情報セキュリティに係る遵守事項

１　システムの管理

　重要なシステムを追加、変更、廃棄等した場合は、その際の設定、構成等の履歴を記録し、厳重に管理すること。

２　システムの開発

　システム開発及び保守時の事故・不正行為対策のため、次の事項を必ず遵守することとする。

（１）責任者、監督者を定めること。
（２）作業者及び作業範囲を明確にすること。
（３）システム開発及び保守等の事故・不正行為に係るリスク分析を行うこと。
（４）開発・保守するシステムは、可能な限り運用システムと切り離すこと。
（５）開発・保守に際しては、可能な限りソースコードの提出をすること。
（６）開発・保守に際しては、セキュリティ上問題となりうるおそれのあるソフトウェアを使用しないこと。
（７）開発・保守の際のアクセス制限を明確にすること。
（８）機器の搬出入は、運用管理者が立ち会いを求め、その内容を確認してもらうこと
（９）開発・保守記録の提出をすること。
（10）マニュアル等は、定められた場所に納入すること。
（11）開発・保守を行った者のユーザＩＤ 、パスワードを当該開発・保守終了後速やかに抹消すること。

３　システムの導入

（１）新たにシステムを導入する場合は、原則として既に稼働しているシステムに接続する前に、十分な試験を行うこと。ただし、導入前に十分な試験を行うことが困難な　場合は、リスク分析を行い、運用管理者と協議の上、その結果を踏まえ対処方針を決　定すること。
（２）試験に使用したデータ及びその結果は厳重に保管すること。

４　ソフトウェアの保守及び更新

（１）ソフトウェア（独自開発ソフトウェア、汎用ソフトウェア）を更新又は一部修正プログラムを組み込む場合は、不具合、他のシステムとの相性等の確認を行うこと。
（２）情報セキュリティに重大な影響を及ぼす不具合に対処した修正プログラムについては速やかに組み込むこと。また、更新することによって、従来に増して強固なセキ　ュリティ対策ができる場合は、早期に運用管理者に情報を提供すること。

５　情報機器の廃棄等

　情報が記録された情報機器を廃棄する場合は、その内容が絶対に復元できないようにすること。

　なお、情報機器の廃棄に関しては、データ消去実施日時、ＨＤＤ情報、実施結果、消去方法などの消去記録とコメントを記した消去作業完了証明書を提出すること。

６　他の情報システムとの接続

　他の情報システムと接続する場合は、事前に十分な試験を行うこと。試験を行うことが困難な場合は、リスク分析を行い、運用管理者と対処方針を協議すること。

７　運用管理
（１）保守を行う要員の業務範囲及び責任範囲を明確にすること。
（２）北薩森林管理署総務グループとの連絡体制を確立すること。なお、保守対象時間外であっても緊急時には連絡の取れる体制とすること。
（３）ネットワーク構成等の重要な情報は、公開しないこと。
（４）ユーザの情報は、厳重に管理すること。
（５）業務上知り得た情報は、外部に漏らさないこと。

８　事後対応
（１）情報セキュリティに関する事案がある場合は、総務グループに報告し、速やかに原因の究明に努めること。
（２）事案に係る関係機器のアクセス記録及び事案内容並びに経過について整理し、保存すること。また、事案に係る再発防止の措置を検討し、速やかに対策を講じること。