対策基本規程、その他関連規程の点検と評価を行うための監査体制を整備する。

9. 改廃

この基本方針の改廃は、理事会が行う。

附 則

この基本方針は、2025年4月1日から施行する。

別表

用語	定義
情報セキュリティ	情報の機密性、完全性、および可用性を維持すること。
機密性	情報へのアクセスを許可された者だけが、その情報にアクセスできる状態を確保すること。
完全性	情報が破壊、改ざん、または消去されていない状態を確保すること。
可用性	情報へのアクセスを許可された者が、必要時に中断することなく、情報及び関連資産にアクセスできる状態を確保すること。
情報資産	本法人の活動により収集、保存、加工、伝送されるすべてのデータ及び本学が運用する通信回線を含む情報システム全体を指し、装置の種類や設置場所、媒体を問わない。
情報の格付け	情報の重要度や機密性に基づいて情報を分類し、適切な保護レベルを割り当てることにより、統一したセキュリティ水準で情報を取扱うことを目的とする。
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、本法人の規程又は法令に違反する意図的又は偶発的に生じる事件や事故をいう。事象とは、その可能性のある状態をいう。
情報セキュリティ対策推進体制	<p>情報セキュリティ対策を効果的に実施・維持するための枠組みや仕組みを指す。この体制には、以下の要素を含む。</p> <ul style="list-style-type: none"> ○責任者の設置：情報セキュリティに関する責任者（例えば、最高情報セキュリティ責任者）を設置し、全体の統括を行う。 ○委員会の設置：情報セキュリティ委員会を設置し、ポリシーの策定や対策の実施を監督する。 ○規程・手順の整備：情報セキュリティに関する基本方針や具体的な手順書を整備し、周知徹底する。 ○情報セキュリティインシデント即応体制の整備：インシデントの発生から復旧までの一連のプロセスを管理し、被害を最小限に抑える。 ○教育・訓練：定期的な情報セキュリティ教育や訓練を実施し、意識向上を図る。 ○監査・評価：情報セキュリティ対策の実施状況を定期的に監査・評価し、必要に応じて改善を行う。