二本松市情報セキュリティポリシー

平成１８年３月　策定
平成２８年３月　改定

〈目　　次〉

序　情報セキュリティポリシーの構成

情報セキュリティポリシーとは、二本松市が所掌する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものを総称する。

情報セキュリティポリシーは、二本松市が所掌する情報資産に関する業務に携わる全職員、非常勤及び臨時職員（以下「職員等」という。）及び外部委託事業者に浸透、普及、定着させるものであり、安定的な規範であることが要請される。しかしながら一方では、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ柔軟に対応することも必要である。

このようなことから、情報セキュリティポリシーを一定の普遍性を備えた部分（基本方針）と情報資産を取り巻く状況の変化に依存する部分（対策基準）に分けて策定することとした。

具体的には、情報セキュリティポリシーを、

①情報セキュリティ基本方針
②情報セキュリティ対策基準

の２階層に分け、それぞれを策定することとする。また、情報セキュリティポリシーに基づき、情報システム毎の具体的な情報セキュリティ対策の実施手順として情報セキュリティ実施手順を策定することとする（下表参照）。

情報セキュリティポリシーの構成

文　書　名		内　容
情報セキュリティポリシー	情報セキュリティ基本方針	情報セキュリティ対策に関する統一的かつ基本的な方針。
	情報セキュリティ対策基準	情報セキュリティ基本方針を実行に移すための全てのネットワーク及び情報システムに共通の情報セキュリティ対策の基準。
情報セキュリティ実施手順		ネットワーク及び情報システム毎に定める情報セキュリティ対策基準に基づいた具体的な実施手順。

第１章　二本松市情報資産に係る情報セキュリティ基本方針

１　目的

二本松市の各情報システムが取り扱う情報には、市民の個人情報のみならず行政運営上重要な情報など、外部への漏洩等が発生した場合には極めて重大な結果を招く情報が多数含まれている。

したがって、情報資産及び情報資産を取り扱うネットワーク及び情報システムを様々な脅威から防御することは、市民の財産、プライバシー等を守るためにも、また、事務の安定的な運営のためにも必要不可欠である。ひいては、このことが二本松市に対する市民からの信頼の維持向上に寄与するものである。

また、近年のいわゆるＩＴ革命の進展により、電子商取引の発展や電子自治体の実現が期待されているところである。二本松市がこれらに積極的に対応するためには、全てのネットワーク及び情報システムが高度な安全性を有することが不可欠な前提条件である。

そのため、二本松市の情報資産の機密性、完全性及び可用性(注)を維持するための対策（情報セキュリティ対策）を整備するために二本松市情報セキュリティポリシーを定めることとし、このうち、情報セキュリティ基本方針については二本松市の情報セキュリティ対策の基本的な方針として、情報セキュリティポリシーの対象、位置付け等を定めるものとする。

（注）：国際標準化機構（ISO）が定めるもの（ISO7498－2：1989）
機密性（confidentiality）
：情報にアクセスすることが認可された者だけがアクセスできることを確実にすること。
完全性（integrity）
：情報及び処理の方法の正確さ及び完全である状態を安全防護すること。
可用性（availability）
：許可された利用者が必要なときに情報にアクセスできることを確実にすること。

２　定義

（１）ネットワーク
コンピュータ等を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）をいう。

（２）情報システム
コンピュータ、ネットワーク及び電磁的記録媒体で構成され、処理を行う仕組みをいう。

（３）情報資産
ネットワーク及び情報システム、それらの開発と運用に係る全ての情報並びにそれらで取り扱う全ての情報をいう。
なお、情報資産には紙等の有体物に出力された情報も含むものとする。

（４）情報セキュリティ
情報資産の機密性、完全性及び可用性を維持することをいう。

３　情報セキュリティポリシーの位置付けと職員等及び外部委託事業者の義務

情報セキュリティポリシーは、二本松市が所掌する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものであり、情報セキュリティ対策の頂点に位置するものである。

したがって、二本松市長をはじめとして二本松市が所掌する情報資産に関する業務に携わる全ての職員等及び外部委託事業者は、情報セキュリティの重要性について共通の認識を持つとともに業務の遂行に当たって情報セキュリティポリシーを遵守する義務を負うものとする。

４　情報セキュリティ管理体制

二本松市の情報資産について、市長、副市長及び各部局の長が率先して情報セキュリティ対策を推進・管理するための体制を確立するものとする。

５　情報資産の分類

情報資産をその内容に応じて分類し、その重要度に応じた情報セキュリティ対策を行うものとする。

６　情報資産への脅威

情報セキュリティを維持するうえで、情報資産を脅かす脅威の発生度合や発生した場合の影響を考慮すると、特に認識すべき脅威は以下のとおりである。

（１）部外者の侵入による機器または情報資産の破壊・盗難、ウイルス攻撃等のサイバー攻撃並びに故意の不正アクセスまたは不正操作による機器または情報資産の破壊・盗聴、改ざん・消去等

（２）職員等または外部委託事業者による機器または情報資産の持出、誤操作、アクセスのための認証情報またはパスワードの不適切管理、故意の不正アクセスまたは不正行為による破壊・盗聴、改ざん・消去等、搬送中の事故等による機器または情報資産の盗難、規律違反等の規定外の端末接続によるデータ漏洩、市民サービス・業務の停止等

（３）地震、落雷、火災等の災害並びに事故、故障等によるサービス及び業務の停止

７　情報セキュリティ対策

上記６で示した脅威から情報資産を保護するために、以下の情報セキュリティ対策を講ずるものとする。

（１）物理的セキュリティ対策
情報システムを設置する施設、情報資産、通信回線及び職員等が業務に使用するパソコン等の管理について、物理的な対策を講ずる。

（２）人的セキュリティ対策
情報セキュリティに関する権限や責任を定め、全ての職員等及び外部委託事業者に情報セキュリティポリシーの内容を周知徹底する等、十分な教育及び啓発が講じられるように必要な対策を講ずる。

（３）技術及び運用におけるセキュリティ対策
情報資産を外部からの不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、ネットワーク管理等の技術面の対策、また、システム開発等の外部委託、ネットワークの監視、情報セキュリティポリシーの遵守状況の確認等の運用面の対策を講ずる。
また、情報資産への侵害が発生した場合等に迅速かつ適切に対応するための危機管理対策

を講ずる。

８　情報セキュリティ対策基準の策定

上記７の情報セキュリティ対策を講ずるに当たっては、遵守すべき行為及び判断等の基準を統一的なレベルで定める必要がある。そのため、情報セキュリティ対策を行う上で必要となる基本的な要件を明記した情報セキュリティ対策基準を策定するものとする。

９　情報セキュリティ実施手順の策定

情報セキュリティ対策基準を遵守して情報セキュリティ対策を実施するために、個々の情報資産の対策手順等をそれぞれ定めていく必要がある。そのため、情報資産に対する脅威及び情報資産の重要度に対応する情報セキュリティ対策基準の基本的な要件に基づき、各部局の長等が所掌する情報資産の情報セキュリティ実施手順を策定するものとする。

なお、情報セキュリティ実施手順は、公にすることにより二本松市の行政運営に重大な支障を及ぼす恐れのある情報であることから非公開とする。

10　情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシーが遵守されていることを検証するため、定期的に又は必要に応じて監査及び自己点検を実施する。

11　評価及び見直しの実施

情報セキュリティについて監査を行うなどして、情報セキュリティポリシーに定める事項及び情報セキュリティ対策の評価を実施するとともに、情報セキュリティを取り巻く状況の変化に対応するために、情報セキュリティポリシーの見直しを実施する。

第２章　二本松市行政全般における情報セキュリティ対策基準

この二本松市情報セキュリティ対策基準は、二本松市情報セキュリティ基本方針を実行に移すための二本松市行政全般の情報資産に関する安全対策の基準で、情報セキュリティ対策を実施するに当たっての遵守すべき事項や、判断等の統一的な基準として定めるものとする。

１　対象範囲

（１） 行政機関の範囲

このセキュリティ対策基準が対象とする行政機関は、市長部局、各行政委員会及び議会事務局とする。ただし、各教育機関のうち小中学校において教育のために用いるシステム等（本対策基準が対象とするシステムと物理的又は論理的に分けられたシステム等のみ）は対象外とする。

（２） 情報資産の範囲

このセキュリティ対策基準が対象とする情報資産の範囲は次のとおりとする。

- ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体
- ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）
- 情報システムの仕様書及びネットワーク図等のシステム関連文書

２　組織・体制

二本松市の情報セキュリティ管理については、以下の組織・体制とする。

- 最高情報統括責任者（ＣＩＯ）
- ネットワーク管理者
- ネットワーク担当者
- 統括情報セキュリティ担当者
- 情報セキュリティ担当者
- 情報システム管理者
- 情報システム担当者
- 二本松市電子情報化推進本部
- コンピュータセキュリティインシデント対応チーム（ＣＳＩＲＴ）

３　情報資産の分類と管理

（１）情報資産の管理責任

ア　管理責任

情報資産は、当該情報資産を作成した各課等の情報セキュリティ担当者が管理責任を有する。

イ　利用者の責任

情報資産を利用する者は、情報資産の分類に従い利用する責任を有する。

ウ　重要性の効力

情報資産が複製又は伝送された場合には、当該複製等も分類に基づき管理しなければならない。

（２）情報資産の分類と管理方法

ア　情報資産の分類

対象となるネットワーク及び情報システムの情報資産は、各々の情報資産の機密性、完全性及び可用性を踏まえ、次の重要性分類に従って分類する。

重　要　性　分　類
Ⅰ　個人情報及びセキュリティ侵害が二本松市の住民の生命、財産等へ重大な影響を及ぼす情報。 Ⅱ　公開することを予定していない情報及びセキュリティ侵害が行政事務の執行等に重大な影響を及ぼす情報。 Ⅲ　外部に公開する情報のうち、セキュリティ侵害が、行政事務の執行等に軽微な影響を及ぼす情報。 Ⅳ　上記以外の情報。

イ　情報資産の管理方法

（ア）情報資産の分類の表示

・情報システムで扱う情報資産について、第三者が重要性の識別を容易に認識できないように留意しつつ、印刷、ディスプレイ等への表示、記録媒体等に格納する際の媒体（ＦＤへのラベル等）について、ファイル名、記録媒体等に情報資産の分類が分かるように表示をする等適切な管理を行わなければならない。

（イ）情報資産の取扱い

①情報の作成

・職員等は、業務上必要のない情報を作成してはならない。

・情報を作成する者は、情報の作成時に情報資産の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

・情報を作成する者は、作成途上の情報についても、紛失や流出等を防止しなければならない。また、情報の作成途上で不要になった場合は、当該情報を消去しなければならない。

・職員等は、保有する個人情報について、一時的に加工等の処理を行うため複製等を行う場合は、その対象を必要最小限に限り、処理終了後は不要となった情報を速やかに削除しなければならない。

②情報資産の入手

・庁内の者が作成した情報資産を入手した者は、入手元の情報資産の分類に基づいた取扱いをしなければならない。

・庁外の者が作成した情報資産を入手した者は、情報資産の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

・情報資産を入手した者は、入手した情報資産の分類が不明な場合、情報セキュリティ担当者に判断を仰がなければならない。

③情報資産の利用

・情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。

・情報資産を利用する者は、情報資産の分類に応じ、適切な取扱いをしなければならない。

・情報資産を利用する者は、記録媒体に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って、当該記録媒体を取り扱わなければならない。

④情報資産の保管

・情報セキュリティ担当者又は情報システム管理者は、情報資産の分類に従って、アクセス権限を定め、情報資産を適切に保管しなければならない。

・情報セキュリティ担当者又は情報システム管理者は、情報資産を記録した外部記録媒体を長期保管する場合は、書込禁止等の措置を講じなければならない。

・情報セキュリティ担当者又は情報システム管理者は、重要な情報資産（重要性分類Ⅱ以上）の情報を記録した外部記録媒体を保管する場合、火災、水害、埃、振

動、温度、湿度等の影響を可能な限り排除した施錠可能な場所に保管しなければならない。

⑤情報の送信

・重要な情報資産（重要性分類Ⅱ以上）を電子メール等で送信してはならない。ただし、業務上必要な場合は、情報セキュリティ担当者の許可を得て、これを送信することができる。

・電子メール等により重要な情報資産（重要性分類Ⅱ以上）を送信する者は、暗号化又はパスワードの設定を行う等、情報資産の不正利用を防止するための措置を講じなければならない。

⑥情報資産の運搬

・車両等により重要な情報資産（重要性分類Ⅱ以上）を運搬する者は、必要に応じ鍵付きのケース等に格納し、暗号化又はパスワードの設定を行う等、情報資産の不正利用を防止するための措置を講じなければならない。

・重要な情報資産（重要性分類Ⅱ以上）を運搬する者は、情報セキュリティ担当者に許可を得なければならない。

⑦情報資産の提供及び公表

・重要な情報資産（重要性分類Ⅱ以上）を外部に提供する者は、必要に応じ暗号化又はパスワードの設定を行わなければならない。

・情報資産を外部に提供する者は、二本松市電子計算機処理に係る管理運営規程（平成１７年１２月１日訓令第１２号）（以下「管理運営規程」という。）第１１条の規定によるほか、重要な情報資産（重要性分類Ⅱ以上）については、ネットワーク管理者に許可を得なければならない。

・情報セキュリティ担当者は、住民に公開する情報資産について、完全性を確保しなければならない。

⑧情報資産の廃棄

・記録媒体が不要となった場合は、当該媒体に含まれる重要な情報資産（重要性分類Ⅱ以上）は、記録媒体の初期化など情報資産を復元できないように消去を行ったうえで廃棄しなければならない。

・重要な情報資産（重要性分類Ⅱ以上）を記録した記録媒体の廃棄は、情報セキュリティ担当者の許可を得ることとし、行った処理について、日時、担当者及び処理内容を記録しなければならない。

４　物理的セキュリティ

（１）サーバ等

ア　装置の取付け等

（ア）情報システム管理者は、ネットワーク及び情報システムの取付けを行う場合は、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適切な固定等必要な措置を施さなければならない。

（イ）情報システム管理者は、次のサーバは二重化し、ミラーリング等により常に同一データを保持し、メインサーバに障害が発生した場合には速やかにセカンダリサーバに移行させ、システムの運用が停止しないようにしなければならない。

・重要な情報資産（重要性分類Ⅱ以上）を格納しているサーバ

・住民サービスに関するサーバ

・セキュリティサーバ

（ウ）情報システム管理者は、ネットワーク管理者、情報システム管理者、情報システム担当者及び契約により操作を認められた外部委託事業者以外の者が容易に操作できないように、利用者のＩＤ、パスワードの設定等の措置を施さなければならない。

イ　電源

（ア）情報システム管理者は、ネットワーク管理者及び施設管理部門と連携し、サーバ等の機器の電源については、停電等による電源供給の停止に備え、当該機器を適切に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。
（イ）情報システム管理者は、ネットワーク管理者及び施設管理部門と連携し、落雷等による過電流に対してサーバ等の機器を保護するための措置を施さなければならない。

ウ　通信ケーブル等の配線

情報システム管理者は、通信ケーブル及び電源ケーブルが傍受又は損傷等を受けることがないように可能な限り必要な措置を施さなければならない。また、損傷等があった場合は、施設管理部門と連携して対応しなければならない。

エ　外部に設置する装置

（ア）外部に設置する装置は、最高情報統括責任者の承認を受けたものでなければならない。また、最高情報統括責任者は、定期的に当該装置の情報セキュリティの水準について確認しなければならない。
（イ）ネットワーク管理者又は情報システム管理者は、二本松市外に持ち出される端末、記録媒体等について、管理簿を設ける等適切に管理しなければならない。

オ　装置の定期保守及び修理

（ア）情報システム管理者は、重要な情報資産（重要性分類Ⅱ以上）を取り扱うサーバ等の定期保守を実施しなければならない。
（イ）情報システム管理者は、記録媒体を内蔵する機器を外部の事業者に修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合、情報システム管理者は、外部の業者に故障を修理させるにあたり、修理を委託する事業者との間で、守秘義務契約を締結する他、秘密保持体制の確認などを行わなければならない。

カ　装置等の廃棄

情報システム管理者は、機器を廃棄、リース返却等をする場合、機器内部の記憶装置から、すべての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

（２）管理区域

ア　管理区域

（ア）ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等又は重要性分類Ⅱ以上の情報資産の管理並びに運用を行うための部屋（以下「管理区域」という。）は、外部から通じるドアを必要最小限にする等、外部からの侵入が用意にできないよう措置を講じなければならない。
（イ）消火剤は機器及び記録媒体に影響を与えるものであってはならない。

イ　管理区域の入退室管理

（ア）管理区域の入退室は許可された者のみとし、ＩＤカード等による入退室管理を行い、職員等及び外部委託事業者は身分証明書等を携帯し、求めにより提示しなければならない。
（イ）情報システム管理者は、重要な情報資産（重要性分類Ⅱ以上）を扱うシステムを設置している管理区域について、当該情報システムに関連しないコンピュータ、通信回線装置、外部記録媒体等を持ち込ませないようにしなければならない。

ウ　機器等の搬入場所

（ア）管理区域へ機器などを搬入する場合は、あらかじめ当該機器などの既存情報システムに対する安全性について、職員又は委託した業者による確認を行わなければならない。
（イ）機器等の搬入には職員が同行する等の必要な措置を施さなければならない。

（３）ネットワーク

（ア）外部へのネットワーク接続は必要最低限のものに限定し、できる限り接続ポイントを減らさなければならない。

（イ）特に行政系のネットワークは総合行政ネットワーク（ＬＧＷＡＮ）に集約するように努めなければならない。
（ウ）総合行政ネットワーク（ＬＧＷＡＮ）以外のインターネット接続は、基幹系及び内部情報系ネットワークと切り離された環境で接続しなければならない。
（エ）ネットワークに使用する回線は、伝送途上において破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策が実施されたものでなければならない。
（オ）各フロアに設置されている通信ケーブル等について、ネットワークスイッチから先の通信ケーブル等については情報セキュリティ担当者が管理するものとし、それ以外の通信ケーブル等についてはネットワーク管理者が管理するものとする。
（カ）ネットワーク管理者及び情報セキュリティ担当者は、施設管理部門と連携し、通信ケーブル等が傍受又は損傷等を受けることがないように可能な限り必要な措置を施さなければならない。
（キ）ネットワーク管理者及び情報セキュリティ担当者は、主要な箇所の通信ケーブル等については、損傷等についての定期的な点検を行い、損傷等があった場合は、施設管理部門と連携して対応しなければならない。
（ク）ネットワーク管理者及び情報セキュリティ担当者は、ネットワーク接続口(ハブのポート等)を他者が容易に接続できない場所に設置する等適切に管理しなければならない。
（ケ）ネットワーク管理者及び情報セキュリティ担当者は、自ら又は情報システム担当者及び契約により操作を認められた外部委託事業者以外の者が配線を変更、追加できないように必要な措置を施さなければならない。

（４）職員等の端末等

執務室等に職員等がいない場合は、執務室等の施錠など盗難防止のための措置を施さなければならない。

５　人的セキュリティ

（１）役割・責任

ア　最高情報統括責任者（ＣＩＯ）

二本松市副市長を、二本松市における全てのネットワーク、情報システム、情報資産及び情報セキュリティに関する最終決定権限及び責任を有する最高責任者（ＣＩＯ：最高情報統括責任者）とする。

イ　ネットワーク管理者

（ア）二本松市総務部長を、最高情報統括責任者直属のネットワーク管理者とする。

ネットワーク管理者は、最高情報統括責任者を補佐しなければならない。

（イ）ネットワーク管理者は、二本松市の全てのネットワークにおける開発、設定の変更、運用、更新等を行う権限及び責任を有する。

ただし、行政手続における特定の個人を識別するための番号の利用等に関する法律（平成２５年法律第２７号。以下「番号法」という。）第２条第８号に規定する特定個人情報を含む情報資産の取扱いについては、二本松市特定個人情報等の安全管理措置に関する規程（平成２７年１２月２５日二本松市訓令第１６号）第５条第２項に規定する保護管理者と連携し、同規程に基づき適正に取り扱わなければならない。

（ウ）ネットワーク管理者は、二本松市の全てのネットワークにおける情報セキュリティに関する権限及び責任を有する。

（エ）ネットワーク管理者は、ネットワーク担当者、統括情報セキュリティ担当者、情報セキュリティ担当者、情報システム管理者及び情報システム担当者に対して情報セキュリティに関する指導及び助言を行う権限を有する。

（オ）ネットワーク管理者は、二本松市の情報資産に対する侵害又は侵害のおそれのある場合には、最高情報統括責任者の指示に従い、最高情報統括責任者が不在の場合には

自らの判断に基づき必要かつ十分な全ての措置を行う権限及び責任を有する。
この場合、全ての職員等はネットワーク管理者の指示に従わなければならない。

（カ）ネットワーク管理者は、二本松市の全てのネットワーク、情報システム及び情報資産に関する情報セキュリティ実施手順の維持・管理を行い、緊急時対応計画に基づく訓練を実施する。

（キ）ネットワーク管理者は、必要に応じ、情報セキュリティに関する統一的な窓口として、また、侵害等に対処するため、コンピュータセキュリティインシデント対応チーム（ＣＳＩＲＴ）を、二本松市の部局を横断して組織することができる。

（ク）ネットワーク管理者は、特に重要なものを除き、必要に応じ、二本松市行政組織規則（平成１７年１２月１日規則第５号）第６条の規定する事務について、その事務を分掌する係に属する職員に行わせることができる。

ウ　ネットワーク担当者

（ア）電子情報部門を所掌する課の長をネットワーク担当者とする。ネットワーク担当者は、ネットワーク管理者を補佐しなければならない。

（イ）ネットワーク担当者は、情報セキュリティに関する事故について、連絡を受けた場合には、その状況を確認し、最高情報統括責任者及びネットワーク管理者へ報告しなければならない。

（ウ）ネットワーク担当者は、最高情報統括責任者及びネットワーク管理者による情報セキュリティに関する意思決定が行われた場合には、その内容を関係部局等へ提供しなければならない。

（エ）ネットワーク担当者は、情報資産の適切な管理のため、情報セキュリティに関して、関係機関、他の市町村の情報セキュリティに関する部署及び事業者等と連携して、情報の共有を行う。

（オ）ネットワーク担当者は、職員等が使用する端末及びＵＳＢメモリ等の電子記録媒体の総合的な管理及び配置を行う。

エ　統括情報セキュリティ担当者

（ア）内部部局の長及び各行政委員会事務局等の長を、その部局等の情報セキュリティに関する統括的な権限及び責任を有する統括情報セキュリティ担当者とする。

（イ）統括情報セキュリティ担当者は、所掌に属する部局等における情報セキュリティに関する統括的な権限及び責任を有する。

（ウ）統括情報セキュリティ担当者は、所掌に属する部局等において担当している情報システムの追加・変更の承認等を行う。

（エ）統括情報セキュリティ担当者は、所掌に属する部局等において担当している情報システムの連絡体制の構築並びに情報セキュリティポリシーの遵守に関する意見の集約及び職員等に対する教育、訓練、助言及び指示を行う。

オ　情報セキュリティ担当者

（ア）内部部局の課室長、内部部局の出張所等出先機関の長及び各行政委員会事務局等の課室長を、その所管組織の情報セキュリティに関する権限及び責任を有する情報セキュリティ担当者とする。情報セキュリティ管理者は直属の統括情報セキュリティ担当者を補佐しなければならない。

（イ）情報セキュリティ担当者は、統括情報セキュリティ担当者の下、所管組織内における情報セキュリティポリシーの遵守に関する権限と責任を有する。

（ウ）情報セキュリティ担当者は、所掌に属する課室等における情報資産に対する侵害又は侵害の恐れのある場合には、最高情報統括責任者及びネットワーク管理者へ速やかに報告を行い、指示を仰がなければならない。
この場合、最高情報統括責任者及びネットワーク管理者に報告した後、速やかに統括情報セキュリティ担当者に報告しなければならない。

（エ）情報セキュリティ担当者は、職員等が常に情報セキュリティポリシー及び実施手順を確認できるよう措置を講じなければならない。

カ　情報システム管理者

（ア）各情報システムの担当課室長等を当該情報システムに関する情報システム管理者とする。

（イ）情報システム管理者は、所管する情報システムにおける開発、設定の変更、運用、更新等を行う権限及び責任を有する。

（ウ）情報システム管理者は、情報システムにおける情報セキュリティに関する権限及び責任を有する。

（エ）情報システム管理者は、担当する情報システムに係る情報セキュリティ実施手順の維持・管理を行う。

キ　情報システム担当者

情報システム担当者は、担当する情報システムに関して、情報システム管理者の指示等に従い、開発、設定の変更、運用、更新等の作業を行う。

ク　二本松市電子情報化推進本部

（ア）二本松市の情報セキュリティの維持管理を統一的な視点で行うため、二本松市電子情報化推進本部において、情報セキュリティポリシーの更新等、情報セキュリティに関する重要な事項を審議する。

（イ）二本松市電子情報化推進本部は、情報セキュリティに対する意識を醸成し保つために、市長、副市長及び各部局の長をはじめとした全ての職員等が情報セキュリティの重要性を認識できるよう啓発に努めなければならない。

（ウ）ネットワーク管理者が実施する緊急時対応計画に基づく訓練に協力し、ネットワーク管理者と連携して、実際に情報資産の漏洩等の事故が発生した場合に即応できるように体制を整えなければならない。

ケ　コンピュータセキュリティインシデント対応チーム（ＣＳＩＲＴ）

（ア）コンピュータセキュリティインシデント対応チーム（ＣＳＩＲＴ）は、ネットワーク管理者の指示のもと、二本松市における情報セキュリティに関する統一的な窓口として情報の収集及び情報の発信を行う。

（イ）コンピュータセキュリティインシデント対応チーム（ＣＳＩＲＴ）は、ネットワーク管理者の指示のもと、情報セキュリティに対する侵害・脅威等に対処する。

コ　職員

（ア）情報セキュリティ対策の遵守義務

全ての職員は、情報セキュリティポリシー及び職員向け実施手順に定められている事項を遵守しなければならない。

情報セキュリティ対策について不明な点、遵守することが困難な点等については、速やかに情報セキュリティ担当者に相談し、指示等を仰がなければならない。

（イ）その他

・全ての職員は、業務以外の目的で情報資産の外部への持出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

・全ての職員は、使用する端末や記録媒体について、第三者に使用されること、又は許可なく情報資産を閲覧されることがないように、適切な措置を施さなければならない。

・全ての職員は、情報セキュリティ担当者の許可を得ず、端末等を執務室外に持ち出してはならない。

・全ての職員は、異動、退職等により業務を離れる場合には、知り得た情報資産を秘匿しなければならない。

サ　非常勤及び臨時職員

（ア）情報セキュリティ対策の遵守義務

・全ての非常勤及び臨時職員は、情報セキュリティポリシー及び職員向け実施手順に定められている事項を遵守しなければならない。

・情報セキュリティ対策について不明な点、遵守することが困難な点等については、速やかに情報セキュリティ担当者に相談し、指示等を仰がなければならない。

（イ）非常勤及び臨時職員の雇用及び契約

・非常勤及び臨時職員には、雇用及び契約時に必ず情報セキュリティポリシーのうち、非常勤及び臨時職員が守るべき内容を理解させ、また、実施及び遵守させなければならない。

・非常勤及び臨時職員には、雇用及び契約の際、必要な場合は情報セキュリティポリシーを遵守する旨の同意書への署名を求めるものとする。

・非常勤及び臨時職員に端末による作業を行わせる場合においては、インターネットへの接続及び庁内ＬＡＮのメールの使用が不要の場合には、これを利用できないように設定しなければならない。

（ウ）その他

・全ての非常勤及び臨時職員は、業務以外の目的で情報資産の外部への持出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

・全ての非常勤及び臨時職員は、使用する端末や記録媒体について、第三者に使用されること又は許可なく情報資産を閲覧されることがないように、適切な措置を施さなければならない。

・全ての非常勤及び臨時職員は、情報セキュリティ担当者の許可を得ず、端末等を執務室外に持ち出してはならない。

・全ての非常勤及び臨時職員は、異動、退職等により業務を離れる場合には、知り得た情報資産を秘匿しなければならない。

シ　外部委託に関する管理

ネットワーク及び情報システムの開発・保守を外部委託事業者に発注する場合は、外部委託事業者から再委託を受ける事業者も含めて、管理運営規程第１４条に規定する事項のほか下記事項を明記した契約を締結しなければならない。

・情報セキュリティポリシー及び情報セキュリティ実施手順の遵守
・提供された情報の返還義務
・二本松市に対する報告義務
・二本松市による定期的な報告徴収、監査、検査の実施
・従業員に対する教育の実施
・情報セキュリティポリシー遵守のために構築する体制
・情報セキュリティポリシーが遵守されなかった場合の規定（損害賠償等）

（２）教育・訓練

ア　最高情報統括責任者は、説明会の実施等により市長及び各部局の長を含め全ての職員等及び関係する者に対し情報セキュリティポリシーについて啓発しなければならない。また、新規採用の職員等を対象とする情報セキュリティポリシーに関する研修を設けなければならない。

情報セキュリティポリシーに関する教育・訓練プログラムは、二本松市電子情報化推進本部で承認されたものを使用する。

また、最高情報統括責任者は、一般職員とは別に、ネットワーク管理者、ネットワーク担当者、統括情報セキュリティ担当者、情報セキュリティ担当者、情報システム管理者、情報システム担当者及び新規採用の職員に対して、それぞれの役割、情報セキュリティに関する理解度等に応じた研修を実施しなければならない。

イ　ネットワーク管理者は、最新の技術力を維持するための研修を常に受けなければならない。ネットワーク管理者は、緊急時対応を想定した訓練を職員等に計画的に行わせなければならない。訓練の計画に当たっては、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の範囲等を適宜定めることとする。また、より効果的に実施できる

よう計画を立てることとする。

ウ　情報システム管理者及び情報システム担当者は、情報システムに関する研修を受けなければならない。

エ　職員等は、定められた研修に参加し情報セキュリティポリシー及び実施手順を理解し、情報セキュリティ上の問題が生じないようにしなければならない。

（３）事故、欠陥に対する報告

ア　職員等は、情報セキュリティに関する事故、システム上の欠陥及び誤動作を発見した場合には、速やかにネットワーク管理者又はネットワーク担当者に報告し、ネットワーク管理者の指示に従い必要な措置を講じなければならない。また、別途、職員等は、情報セキュリティ担当者に報告し、情報セキュリティ担当者は、報告のあった事故等について必要に応じ、最高情報統括責任者及び統括情報セキュリティ担当者に報告しなければならない。

イ　職員等は、二本松市が管理するネットワーク及び情報システムに関する事故、欠陥に関する住民等外部からの報告・連絡を受けた場合には、速やかにネットワーク管理者又はネットワーク担当者に報告し、ネットワーク管理者の指示に従い必要な措置を講じなければならない。また、別途、職員等は、情報セキュリティ担当者に報告し、情報セキュリティ担当者は、報告のあった事故等について必要に応じ、最高情報統括責任者及び統括情報セキュリティ担当者に報告しなければならない。

ウ　ネットワーク管理者は、これらの事故等を分析し、再発防止のための情報資産として記録を保存しなければならない。

（４）アクセスのための認証情報及びＩＤ・パスワードの管理

ア　ＩＣカード等の管理

職員等は、自己の管理するＩＣカード等に関し、次の事項を遵守しなければならない。

・業務上必要のない時は、ＩＣカード等をカードリーダ又は端末のスロット等から抜いておかなければならない。

・職員等はＩＣカード等を紛失した場合には、速やかにネットワーク管理者及び情報システム管理者に通報し、指示を仰がなければならない。

・ネットワーク管理者及び情報システム管理者は通報があり次第速やかに当該ＩＣカード等を使用したアクセス等を停止しなければならない。

・ネットワーク管理者及び情報システム管理者は、ＩＣカード等を廃棄する場合は、破砕するなどの復元不可能な処理を行わなければならない。また、その処理を行った日付及び処理内容を記録しなければならない。

イ　ＩＤ、パスワードの管理

職員等は、自己の管理するＩＤ、パスワードに関し、次の事項を遵守しなければならない。

・自己が利用しているＩＤは、他人に利用させないこと。

・共用ＩＤを利用する場合は、共用ＩＤの利用者以外に利用させないこと。

・パスワードを秘密にし、パスワードの照会等には原則として応じないこと。

・パスワードのメモを作らないこと。

・端末にパスワードを記憶させないこと。必要に応じて暗号化等を行うことによって他者がパスワードを読めないようにすること。

・職員等間でパスワードを共有しないこと。

・複数の情報システム間で、同一のパスワードを使用しないこと。

・仮のパスワードは、最初のログイン時点で変更すること。

・パスワードは定期的に変更すること。

・パスワードが流出した恐れがある場合には、情報セキュリティ担当者に速やかに報告し、直ちにパスワードを変更すること。

６　技術的セキュリティ

（１）ネットワーク、情報システム及び情報資産の管理

情報資産の重要性分類に従ってネットワーク、情報システム及び情報資産を以下のとおり管理する。

ア　重要性分類Ⅰ及びⅡ

・ネットワーク管理者及び情報システム管理者は、ネットワーク構成図、情報システム仕様書等に関し、記録媒体の形態に関わりなく適切な保管をしなければならない。

・情報システム管理者は、所管する重要性分類Ⅰ以上の情報資産を最高情報統括責任者が定めた暗号により暗号化しなければならない。また、重要性分類Ⅱ以上の情報資産を外部へ送信又は搬出する際には、最高情報統括責任者が定めた電子署名方式及び暗号を使用しなければならない。

・緊急時に直ちに対処できるようにするため、最高情報統括責任者が定めた特に重要な情報システムは、ミラーリングにより常時バックアップしなければならない。また、最高情報統括責任者が定めた重要なネットワーク及び情報システムは、システムを二重化しなければならない。

・ネットワーク管理者及び情報システム管理者は、ミラーリング及び二重化したネットワーク及び情報システムの動作検証を定期的に行わなければならない。

・情報システム管理者は、情報システムのミラーリング等に関わりなく情報資産の重要度に応じて期間を設定し、定期的に情報資産のバックアップ用の複製をとらなければならない。

・ネットワーク管理者及び情報システム管理者は、閲覧権限がない職員等が所管するシステムにアクセスすることが不可能となるように、システム上制限しなければならない。

・汎用受付システム等、外部の者が利用できるシステムにおいては、必要に応じ他のネットワーク及び情報システムと物理的に分ける等、情報セキュリティ対策について特に強固に対策をとらなければならない。

イ　重要性分類Ⅲ及びⅣ

・原則、重要性分類Ⅱ以上に分類される情報資産の管理に準拠するが、重要性分類Ⅲ以下の情報資産は公開を前提としているため、この範囲において基準を緩和することができる。ただし、Ｗｅｂサイトにより情報を公開・提供する場合には、当該サイトに係るシステムにおいて盗難、改ざん、消去、踏み台、ＤｏＳ等を防止しなければならない。また、メールシステム等においても、他のシステムに対する攻撃の踏み台とならないように適切な管理を実施しなければならない。

（２）ネットワークに接続する機器等の管理

ア　パソコン等の端末等の持込みの禁止

職員等は、私物のパソコン及び記録媒体を庁舎内に持ち込んで業務に使用してはならない。ただし、業務上必要な場合でこれらを使用する以外に方法がない場合に限り、ネットワーク管理者の許可を得て、これらを使用することができる。

イ　持出し及び持込みの記録

ネットワーク担当者は、ネットワーク管理者の許可を得た端末等の持込みについて、記録を作成し、保管しなければならない。また、その内容を定期的に最高情報統括責任者に報告しなければならない。

ウ　複合機のセキュリティ管理

・情報セキュリティ担当者は、複合機を使用する場合、その機能や取り扱う情報資産の分類に応じ、適切なセキュリティ対策を講じなければならない。

・情報セキュリティ担当者は、複合機の使用を終了する場合、当該複合機の持つ電磁的記録媒体の全ての情報を抹消又は再利用できないようにしなければならない。

エ　特定用途機器のセキュリティ管理

ネットワーク管理者は、ＩＰ電話、ネットワークカメラシステム等通信回線に接続されている又は電磁的記録媒体を内蔵している特定の用途のために用いられる特定用途機器について、その取り扱う情報資産の分類に応じ、適切なセキュリティ対策を講じなければならない。

オ　無線ＬＡＮ及びネットワークの盗聴対策

ネットワーク管理者は、無線ＬＡＮの利用を認める場合、解読が困難な暗号化及び認証技術の使用を義務付けなければならない。また、機密性の高い情報を取り扱うネットワークについて、情報の盗聴を防ぐため、暗号化等の措置を講じなければならない。

カ　機器構成の変更の禁止

職員等は、各自に供用された端末等に対して機器の増設又は改造を行ってはならない。特に機器を増投して他の環境（インターネット等）へのネットワーク接続を行うことや、庁外からのアクセスを可能とする仕組みを構築した職員等は地方公務員法による懲戒処分の対象とする。ただし、業務を円滑に遂行するための合理的理由がある場合、かつネットワーク管理者及び情報システム管理者の事前の了解を得た場合に限り、機器の増設又は変更を行うことができる。

キ　システム管理記録及び作業の確認

・情報システム管理者は、所管する情報システムの運用において実施した作業について、作業記録を作成しなければならない。

・情報システム管理者は、所管するシステムにおいて、システム変更等の作業を行った場合は、作業内容について記録を作成し、窃取、改ざん等をされないように適切に管理しなければならない。

・情報システム管理者、情報セキュリティ担当者又は情報システム担当者及び契約により操作を認められた外部委託事業者がシステム変更等の作業を行う場合は、２名以上で作業し、互いにその作業を確認しなければならない。

・ネットワーク管理者及び情報システム管理者は、職員等からのシステム障害の報告、システム障害に対する処理結果又は問題等を、障害記録として記録し、適切に保存しなければならない。

ク　ログの取得等

・ネットワーク管理者及び情報システム管理者は、各種アクセス記録及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。また、定期的にそれらを分析、監視しなければならない。

・ネットワーク管理者及び情報システム管理者は、アクセス記録等が窃取、改ざん、誤消去等されないように必要な措置を講じなければならない。

（３）ネットワーク及び情報システムを使用する際の規定

ア　業務目的以外の使用の原則禁止

職員等によるネットワーク及び情報システム資源の使用は、業務目的に沿ったもののみが許可される。業務目的以外での情報システムへのアクセス、メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

イ　情報資産の持出し及びインターネット等による情報資産の送信禁止

職員等は、重要性分類Ⅱ以上に該当する情報資産を取り扱う場合、次の行為を行ってはならない。特に、インターネットへの自動転送は厳禁する。

・庁外への持出し

・インターネット等による庁外との送受信

・個人の所有する情報が記録された媒体の管理区域への持込み

ただし、情報資産のバックアップ等、合理的理由のある場合、かつ最高情報統括責任者の事前の了解を得た場合に限り、庁外への持出し又は庁外との送受信ができるものとする。

ウ　電子メールのセキュリティ管理

・ネットワーク管理者は、権限のない利用者により、外部から外部への電子メール転送(電子メールの中継処理)が行われることを不可能とするよう、電子メールサーバの設定を行わなければならない。

・ネットワーク管理者は、大量のスパムメール等の受信又は送信を検知した場合は、メールサーバの運用を停止しなければならない。

・ネットワーク管理者は、電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能にしなければならない。

・ネットワーク管理者は、職員等が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を職員等に周知しなければならない。

・ネットワーク管理者は、システム開発や運用等のため庁舎内に滞在している外部委託事業者の作業員による電子メールアドレス利用について、委託先との間で利用方法を取り決めなければならない。

エ　電子メールの利用制限

・職員等は、自動転送機能を用いて、外部の者に電子メールを転送してはならない。ただし、業務上の必要がある場合は、ネットワーク管理者及び統括情報セキュリティ担当者の許可を得た上で、使用することができる。

・職員等は、業務上必要のない送信先に電子メールを送信してはならない。

・職員等は、複数人に電子メールを送信する場合、必要がある場合を除き、他の送信先の電子メールアドレスが分からないようにしなければならない。

・職員等は、重要な電子メールを誤送信した場合、情報セキュリティ担当者に報告しなければならない。

・職員等は、ウェブで利用できるフリーメール、ネットワークストレージサービス等を使用してはならない。ただし、業務上の必要がある場合は、最高情報統括責任者の許可を得るとともに、暗号化又はパスワードの設定を行う等、情報資産の不正利用を防止するための措置を講じた上で、使用することができる。

オ　ソーシャルメディアサービスの利用制限

・情報セキュリティ担当者は、業務上必要な場合に限り、利用するソーシャルメディアサービスごとに、最高情報統括責任者の許可を得た上で、二本松市が管理するアカウントを使用して利用することができる。

・情報セキュリティ担当者は、二本松市のアカウントによる発信が、実際の二本松市のものであることを明らかにするために、アカウントの運用組織を明示する等の方法でなりすまし対策を行うほか、パスワードや認証のためのコード等の認証情報を適切に管理しなければならない。

・重要な情報資産（重要性分類Ⅱ以上）は、ソーシャルメディアサービスで発信してはならない。

カ　無許可ソフトウェアの導入の禁止

・職員等は、各自に供用された端末等に対して、最高情報統括責任者が定める以外のソフトウェアの導入を行ってはならない。特にネットワーク上の情報資産を盗聴するような監視ソフトウェアやネットワークの状態を探索するセキュリティ関連のソフトウェア及びハッキングソフトウェアの使用は厳禁し、導入又は使用した職員等は地方公務員法による懲戒処分の対象とする。ただし、業務を円滑に遂行するために必要なソフトウェアについては、合理的理由のある場合、かつネットワーク管理者及び情報システム管理者の事前の了解を得た場合に限り、利用することができる。

・情報セキュリティ担当者及び情報システム管理者は、ソフトウェアのライセンスを管理しなければならない。

キ　情報及びソフトウェアの交換

情報システム管理者は、他の団体と情報システムに関する情報及びソフトウェアを交換する場合、その取扱いに関する事項をあらかじめ定め、ネットワーク管理者の許可を

得なければならない。

ク　情報システムの入出力データ

・情報システム管理者は、情報システムに入力されるデータについて、適切なチェック等を行い、それが正確であることを確実にするための対策を施さなければならない。

・情報システム管理者は、エラー又は故意の行為により情報が改ざんされる恐れがある場合、これを検出する手段を講じなければならない。また、改ざんの有無を検出し、必要な場合は情報の修復を行う手段を講じなければならない。

・情報システム管理者は、情報システムから出力されるデータは、保存された情報の処理が正しく反映され、出力されることを確保しなければならない。

ケ　無許可でのネットワーク接続の禁止

職員等は、ネットワーク管理者の許可なくパソコン等の端末等をネットワークに接続してはならない。

コ　業務以外の目的でのウェブ閲覧の禁止

・職員等は、業務以外の目的でウェブを閲覧してはならない。

・ネットワーク管理者及びネットワーク担当者は、職員等のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、情報セキュリティ担当者に通知し適切な措置を求めなければならない。

（４）アクセス制御

ア　利用者登録

ネットワーク管理者及び情報システム管理者は、利用者の登録、変更、抹消、登録した情報資産の管理、異動や二本松市外への出向等の職員等及び退職者における利用者ＩＤの取扱い等については、定められた方法に従って行わなければならない。

必要な利用者登録・変更は、ネットワーク管理者又は情報システム管理者に対する申請により行う。

イ　管理者権限

（ア）ネットワークの管理者権限は、１人の者に与え厳重に管理しなければならない。

ネットワーク管理者の権限を代行する者は、ネットワーク管理者が指名し、最高情報統括責任者が認めた者でなければならない。代行者を認めた場合、最高情報統括責任者は速やかに統括情報セキュリティ担当者、情報セキュリティ担当者及び情報システム管理者に周知しなければならない。

（イ）情報システムの管理者権限は、必要最小限の者に与え、厳重に管理しなければならない。

情報システム管理者の権限を代行する者は、情報システム管理者が指名し、最高情報統括責任者が認めた者でなければならない。代行者を認めた場合、最高情報統括責任者は速やかにネットワーク管理者、統括情報セキュリティ担当者及び情報セキュリティ担当者に周知しなければならない。

（ウ）管理者権限のＩＤ・パスワードの設定は、外部委託業者に行わせてはならない。

ウ　インターネット以外のネットワークにおけるアクセス制御

ネットワーク管理者は、アクセス可能なネットワーク又はネットワーク上のサービス毎にアクセス出来る者を定めなければならない。

ネットワーク管理者及び情報システム管理者は、ネットワークサービスを使用する権限を有しない職員等が当該サービスを使用できるようにしてはならない。

エ　強制的な経路制御

ネットワーク管理者は、不正アクセスを防止するため、適切なネットワーク経路制御を施さなければならない。

オ　外部からのアクセス

外部からのアクセスの許可は、必要最低限にしなければならない。

カ　総合行政ネットワーク（ＬＧＷＡＮ）及び住民基本台帳ネットワークシステムとの接

続

総合行政ネットワーク（ＬＧＷＡＮ）及び住民基本台帳ネットワークシステムについては、当該接続において取り扱う情報資産の重要性を考慮し、適切なアクセス制御を実施する。

キ　外部ネットワークとの接続

（ア）外部ネットワークとの接続に当たり、当該外部ネットワークのネットワーク構成、機器構成、セキュリティレベル等を詳細に検討し、二本松市の全てのネットワーク、情報システム及び情報資産に影響が生じないと明確に確認したうえで、最高情報統括責任者の許可に基づき接続しなければならない。

その利用はネットワーク管理者の適切な管理下で行い、接続に際しては情報セキュリティに留意したネットワーク構成を採らなければならない。

この場合、当該外部ネットワークの瑕疵により二本松市のデータの漏洩、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理責任者による損害賠償責任を契約上担保しなければならない。

（イ）クラウドサービスを利用し、重要な情報資産（重要性分類Ⅱ以上）を取り扱う場合は、特に安全に配慮し、適切な措置を講じなければならない。

（ウ）接続した外部ネットワークのセキュリティに問題が認められ、二本松市の情報資産に脅威が生じることが想定される場合には、ネットワーク管理者の判断に従い、速やかに当該外部ネットワークを物理的に遮断しなければならない。

ク　ＩＤ・パスワードの管理方法

ネットワーク管理者又は情報システム管理者は、パスワードの発行に当たっては、仮のパスワードを発行し、ログイン後直ちに仮のパスワードを変更させなければならない。また、職員等のＩＤ・パスワードに関する情報を厳重に管理しなければならない。

（５）システム開発、導入、保守等

ア　情報システムの調達

（ア）ネットワーク管理者は応用ソフトウェアの開発、変更及び運用についての手順及び基準を明らかにしなければならない。

（イ）ネットワーク管理者は機器及び基本ソフトウェアの導入、保守及び撤去についての手順及び基準を明らかにしなければならない。

（ウ）ネットワーク管理者及び情報システム管理者は、情報システムの調達に当たっては、一般に公開する調達仕様書が情報セキュリティ確保の上で問題のないようにしなければならない。

（エ）ネットワーク管理者及び情報システム管理者は、機器及びソフトウェアを購入等する場合は、当該製品が情報セキュリティ上問題にならないかどうか、確認しなければならない。

イ　ネットワーク及び情報システムの更新

ネットワーク管理者及び情報システム管理者は、重要な情報資産（重要性分類Ⅱ以上）を取り扱うネットワーク及び情報システムを更新するに当たり、更新の内容、必要性、計画等を文書にて最高情報統括責任者に提出し承認を得なければならない。ネットワーク及びシステムの移行は、擬似環境による動作確認後に行わなければならない。移行の際にはシステムに記録されている情報資産の保存を確実に行い、復帰が即座に可能な状態にしておき、原則として執務時間外に行わなければならない。その作業を行う際には、職員２名以上で互いに確認しながら実施するとともに、作業内容を記録しなければならない。

また、システム更新後のリスク管理及び業務運営体制を明確にしなければならない。

ウ　情報システムの開発及び導入

ネットワーク管理者及び情報システム管理者は、システム開発及び保守時の事故・不正行為対策のため、次の事項を確認・実施しなければならない。

・責任者及び監督者
・作業者及び作業範囲
・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
・開発・保守するシステムと運用システムとの分離
・開発・保守に関するソースコードの提出
・開発・保守の際のセキュリティ上問題となりうる恐れのあるＯＳ、ミドルウェア及びアプリケーションソフトの使用禁止
・開発・保守の際のアクセス制限
・機器の搬出入の際の、情報システム管理者の許可及び確認
・開発・保守記録の提出義務
・マニュアル等の定められた場所への保管
・開発・保守を行った者の利用者ＩＤ、パスワード等の当該開発・保守終了後に不要となった時点での速やかな抹消
・守秘義務
・再委託管理

エ　システムの導入

（ア）情報システム管理者は、新たにシステムを導入する際には、手順を明確にし、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わなければならない。

（イ）情報システム管理者は、試験に使用したデータ及びその結果を最高情報統括責任者及びネットワーク管理者へ提出するとともに厳重に保管しなければならない。

（ウ）情報システム管理者は、個人情報及び機密性の高い生データを、試験用のデータとして使用してはならない。

（エ）情報システム管理者は、情報システムにおける入出力データの正確性を確保しなければならない。また、故意又は過失による情報の改ざん、漏洩を検出する機能を設けなければならない。

オ　ソフトウェアの保守及び更新

ソフトウェア（独自開発ソフトウェア及び汎用ソフトウェア）等を更新、又は修正プログラムを導入する場合は、不具合及び他のシステムとの相性の確認を行い、計画的に更新し又は導入しなければならない。

情報システム管理者は、情報セキュリティに重大な影響を及ぼす不具合に対する修正プログラムについて、速やかな対応を行うこととし、その他のソフトウェアの更新等については、計画的に実施しなければならない。

カ　システムの受託事業者への規定

（ア）新たなシステムの開発を外部の事業者に委託する場合は、ソースコードの提出を求め、再委託契約を行う際には再委託先について契約課において経営状況等、契約履行が可能であるか確認をとり、導入前の検査要求事項等を契約に定めなければならない。

（イ）信頼のおける事業者に委託するために、必要な資格等を定めなければならない。

（ウ）情報システム管理者は、作業中に身分証明書の提示を事業者に求め、契約で定められた資格を有するものが作業に従事しているか確認を行わなければならない。

また、守秘のための契約を事業者と結ばなければならない。

キ　機器の修理及び廃棄

（ア）記憶媒体の含まれる機器について、外部の事業者に修理させ又は廃棄する場合は、その内容が消去された状態で行わなければならない。

（イ）故障を外部の事業者に修理させる際、情報資産を消去することが難しい場合は、修理を委託する事業者に対し秘密を守ることを契約に定めなければならない。また重要な機器については、復元不可能な廃棄を行わなければならない。

ク　管理記録

ネットワーク管理者及び情報システム管理者は、担当するシステムにおいて行ったシステム変更等の作業については、記録を作成し適切に管理を行わなければならない。

（６）コンピュータウイルス対策

ア　無許可ソフトウェアの導入は禁止する。

イ　外部ネットワークから情報又はソフトウェアを取り入れる際には、ＦＷ段階でウイルスチェックを行うとともに、サーバ側、端末側においてもウイルスチェックを行なわなければならない。

ウ　外部のネットワークへ情報又はソフトウェアを送信する際にもＦＷ段階でウイルスチェックを行い外部へウイルスが拡散することを未然に防止しなければならない。

エ　ネットワーク管理者は、次の事項を実施しなければならない。

・常時ウイルスに関する情報収集に努めること。

・サーバ及び端末において、ウイルスチェックを行うこと。

・ウイルスチェック用ソフトウェアのパターンファイルは常に最新のものに保つこと。

・ソフトウェア等に関する公開された脆弱性の解消に対し、必要な措置を講じること。

オ　ネットワーク担当者は、次の事項を実施しなければならない。

・ウイルス情報について職員等に対する注意喚起を行うこと。

カ　情報システム管理者は、次の事項を実施しなければならない。

・サーバ及び端末において、ウイルスチェックを行うこと。

・ウイルスチェック用ソフトウェアのパターンファイルは常に最新のものに保つこと。

キ　職員等は、次の事項を遵守しなければならない。

・外部からデータ又はソフトウェアを取り入れる場合には、必ずウイルスチェックを行うこと。

・差出人が不明又は不自然に添付されたファイルは速やかに削除すること。

・ウイルスチェックの実行を途中で止めないこと。

・ネットワーク管理者が提供するウイルス情報を常に確認すること。

・添付ファイルのあるメールを送受信する場合は、ウイルスチェックを行うこと。

ク　ネットワーク管理者及び情報システム管理者は、職員等から報告のあった情報、システムの障害に対する処理又は問題等は障害記録として体系的に記録し、常に活用できるよう保存しなければならない。

（７）不正アクセス対策

ア　ネットワーク管理者は、次の事項を実施しなければならない。

・使用終了若しくは使用される予定のないポートを長期間空けた状態のままにしてはならない。

・セキュリティホールの発見に努め、メーカー等からパッチの提供があり次第速やかにパッチを当てなければならない。

・重要なシステムの設定に係るファイル等について、定期的に当該ファイルの改ざんの有無を検査すること。

イ　攻撃を受けることが明確な場合には、ネットワーク管理者はシステムの停止を含む必要な措置を講じなければならない。

また、関係機関との連絡を密にして情報の収集に努めなければならない。

ウ　ネットワーク管理者は、職員等及び外部委託業者が使用しているパソコン等の端末からの庁内のサーバ等及び外部のサイトに対する攻撃を監視しなければならない。

エ　攻撃を受け、当該攻撃が不正アクセス禁止法違反等犯罪の可能性がある場合には記録の保存に努めるとともに、警察・関係機関との緊密な連携に努めなければならない。

オ　攻撃の可能性が明確であるにもかかわらず職員等の怠惰が原因でデータの漏洩、破壊、改ざん又はシステムダウン等により業務に深刻な影響をもたらした場合、当該職員等を地方公務員法による懲戒の対象とする。

カ　職員等による不正アクセスがあった場合、ネットワーク管理者又は情報システム管理者は当該職員等が所属する課室等の情報セキュリティ担当者に通知し、適切な処置を求

めなければならない。
　職員等による不正アクセスの結果、データの漏洩、破壊、改ざん又はシステムダウン等により業務に深刻な影響をもたらした場合、当該職員等を地方公務員法による懲戒の対象とし、悪質な場合には刑事告発の対象とする。

キ　ネットワーク管理者は、不正アクセスの監視のため、保有する個人情報を含むか又は含むおそれがある一定量以上の情報が情報システムからダウンロードされた場合に警告表示がなされるよう措置を講じなければならない。また、その措置について定期的に確認をしなければならない。

ク　ネットワーク管理者及び情報システム管理者は、サービス不能攻撃や標的型攻撃に対して、攻撃を受ける可能性があることを想定して、対策を施さなければならない。

（８）セキュリティ情報の収集

ア　ネットワーク管理者、ネットワーク担当者及び情報セキュリティ担当者は、情報セキュリティに関する情報を収集し、二本松市の全てのネットワーク及び情報システムについてソフトウェアにパッチを当てる等、セキュリティ対策上必要な措置を講じなければならない。

イ　最高情報統括責任者は、これらの情報を定期的に取りまとめ、関係部局等に通知するとともに、情報セキュリティポリシーの改定につながる情報については二本松市電子情報化推進本部に報告しなければならない。

ウ　ネットワーク管理者は、緊急時対応計画に定める緊急に連絡すべき情報を入手した場合は当該計画に定める情報連絡先に連絡しなければならない。

７　運用

（１）情報システムの監視

ア　セキュリティに関する事案を検知するため、ネットワーク管理者及び情報システム管理者は、常に情報システムの監視を行わなければならない。

イ　外部と常時接続するシステムについては、ネットワーク侵入監視装置を設置し、２４時間監視を行わなければならない。

ウ　内部のシステムについて、アクセスコントロール等を行い、異常な運用等の監視を行わなければならない。

エ　情報システムの監視に当たっては、サーバ間の時刻同期を行い、監視した記録を保存しなければならない。

オ　監視により得られた結果については、盗難、改ざん、消去等を防止するために必要な措置を施し、安全な場所に保管しなければならない。また、これらの記録の正確性を確保するため、正確な時刻の設定を行わなければならない。

（２）情報セキュリティポリシーの遵守状況の確認

ア　統括情報セキュリティ担当者及び情報セキュリティ担当者は、情報セキュリティポリシーが遵守されているかどうかについて、また、問題が発生していないかについて常に確認を行い、問題が発生していた場合には速やかに最高情報統括責任者及びネットワーク管理者に報告しなければならない。

イ　最高情報統括責任者は発生した問題に速やかに適切に対処しなければならない。

ウ　職員等は、情報セキュリティポリシーの違反が発生した場合は、直ちにネットワーク管理者及び情報セキュリティ担当者に報告を行わなければならない。違反の発生時には、それが直ちに情報セキュリティ上重大な影響を及ぼす可能性があるとネットワーク管理者が判断した場合は、緊急時対応計画に従って連絡を行わなければならない。

エ　ネットワーク管理者及び情報システム管理者は、サーバ等のシステム設定が情報セキュリティポリシーを遵守しているかどうかについて、また問題が発生していないかにつ

いて定期的に確認を行い、問題が発生していた場合には速やかに適切に対処しなければならない。

オ　最高情報統括責任者は、不正アクセス、不正プログラム等の調査のために、端末等のアクセス記録、電磁的記録媒体等のログ、電子メール等の送受信記録等の情報を閲覧できる権限を有する職員を情報セキュリティ実施手順に定めなければならない。ただし、法令で定められた個人情報の保護に関係する情報の閲覧に関しては、当該法令に定められた手続に従う。

カ　情報セキュリティ担当者は、職員等が常に情報セキュリティポリシー及び実施手順を参照できるよう配慮しなければならない。

（３）侵害時の対応

情報資産への侵害が発生した場合における連絡、証拠保全、被害拡大の防止、復旧等の必要な措置を迅速かつ円滑に実施し、再発防止の措置を講じるために、緊急時対応計画を次のとおり定める。

ア　連絡先

具体的には、情報システムごとに情報セキュリティ実施手順に明記する。

・二本松市長
・最高情報統括責任者
・ネットワーク管理者
・ネットワーク担当者
・情報システム管理者
・ネットワーク及び情報システムに係る外部委託事業者
・秘書広報課
・総務省
・福島県（情報セキュリティ担当部署）
・警察
・関係機関
・影響が考えられる個人及び法人

イ　事案の調査

セキュリティに関する事案を認めた者は、次の項目について、速やかにネットワーク管理者に報告しなければならない。

・症状の分類
・事案が発生した原因として、想定される行為
・確認した被害・影響範囲
・記録

ネットワーク管理者は、事実の詳細な調査を行うとともに、最高情報統括責任者との情報共有及び二本松市電子情報化推進本部への報告を行わなければならない。

ウ　事実への対処

（ア）ネットワーク管理者は、次の事実が発生した場合、それぞれ定められた連絡先へ連絡しなければならない。

・サイバーテロその他市民に重大な被害が生じる恐れがあるとき（二本松市長、最高情報統括責任者、総務省、福島県、警察、影響が考えられる個人及び法人）
・不正アクセスその他犯罪と思慮されるとき（二本松市長、最高情報統括責任者、総務省、福島県、警察）
・踏み台となって他者に被害を与える恐れがあるとき（二本松市長、最高情報統括責任者、総務省、福島県、警察）
・情報システムに関する被害（情報システム管理者、必要と認められる事業者等）
・その他情報資産に係る被害（関係部局等）

（イ）ネットワーク管理者は、次の事実が発生し情報資産の防護のためにネットワークの

切断がやむを得ない場合は、ネットワーク管理者自ら又は職員等に指示し、当該端末のＬＡＮケーブルの即時取外し、又は機器の電源の強制的な遮断など、速やかにネットワークを切断する措置を講ずる。
・異常なアクセスが継続しているとき、又は不正アクセスが判明したとき
・システムの運用に著しい支障をきたす攻撃が継続しているとき
・コンピュータウイルス等不正プログラムがネットワーク経由で拡がっているとき
・情報資産に係る重大な被害が想定されるとき

（ウ）情報システム管理者は、次の事案が発生し情報資産の防護のために情報システムの停止がやむを得ない場合は、情報システムを停止し、情報システム管理者自ら又は職員等に指示し、当該システムのＬＡＮケーブルの即時取外し、又は機器及び当該システムに接続する端末の電源の強制的な遮断など、速やかにネットワークを切断する措置を講ずる。また、その講じた措置について、速やかにネットワーク管理者に報告しなければならない。
・コンピュータウイルス等不正プログラムが情報資産に深刻な被害を及ぼしているとき
・災害等により電源を供給することが危険又は困難なとき
・その他の情報資産に係る重大な被害が想定されるとき

（エ）ネットワーク担当者は、事案に係るシステムのアクセス記録及び現状を保存し、事実に対処した経過を記録する。

（オ）ネットワーク管理者は、事案に係る証拠保全の実施を完了するとともに、再発防止の暫定措置を検討し、再発防止の暫定措置を講じた後、復旧する。また、復旧後、必要と認められる期間、再発監視を行う。

エ　再発防止の措置

（ア）ネットワーク管理者は、当該事実に係るリスク分析を実施し、情報セキュリティポリシー及び実施手順の改善に係る再発防止計画を策定し、二本松市電子情報化推進本部へ報告しなければならない。

二本松市電子情報化推進本部は、情報セキュリティポリシー及び実施手順の改善に係る再発防止計画が有効であると認められる場合は、これを承認する。

（イ）ネットワーク管理者は、各種セキュリティ対策の改善に係る再発防止計画を策定し、最高情報統括責任者へ報告しなければならない。最高情報統括責任者は、これらの再発防止計画が有効であると認められる場合は、これを承認し、事実の概要と併せ職員等に周知しなければならない。

（ウ）ネットワーク管理者及び情報システム管理者は、情報セキュリティを取り巻く状況の変化や組織体制の変動に応じ、必要に応じて、緊急時対応計画を見直さなければならない。なお、見直しに当たっては、最高情報統括責任者の承認を受けなければならない。

（４）外部委託による運用契約

運用を外部委託する場合は、委託に関する責任を有する部署を明確にするとともに、外部委託事業者に対し必要なセキュリティ要件を記載した契約書による契約を締結しなければならない。

委託に関する責任を有する部署は、委託先において必要なセキュリティ対策が確保されていることを確認し、その内容をネットワーク管理者に報告するとともに、その重要度に応じて最高情報統括責任者に報告しなければならない。

（５）例外措置

ア　例外措置の許可

情報セキュリティ担当者及び情報システム管理者は、情報セキュリティ関係規定を遵

守することが困難な状況で、行政事務の適正な遂行を継続するため、遵守事項とは異なる方法を採用し、又は遵守事項を実施しないことについて合理的な理由がある場合には、最高情報統括責任者の許可を得て、例外措置を取ることができる。

イ　緊急時の例外措置

情報セキュリティ担当者及び情報システム管理者は、行政事務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、事後速やかに最高情報統括責任者に報告しなければならない。

ウ　例外措置の申請書の管理

最高情報統括責任者は、例外措置の申請書及び審査結果を適切に保管しなければならない。

8　法令遵守

職員等は、職務の遂行において使用する情報資産について、次の法令等を遵守しこれに従わなければならない。

- 地方公務員法(昭和２５年法律第２６１号)
- 著作権法（昭和４５年法律第４８号）
- 不正アクセス行為の禁止等に関する法律（平成１１年法律第１２８号）
- 行政機関の保有する個人情報の保護に関する法律（平成１５年法律第５８号）
- 行政手続における特定の個人を識別するための番号の利用等に関する法律（平成２５年法律第２７号）
- 二本松市個人情報保護条例（平成１７年二本松市条例第１８号）
- 二本松市電子計算機処理に係る管理運営規程（平成１７年二本松市訓令第１２号）
- 二本松市特定個人情報等の安全管理に関する規程（平成２７年二本松市訓令第１６号）

9　情報セキュリティに関する違反に対する対応

情報セキュリティポリシーに違反した職員等及びその監督責任者に対しては、その重大性、発生した事実の状況等に応じて地方公務員法による懲戒処分の対象とする。

なお、職員等に情報セキュリティポリシーに違反する行動がみられた場合には、速やかに次の措置を講じなければならない。

- ネットワーク管理者が違反を確認した場合は、ネットワーク管理者は当該職員等が所属する課室等の情報セキュリティ担当者に通知し、適切な措置を求めなければならない。
- 情報システム管理者等が違反を確認した場合は、違反を確認した者は速やかにネットワーク管理者及び当該職員等が所属する課室等の情報セキュリティ担当者に通知し、適切な措置を求めなければならない。
- 情報セキュリティ担当者の指導によっても改善されない場合、ネットワーク管理者は、当該職員等のネットワーク又は情報システムの使用に関する権利を停止あるいは剥奪することができる。その後速やかに、ネットワーク管理者は、職員等の権利を停止あるいは剥奪した旨を最高情報統括責任者及び当該職員等が所属する課室等の情報セキュリティ担当者に通知しなければならない。

１０　評価・見直し

（１）監査

ア　二本松市電子情報化推進本部は、ネットワーク及び情報システムの情報セキュリティについて監査を定期的に行わなければならない。

なお、ネットワーク管理者及び情報システム管理者は、監査とは別に所管するネットワーク及び情報システムについて点検を実施しなければならない。

イ　外部委託事業者に委託している場合は、外部委託事業者から下請けとして受託している事業者も含めて、情報セキュリティポリシーの遵守について、必要に応じ、監査を実施しなければならない。

ウ　二本松市電子情報化推進本部は監査結果を取りまとめ、この報告結果を最高情報統括責任者及びネットワーク管理者に通知するとともに、情報セキュリティポリシーの更新の際に参照する情報資産として活用しなければならない。

エ　最高情報統括責任者は、監査結果を踏まえ、指摘事項を所管する統括情報セキュリティ責任者に対し通知し、当該事項への対処を指示するとともに、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。

オ　二本松市電子情報化推進本部は、監査を実施するため、必要に応じ、職員のうち十分な専門的知識を有する者を指名して内部監査班を組織し、監査を行うことができる。この場合、内部監査班は、監査結果を二本松市電子情報化推進本部に報告しなければならない。

（２）点検

情報セキュリティ担当者は、情報セキュリティポリシーに沿った情報セキュリティ対策が実施されているかどうかについて職員等にアンケート等を行い、また、自己点検を行わなければならない。統括情報セキュリティ担当者はこれを取りまとめ、二本松市電子情報化推進本部に報告する。二本松市電子情報化推進本部は、この報告結果を情報セキュリティポリシーの更新の際に参照する情報資産として活用することとする。

（３）情報セキュリティポリシーの更新

新たに必要な対策が発生した場合又は監査の結果及び点検の結果を踏まえ、二本松市電子情報化推進本部において情報セキュリティポリシーの実効性を評価し、必要な部分を見直し、更新の内容、時期等について検討を行う。情報セキュリティポリシーの更新に当たっては、この検討結果に基づき、実施することとする。