一般社団法人練馬区産業振興公社の
情報セキュリティ対策に関する規程

（平成26年4月1日規程第31号）

第１章　総則

（目的）

第１条　この規程は、一般社団法人練馬区産業振興公社情報セキュリティポリシー（以下「セキュリティポリシー」という。）に基づき、一般社団法人練馬区産業振興公社（以下「公社」という。）における情報セキュリティに関する対策（以下「情報セキュリティ対策」という。）の実施に関し、必要な事項を定めることを目的とする。

（定義）

第２条　つぎに掲げる用語の定義は、当該各号に定めるとおりとする。

⑴　情報システム

公社が管理する情報機器、ソフトウェア、情報ネットワークによって構成されるシステムの総称をいう。

⑵　情報機器

電子データを処理し､保管することが可能な機器のうち､職員が使用するパソコン、他の情報機器が利用するデータ等を蓄積したサーバをいう。

⑶　ソフトウェア

オペレーティングシステムやアプリケーションソフト等、端末が動作するプログラムの総称をいう。

⑷　ネットワーク

情報機器間で電子データを送受信するネットワークをいう。

⑸　帳票

公社において事務処理上の必要から紙に出力したもの、または職務上管理を要するものをいう。

⑹　記録媒体

フロッピーディスク、ＣＤ、ＭＯ、磁気テープ、ＵＳＢフラッシュメモリ等の移動が容易な各種外部記憶媒体をいう。

第２章　組織・体制

（情報セキュリティ統括責任者）

第３条　公社における情報セキュリティに関する最終的な権限および責任を有するものとして、情報セキュリティ統括責任者を置く。

２　情報セキュリティ統括責任者は、常務理事をもって充てる。

３　情報セキュリティ統括責任者は、情報セキュリティ責任者に対し、情報システムおよび情報セキュリティの状況等について報告を求め、または助言することができる。

（情報セキュリティ責任者）

第４条　公社における情報システムおよび情報セキュリティに関する権限および責任を有するものとして、情報セキュリティ責任者を置く。

２　情報セキュリティ責任者は、事務局長をもって充てる。

３　情報セキュリティ責任者は、公社における情報セキュリティ対策に関して、職員に対する教育や研修、助言および指示を行うものとする。

４　公社における情報システムの運用管理ならびに情報セキュリティ対策の実務等については、情報セキュリティ責任者があらかじめ指名するものに行わせることができる。

（職員の責務）

第５条　職員は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たっては、セキュリティポリシーを遵守し、必要な情報セキュリティ対策を講じなければならない。

２　職員は、情報セキュリティ責任者が実施する教育や研修を受講しなければならない。

（外部への委託）

第６条　情報システムに関わる業務を外部事業者に委託する場合は、次に掲げる事項を契約書等に明記しなければならない。

⑴　権利および義務の譲渡禁止に関する事項

⑵　第三者への提供および再委託の禁止、制限に関する事項

⑶　漏えいおよび盗用の防止に関する事項

⑷　秘密の保持に関する事項

⑸　事故発生時の報告義務に関する事項

第３章　情報システムの管理

第１節　ネットワーク管理

（ネットワークの原則）

第７条　公社は、インターネットと公社内ネットワークの境界にファイアウォールを設置し、外部からの不正なアクセスを防止しなければならない。

２　公社は、オープンエリアから、許可されていない端末が公社内ネットワークに接続することを防止する措置を講じる。

第２節　アクセス管理

（アクセス制御の原則）

第８条　情報セキュリティ責任者は、情報システムの取り扱いにあたり、アクセス制限を実施する。

（アカウントの発行）

第９条　情報システムのユーザアカウントは、業務の遂行に必要な範囲で発行するものとし、共有は禁止とする。

２　情報セキュリティ責任者は、情報システムのユーザアカウントを適切な方法で職員に発行し、ユーザアカウントの発行状況およびアクセス権限の範囲等を職員別に作成する「システムユーザ管理簿」に記録する。

3　情報セキュリティ責任者は、職員が、異動や退職等によって担当する業務の変更が生じた場合は、速やかに当該職員が有していたアカウントＩＤを無効化または変更を行い、当該職員の「システムユーザ管理簿」を更新する。

（パスワードの管理）

第10条　ユーザアカウントの認証は、原則としてパスワード認証とする。

2　前項のパスワードは、英字、数字、記号のうち少なくとも２種類を使用した、６文字以上の文字列とする。

3　情報セキュリティ責任者は、ＯＳのログイン認証に用いるパスワードの付与およびパスワードのリセットを少なくとも６か月に１回行う。

4　職員は、他人に自らのパスワードを教えてはならない。

5　職員は、他人にパスワードを知られた場合は、速やかに情報セキュリティ責任者にその旨を通知し、新たなパスワードの付与を受ける。

第３節　情報機器の管理

（情報機器の把握）

第11条　情報セキュリティ責任者は、公社が保有する情報機器の導入・利用・処分状況を管理するため、次の事項を記載した「情報機器管理台帳」を作成する。

⑴　情報機器の管理番号もしくは情報機器名（型番）

⑵　利用部門もしくは設置場所

⑶　導入日

⑷　廃棄日（リースの場合は返却日）

⑸　ウイルス対策ソフトウェアの有無

⑹　公社外への持ち出しの可否

2　情報セキュリティ責任者は、情報機器の導入、処分等の変更が発生した場合は、「情報機器管理台帳」を更新する。

（情報機器の接続の制限）

第12条　公社外の情報機器を公社内ネットワークに接続することは原則禁止とする。

2　職員は、業務上止むを得ず、外部の情報機器を公社内ネットワークに接続する場合は、次の事項を記載した「ネットワーク接続申請書（第1号様式）」を起票し、情報セキュリティ責任者の承認を得るものとする。

⑴　情報システムに接続する情報機器

⑵　情報システムに接続する目的

⑶　情報システムへの接続に際し確認すべき事項（接続期間、個人情報の取扱いなど）

（情報機器の持ち出しの管理）

第13条　情報セキュリティ責任者は、公社外へ持ち出すノートパソコン等の情報機器について、「情報機器管理台帳」により明確にする。

2　職員は、「情報機器管理台帳」により持ち出しを許可されていない情報機器は、持ち出してはならない。

3　職員は、業務上やむを得ず、許可されていない情報機器を持ち出す場合は、「情報機器外部使用届（第２号様式）」を作成し、情報セキュリティ責任者の承認を得るもの

とする。

（不正操作の防止措置）

第14条　職員は、情報機器の不正操作等を防止するため、離席時に、パスワード付スクリーンセーバを起動させるか、画面をロック（ログオフ含む）する。

２　職員は、パスワード付スクリーンセーバを１０分以内で起動するように設定する。

（情報機器の盗難防止）

第15条　職員は、ノートパソコンの紛失・盗難を防止するため、チェーンロック等により所定の位置に固定するか、業務終了後に施錠可能な場所で保管する。

（情報機器の廃棄処理）

第16条　情報セキュリティ責任者は、情報機器を廃棄する場合には、ハードディスク内の情報を完全に消去することができるソフトウェアを利用して、情報機器内の情報を消去する又はハードディスクを物理的に破壊し、ハードディスク内の情報が復元不可能な状態で廃棄する。

（サーバの設置）

第17条　情報セキュリティ責任者は、ラック内に施錠して格納する等の方法により、サーバの盗難防止措置、倒壊防止措置を講じる。

２　情報セキュリティ責任者は、サーバには無停電電源装置（ＵＰＳ）を設置するなどし、停電対策を講じるものとする。

第４節　バックアップの管理

（サーバ内のデータのバックアップ）

第18条　情報セキュリティ責任者は、サーバに保存されたデータについては、定期的にバックアップを行うものとする。

第５節　ソフトウェアの管理およびウイルス対策

（ソフトウェアの利用制限）

第19条　職員は、業務に不要なソフトウェアをインストールし、利用してはならない。

２　職員は、ＯＳのセキュリティ設定を変更してはならない。

（セキュリティパッチの適用）

第20条　情報セキュリティ責任者は、ソフトウェアに関するセキュリティパッチが公開された場合は、職員に通知して導入を指導し、利用するソフトウェアを常に最新の状態であるように保つものとする。

（ウイルス対策ソフトの導入）

第21条　情報セキュリティ責任者は、公社内ネットワークまたはインターネットに接続するすべての情報機器に、ウイルス対策ソフトを導入する。

（ウイルス対策ソフトの稼働）

第22条　職員は、ウイルス対策ソフトの定義ファイルを常に最新の状態に維持する。

２　職員は、ウイルス対策ソフトを常に稼働させる。

３　職員は、少なくとも１か月に１度、ウイルス対策ソフトによりハードディスクを完全スキャンする。

4　職員は、ウイルス対策ソフトの設定を許可なく変更してはならない。

第６節　インターネット、電子メールの利用

（インターネットの閲覧制限）

第23条　職員は、インターネットブラウザを利用して業務とは明らかに関係のないページを閲覧してはならない。

2　職員は、業務上知り得た機密情報をインターネット上の掲示板、ブログ等に書き込んではならない。

（電子メールの利用）

第24条　職員は、公社が管理する端末以外で、公社が発行するメールアカウントを許可なく利用してはならない。

2　職員は、受信した電子メールを許可なく個人の情報機器や携帯電話等に転送してはならない。

3　職員は、電子メールを送信する場合、送信先の電子メールアドレスの誤入力に注意する。

4　職員は、個人情報および機密性の高いデータファイルを電子メールによって送信する場合には、データの暗号化やパスワード設定により、第三者による盗聴を防止する。

5　前項について、職員は、送信先にデータの復号のためのパスワード等を伝える場合は、電話もしくは当該データの送信メールとは異なるメールにより行うものとする。

第４章　媒体の管理

（媒体の保管）

第25条　職員は、個人情報などの重要情報を含む帳票および記録媒体（以下「媒体」という。）について、適切な保管期間を定めた上で、キャビネット等で施錠保管する。

（帳票の使用）

第26条　職員は、個人情報などの重要情報を含む帳票については、紛失や盗難を防止するため、以下の事項を実施する。

⑴　帳票を机の上や出力したままプリンタ上に放置しないようにする。

⑵　一時的に使用した帳票は、速やかに保管場所へ戻す。

⑶　帳票を公社外へ持ち出す場合は、鞄や箱などに入れ、手元から離さないようにする。

⑷　帳票を持って直帰しない。

⑸　車内に帳票を保管し、車を離れる場合は車を施錠する。

⑹　帳票を閲覧する場合は、第三者に閲覧されないように注意する。

（記録媒体の利用）

第27条　職員は、職務上記録媒体を利用する必要がある場合は、情報セキュリティ責任者が許可をした記録媒体を利用しなければならない。

2　情報セキュリティ責任者は、許可をした記録媒体については、「記録媒体管理台帳」に記録し、定められた保管場所にて管理を行う。

3　職員は、記録媒体を利用する場合は、公社の内外に関わらず、「記録媒体利用管理簿」に次の事項を記録し、情報セキュリティ責任者の承認を得なければならない。

⑴　記録媒体の利用開始日

⑵　記録媒体の管理番号
⑶　利用者
⑷　利用目的
⑸　記録媒体の返却日

4　職員は、記録媒体を公社外へ持ち出す場合は、盗難、紛失に十分注意するとともに、個人情報などの重要情報を書き込む場合は、パスワード設定やデータの暗号化を行い、情報漏えい策を講ずる。

5　職員は、記録媒体の利用終了後は、バックアップなどで長期保管する必要がある場合を除き、速やかに書き込んだ情報を削除し、保管場所に返却する。

（媒体の処分）

第28条　職員は、保管期間が経過した媒体について、シュレッダー等を用いて廃棄もしくは消去（データフォーマット）する。

2　職員は、一時的にコピー又はプリントアウトした資料、メモ類や誤複写等の帳票は、業務終了後、速やかに廃棄する。

第５章　公社内の安全性の確保

第１節　総則

（エリアのゾーニング）

第29条　情報セキュリティ責任者は、個人情報の安全性を確保するため、施設のエリアを次の２区分とし、入室者を制限する。

⑴　オープンエリア
⑵　ワーキングエリア

2　情報セキュリティ責任者は、前項のエリア区分および出入り口の位置を明確にした「フロア見取り図」を作成する。

（オープンエリアのセキュリティ基準）

第30条　オープンエリアは、営業時間中は、一般に開放し、特段の入室制限は設けないものとする。ただし、不審者を発見した場合は、この限りでない。

（ワーキングエリアのセキュリティ基準）

第31条　ワーキングエリアは、原則として職員のみが入室できるエリアとし、許可された者以外の入室を制限する。

2　ワーキングエリアに、職員以外の者が立ち入る場合は、原則として職員の同行を必要とする。

（施錠の原則）

第32条　職員は､退勤時またはその他の外出時にキャビネット等のある執務室を施錠する。

第２節　入退室の管理

（職員の入室）

第33条　当日最初に出勤した職員は、解錠して入室し、不正侵入等の有無を確認する。

2　前項において、不正侵入等の異常を発見した場合は、速やかに情報セキュリティ責任者に連絡する。

（職員の退室）

第34条　当日最後に執務室から退勤する職員は、キャビネット、窓の施錠状況、パソコンのシャットダウンの実施状況、ノートパソコン放置の有無を確認する。

2　当日最後に執務室から退勤する職員は、出入り口を施錠して退室する。

（入退記録の管理）

第35条　情報セキュリティ責任者は、公社の設備に応じてタイムカード等により、以下の記録を保管する。

⑴　当日最初の入室者および入室時刻

⑵　当日最後の退室者および退室時刻

2　情報セキュリティ責任者は、前項により徴収した記録を1か月に1度確認し、不正な入退室の有無を確認する。

（来訪者の入退室）

第36条　職員は、来訪者を執務室内に入室させる場合は、原則としてオープンエリアに限定する。

2　職員は、やむを得ず来訪者をワーキングエリアに入室させる場合は、当該来訪者に常時同行するものとし、必要に応じて、以下の事項について記録する。

⑴　来訪者の氏名、所属（会社名等）および来訪人数

⑵　来訪目的

⑶　対応した職員名

⑷　来社および辞去時刻

第3節　施錠鍵の管理

（施錠鍵の貸与）

第37条　各部署における担当者は、公社の施錠鍵、セキュリティカード、キャビネットおよびサーバラック等に備わる施錠鍵を用意し、施錠鍵を必要とする職員に限定して使用する。

第6章　緊急時対応

（緊急時対応手順の策定）

第38条　情報セキュリティ責任者は、情報システムの障害や情報セキュリティの事件および事故の発生時における対応手順を定めるものとする。

2　情報セキュリティ責任者は、前項の緊急時対応手順を職員に周知徹底するものとし、必要に応じて、事件や事故の発生を想定した訓練を行う。

（緊急時対応）

第39条　情報セキュリティ責任者は、セキュリティ事故等が発生した場合は、前条の対応手順に基づき、被害拡大の防止、早期復旧を図らなければならない。

2　セキュリティ事故等を発見もしくは発生連絡を受けた職員は、速やかに障害状況等の把握を行うとともに、情報セキュリティ責任者への状況報告および関係者への連絡を行う。

3　情報セキュリティ責任者は、職員からセキュリティ事故等の報告を受けた場合は、

速やかに情報セキュリティ統括責任者に報告する。

（緊急連絡網の整備）

第40条　情報セキュリティ責任者は、緊急時の初動対応を迅速に行うため、内部組織および関連事業者との緊急連絡網を整備する。

付　則

この規程は、平成26年4月1日から施行する。

第 1 号様式（第 12 条関係）

年　　月　　日

事務局長	総務係長

一般社団法人練馬区産業振興公社
情報セキュリティ責任者　殿

利用者　所　属
氏　名

ネットワーク接続申請書

一般社団法人練馬区産業振興公社情報システムに、下記のとおり接続の承認をお願いいたします。

記

１　接続機器

２　接続期間

３　接続目的

４　その他（個人情報の取扱いなど）

５　担当

第 2 号様式（第 13 条関係）

年　　月　　日

事務局長	総務係長

一般社団法人練馬区産業振興公社
　　情報セキュリティ責任者　殿

使用者　所　属
　　氏　名

情報機器外部使用届

一般社団法人練馬区産業振興公社の情報機器を下記のとおり、公社外にて使用いたします。

記

1　情報機器

2　使用期間

3　使用場所

4　その他（個人情報の取扱いなど）

5　担当