

# 情報システム管理規定

制定 2022年1月27日

株式会社 Brain Trust from The Sun

## 第1章 総則

### (目的)

第1条 この規定は、当社の行う小規模不動産特定共同事業における電子取引業務に関して、業務上取扱う情報及び情報システムの管理方法、管理体制等を定めることにより、当社における情報等を適正に管理するとともに当社が有する機密情報等の社外漏えいを防止し、もって当社の社会的信用の維持向上を図ることを目的とする。

### (定義)

第2条 この規定において「情報資産」とは、情報及びその記録媒体をいい、具体的には以下のものとする。なお、情報の内容としては、個人情報、顧客・取引先情報、役職員に関する情報、取引内容等のあらゆる情報を含むものとする。

- (1) ハードディスク・サーバー・可搬媒体等に保存される電子情報
  - (2) 印刷物、音声、画像・映像、企画・アイデア、経営上の意思決定等の有形無形の非電子情報
  - (3) コンピュータ及び周辺機器、サーバー、コンピュータネットワーク、ソフトウェア等を含む情報システム
- 2 この規定において「情報セキュリティ」とは、当社の保有する情報資産について、機密性・完全性・可用性の観点から、その安全性（セキュリティ）を確保し、適切に取扱うことをいう。
- 3 この規定において「機密情報」とは、当社及び当社が受託した業務に関わる当事者に関係する一切の事実又は評価であって、その様態が文書、写真、映像、音声等のいずれであるかを問わず、無断で開示したり、目的外に利用することが禁止されている情報をいい、機密情報と明示されているか否かを問わないものとする。ただし、以下の各号に掲げる情報は除くものとする。
- (1) 既に公知となっている情報
  - (2) 当社の責めによらない事由により公知になった情報
  - (3) 第三者から秘密保持義務を負うことなく合法的に入手した情報
- 4 この規定において「情報システム」とは、情報を保存・利用するためのネットワークシステム、情報機器、ソフトウェア、電子媒体等をいう。
- 5 この規定において「情報システム端末」とは、パソコン、タブレット、スマートフォンその他の情報システムを利用するための端末をいう。
- 6 この規定において「ネットワーク」とは、当社内の LAN・電話回線・無線等で結ばれ

たサーバー・パソコン等の集合体をいう。

- 7 この規定において「ユーザアカウント」とは、各種情報システムへのログインユーザIDその他の情報システムの利用者を識別するための標識となる文字をいう。
- 8 本規定において「役職員」とは、取締役からなる役員、当社内にあって直接又は間接に当社の指揮監督を受けて当社業務に従事している者をいい、当社と雇用関係にある従業員（嘱託社員、パート社員及びアルバイト社員を含む）のみならず、当社との出向契約に基づき業務に従事する出向者及び労働派遣契約に基づき派遣される派遣労働者も含むものとする。

#### （基本方針）

- 第3条 当社は、法令等諸規則を遵守するとともに、当社が実施するあらゆる事業を通じて機密情報の適正な取扱いを実施し、その保護に努めるものとする。
- 2 当社は、顧客情報の流出被害を防ぐため、個人情報保護法及び同法についてのガイドラインで示されるレベルと同様の管理体制を整備し、個人情報の流出を防止するための十分な措置を講じるものとする。
  - 3 当社は、システム障害時に対応するための適切な人員配置を行う等、社内の内部管理体制を整備するものとする。

#### （役職員の責務）

- 第4条 役職員は、機密情報を第三者に開示又は漏洩してはならず、退職後も同様とする。
- 2 役職員は、機密情報を会社の業務以外の目的に使用してはならず、退職した後も同様とする。
  - 3 前各二項の規定は、顧客との契約及び法令諸規則に抵触しない場合で、業務上機密情報を第三者に開示又は使用する必要があるときは、この限りでない。

## 第2章 情報管理体制

#### （統括部門・情報システム管理責任者）

- 第5条 当社の情報システム管理に関する統括部門は、情報システム部（システム）とする。
- 2 当社の情報システム管理責任者は、情報システム部（システム）部長とし、次に掲げる職務を行うものとする。
    - （1）「情報システム管理規定」の周知・指導
    - （2）情報資産の管理及び取扱いに関する指導監督
    - （3）情報資産の紛失や漏洩発生時の対応（未然防止・再発防止策の策定を含む）
    - （4）情報システム管理者からの情報収集、情報システム管理者への連絡・指示
    - （5）上記の他、不動産特定共同事業法、不動産特定共同事業法施行令、不動産特定共同事業法施行規則及び「不動産特定共同事業法の電子取引業務ガイドライン」を遵守する為に必要な対応
  - 3 前項に掲げる情報システム管理責任者は、情報システム管理を行う上で必要かつ適切

な知識及び経験を有する者を任命する。また、当該適任者の任命を実現するため、当社は情報システム管理を十分に行うための予算確保及び人材の育成を行うものとする。

(情報システム管理者)

第6条 当社の情報システム管理者は、当社の最小組織単位（部）ごとに、その部門の責任者が務めるものとし、情報システム管理者は、自らの所属部門に属する役職員の情報資産の一切の取扱いにつき、これを管理・指導し、その責任を有するものとする。

- 2 情報システム管理者は、この規定に従い、自らの部門に存在する情報資産の所在、内容、利用者、規模等を把握し、情報等の適正な取扱いを維持・管理しなければならない。
- 3 情報システム管理者は、自らの部門において情報漏洩等の事故又は違反の発生又はその疑いが生じた場合は、直ちにその旨を情報システム管理責任者に報告し、指示を求めなければならない。

### 第3章 機密情報

(機密情報の分類)

第7条 当社は、当社の情報資産を「非公開情報」と「公開情報」とに分類し、「非公開情報」を機密情報として取扱う。

- 2 当社は、機密情報を、その重要性により、次の種類に分類して管理するものとし、その分類は情報システム管理責任者が決定するものとする。

(1) 極秘情報

秘密保持の必要度が極めて高く、万が一関係者以外に漏えいすると会社全体又は当該業務全体に極めて重大な損害を与えるリスクがあるもの。その内容の共有は、特に命ぜられた管理者等の極めて限られた少人数の特定関係者以外は許されない。

(2) 社外秘情報

万が一社外に漏洩すると会社に損害を与えるおそれがあるもの。その共有は当社役職員のみに限られ、外部には漏らしてはならない。

- 3 当社は、小規模不動産特定共同事業における電子取引業務に際して取扱う顧客に関する情報（以下「顧客情報」という）について、非公開情報の内の「社外秘情報」として取扱うものとする。なお、顧客情報の中でも特に取扱いに注意すべき機微（センシティブ）情報については、非公開情報の内の「極秘情報」として厳正な取扱いを行う。

(機密情報の保管・管理)

第8条 機密情報は、施錠できる保管場所に保管しなければならない。電子化された機密情報は、社内サーバー又は指定した外部クラウド・サーバーに限定して保管することを認

めるものとする。

- 2 機密情報は、機密である旨（「社外秘」や「秘」等）を明示しなければならない。電子化された機密情報を印刷する際には、機密である旨が明示されるようにしなければならない。
- 3 機密情報は、原則として、社外に持出すことを禁止する。
- 4 外部クラウド・サーバー内に保管されている機密情報は、当社に指定された情報システム端末のみからアクセス可能とする。

#### （機密情報の取扱い）

第9条 情報システム管理者は、自らの所属部門に属する業務上取扱う機密情報の保全に努め、不正利用や漏洩がないよう注意を尽くすとともに、役職員に対し、適切な助言と指導を行わなければならない。

- 2 情報システム管理者は、機密情報の社外漏洩が生じるおそれがあると判断した場合には、速やかに情報システム管理責任者に報告し、情報システム管理責任者はその対応策について協議するものとする。

#### （機密情報の開示）

第10条 役職員は、機密情報を開示する場合は、あらかじめ情報システム管理責任者の許可を得なければならない。

#### （機密情報の廃棄）

第11条 機密情報が不要となった場合は、法令等に基づき保存が義務付けられている場合を除き、情報システム管理者は、下記の方法で責任をもって廃棄し、廃棄完了後はその旨を情報システム管理責任者に報告しなければならない。

- （1）機密情報を記録した情報システム端末、又は電子記憶媒体を廃棄するときは、機密情報を完全に消去するか電子記憶媒体を物理的に破壊してから廃棄する。
- （2）機密情報を記録した情報システム端末、又は電子記憶媒体を他に転用するときは、機密情報を完全に消去してから転用する。
- （3）紙媒体に記録された機密情報を廃棄する場合は、シュレッダーにかけて読み取り不能にした上で、廃棄する。

## 第4章 各段階における安全管理措置

### 第1款 取得・入力段階

#### （顧客情報の取扱い）

第12条 情報システム管理責任者は、小規模不動産特定共同事業における電子取引業務に際して取扱う顧客情報について、その取得・入力を行う担当部門及び役職員を指定する。なお、機微（センシティブ）情報の取得・入力を行う役職員は、必要最小限の者に限るものとする。

- 2 前項により指定を受けた担当部門及び役職員は、顧客情報の入力を行う場合には、誤入力等がないよう十分に留意し、情報の正確性の確保に努めるものとする。また、入手した顧客情報について変更が生じた場合は、顧客からの申告を受けて変更内容を反映し、最新の顧客情報を管理するよう努めるものとする。

(管理台帳への記録)

第13条 各部門の情報システム管理者は、小規模不動産特定共同事業における電子取引業務に際して取得する顧客情報について、次の掲げる事項を含む台帳を作成しなければならない。

- (1) 情報の項目
  - (2) 利用目的
  - (3) 保管場所・保管方法・保管期限
  - (4) 管理部署
  - (5) アクセス制御の状況
  - (6) その他の安全管理に関する事項
- 2 情報システム管理責任者は、前項に基づく台帳の作成状況を確認するとともに、当社の情報管理状況の適切性を検証し、必要に応じて、各部門の情報システム管理者に対して随時見直しを指示するものとする。

## 第2款 利用段階

(顧客情報の利用)

第14条 役職員は、顧客情報をその利用目的の範囲内でのみ利用することができ、利用目的の達成に必要な範囲を超えて、顧客情報を保有してはならない。

- 2 役職員は、顧客情報を社外に持ち出して利用するには、会社貸与のパソコン・USBの利用・その他情報システム管理責任者が認める方法によらなければならないものとする。なお、顧客情報の社外への持ち出しは、その必要性等を考慮して必要最小限の顧客情報であって必要最小限の者にのみ認められることに留意する。
- 3 顧客情報の利用・加工は、情報システム管理に関する統括部門在籍の役職員に限り行うことができる。情報システム管理に関する統括部門以外の役職員は、情報システム管理責任者の事前の承認を得なければ、顧客情報を加工してはならないものとする。

## 第3款 保存段階

(顧客情報の保管・保存)

第15条 当社は、顧客情報を次の各号に掲げる媒体の区分に応じて、当該各号に定めるところにより保管・保存する。

①電子媒体で作成された顧客情報 (CD-R等の物理的媒体に格納されているものを除く)
当該顧客情報にかかるファイルが格納されたフォルダにアクセス制御をかけるとともに、当該顧客情報にかかるファイル自体又は当該ファイルを保管するフォルダにパスワードロックをかけて保管・保存する方法
②電子媒体で作成された顧客情報のうちCD-R等の物理的媒体に格納されているもの
③紙媒体により作成された顧客情報
施錠できるキャビネットに保管・保存する方法又は情報システム管理責任者が適格性を認めた外部倉庫業者の倉庫等の外部保管場所において保管する方法

- 2 情報システム管理者は、自身が担当する部門で取扱う顧客情報の保管・保存に関して、前項に掲げるアクセス制御、パスワード及びキャビネットの鍵の管理を厳重に行わなければならない。
- 3 顧客情報の保管期間は、最終の使用日から10年間とする。ただし、保管期間に関わらず、業務上の必要性がなくなった情報については、適切に消去・廃棄しなければならないものとする。
- 4 各部門では、毎年1回を目途に、この規定に基づき作成する台帳に従って、顧客情報の棚卸しを行い、業務上の必要性の有無その他の当該顧客情報の保管・保存の必要性を検証し、不要な情報は適切に消去・廃棄するものとする。

#### 第4款 提供（移送・送信）等段階

##### （顧客情報の提供）

第16条 役職員は、業務上の必要がある場合その他の正当な理由がある場合でなければ、顧客情報を第三者へ提供（移送・送信）してはならない。

- 2 役職員は、顧客情報を第三者へ提供（移送・送信）するに際して、次の各号に掲げる事項を確認しなければならないものとする。
  - (1) 誤送信等が発生しないための送付先の確認
  - (2) 当社と当該第三者との間で秘密保持契約が締結されていること
  - (3) 当該第三者において顧客情報が適切に取り扱われることが確保されていること
  - (4) 顧客情報の第三者への提供（移送・送信）にあたり、当該顧客情報の入手元からの同意を得ることその他の手続が必要な場合には、当該手続が適切に行われていること
- 3 役職員は、電子媒体で作成された顧客情報（CD-R等の物理的媒体に格納されているものを除く）を第三者に送信する場合は、その旨を各部門の情報システム管理者に通知しなければならない。なお、当該通知は、電子メールのCCに各部門の情報システム管理者を入れることにより代えることができるものとする。
- 4 役職員は、電子メール等により顧客情報が含まれるファイル等を送信する場合は、当該ファイルにパスワードを設定するものとする。
- 5 役職員は、電子媒体で作成された顧客情報のうちCD-R等の物理的媒体に格納されているもの又は紙媒体により作成された顧客情報を第三者に提供する場合は、あらかじめ、その旨を各部門の情報システム管理者に通知するとともに、提供先の第

三者から受領書（電磁的方法による場合を含む）を受領しなければならない。

- 6 役職員は、顧客情報を第三者に提供（移送・送信）した場合又は回収した場合は、その旨を台帳に記載するものとする。
- 7 役職員は、顧客情報の提供（移送・送信）において不備又は障害等が発生した場合は、直ちに担当部門の情報システム管理者に報告を行う。第一報を受けた情報システム管理者は、直ちに情報システム管理責任者に報告を行うとともに、不備等の内容及び発生状況等の詳細を調査し、新たな情報が入手できる都度情報システム管理責任者に続報を行う。
- 8 情報システム管理責任者は、前項に掲げる不備等が発生した場合は、必要な部門及び役職員と連携し、適切に対応するものとする。

#### 第5款 削除・廃棄段階

（顧客情報の削除・廃棄）

第17条 当社は、顧客情報を次の各号に掲げる媒体の区分に応じて、当該各号に定めるところにより消去・廃棄する。

①電子媒体で作成された顧客情報 （CD-R等の物理的媒体に格納されているものを除く）
安全・確実な消去・廃棄方法として情報システム管理責任者が認める方法
②電子媒体で作成された顧客情報のうちCD-R等の物理的媒体に格納されているもの
③紙媒体により作成された顧客情報
シュレッダーにかける方法、物理的に粉砕する方法、情報システム管理責任者が適格性を認めた廃棄物処理業者等に溶解させる方法その他安全・確実な廃棄方法として情報システム管理責任者が認める方法

- 2 役職員は、顧客情報の保管期間を経過した場合は、各部門の情報システム管理者に事前に通知した上で、前項に掲げる方法により顧客情報を適切に消去・廃棄しなければならない。
- 3 役職員は、顧客情報の消去・廃棄を行う場合は、対象となる顧客情報の抽出に誤りがないよう十分留意するとともに、消去・廃棄を行った場合は、当該記録（廃棄証明書等）を入手し、情報システム管理責任者に提出するものとする。

#### 第5章 情報セキュリティ

（セキュリティの確保）

第18条 当社は、情報システムのセキュリティを確保するため、情報システム管理責任者は以下に掲げるセキュリティを実施するものとする。

- (1) アクセス者の識別及び認証
- (2) 適切なアクセス制御の実施
- (3) アクセスの記録及び定期的な分析による不正アクセス等の検知及び分析
  - ・アクセス者のログを監視する
  - ・ファイアウォール、ログの定期的な分析を行い、不正アクセスを検知する

- (4) 外部からの不正アクセス又は不正ソフトウェアから保護する仕組の導入
  - ・ 交信情報を暗号化する
  - ・ ネットワーク不正侵入（ハッカー）に対するセキュリティを導入する
  - ・ コンピュータウイルスに対するソフトウェアを導入する
- (5) セキュリティの確保についての定期的な見直し
  - ・ 情報システムに関する機器及び電子媒体等の盗難防止策を導入する
  - ・ 顧客情報を持ち運ぶ際の情報漏えい等の防止対策を導入する
  - ・ 顧客情報の削除及び保管している機器及び電子媒体等の廃棄ルールを定める

(インターネット及び電子メール等の利用)

第19条 役職員は、インターネットの利用に際して、有害な内容や違法な内容のダウンロードは一切してはならず、インターネットの私的利用も禁止する。

- 2 電子メールの利用は、業務上必要なものに限るものとする。

(情報システム・情報システム端末へのアクセス制御)

第20条 情報システム管理責任者は、役職員が当社のパソコン・スマートフォンその他の情報システム端末を利用するに際し、当社の情報システムを利用する役職員の識別・認証を的確に行えるようにするため、当該情報システム端末の利用に当たって、ユーザアカウントごとに、ID・パスワード、指紋認証システム、その他の識別符号の入力が必要となるようにしなければならない。ただし、情報システムの整備のために必要な場合その他情報システム管理責任者が認める場合は、この限りでない。

- 2 前項に定めるものの他に、情報システム管理責任者は、当社の情報システムの利用者の本人確認を的確に行うために必要な措置を講じなければならないものとする。
- 3 役職員は、当社の情報システムを利用するにあたり必要となる ID、パスワードその他の識別符号を厳重に管理しなければならないが、正当な理由なく第三者に伝達・漏洩してはならないものとする。

(外部からの不正アクセス等の防止)

第21条 情報システム管理責任者は、以下に掲げる方法等により、当社の情報システム、情報システム端末及びこれらに保存される機密情報を、内部及び外部からの不正アクセス、外部の不正ソフトウェア又はウイルス等によるサイバー攻撃から保護するものとする。

- (1) アクセス可能な通信経路の限定
  - ・ 情報システム管理責任者は、機密情報が記録されたファイルにパスワードを設定し、必要に応じて、当該ファイルやこれを含むフォルダへのアクセス制限を職務内容、権限に応じて設定する。
- (2) 外部ネットワークとの間のファイアウォールの設置
  - ・ 情報システム管理責任者は、当社で使用する全てのパソコンその他の情報システム端末のオペレーティングシステムを可能な限り最新の状態に保持する。また、当

社で使用する全てのパソコンその他の情報システム端末にコンピュータウイルス対策ソフトを設定し、これを常に最新の状態に保持する。当社ネットワークと外部ネットワークの間には、次世代型ファイアウォール等のネットワーク型セキュリティシステムを導入し、これを常に最新の状態に保持する。

(3) アクセス履歴その他必要な記録の取得・保存

・情報システム管理責任者は、アクセス履歴その他必要な記録を取得し、これを保存する。

(調査権)

第22条 情報システム管理責任者は、事前通知なしに、役職員が利用しているパソコン等の情報システム端末を調査し、その使用・管理状況を調査することができる。

## 第6章 漏えい等・システム障害時の対応

(漏えい等事案への対応)

第23条 以下のいずれかに該当する事実を知った役職員は、直ちに自己の所属する部門の情報システム管理者、情報システム管理責任者及び取締役会に報告するものとする。

(1) 情報漏えい、滅失及び毀損（以下まとめて「漏えい等」という）が発生した場合もしくはその可能性を把握した場合

(2) この規定に違反した事実もしくはその可能性を把握した場合

(3) システム障害が発生した場合もしくはその可能性を把握した場合

2 情報システム管理者及び情報システム管理責任者は、被害の拡大防止又は復旧等のために必要な措置を講ずるものとする。

3 情報システム管理者は、事案の発生した経緯、被害状況及び発生原因等を調査し、情報システム管理責任者に報告する。

4 情報システム管理責任者は、前項の規定に基づく報告を受けた場合には、当該事案の内容、経緯、被害状況等を取締役会に速やかに報告・協議の上、事案の内容や影響等に応じて以下の措置を講じるものとする。

(1) 漏えい事案等の対象となった本人への事実関係等の速やかな通知

(2) 取締役会及びコンプライアンス委員会への報告

(3) 二次被害の防止の観点からの事実関係及び拡大防止策の公表

5 情報システム管理責任者は、事案の発生した原因を分析し、再発防止のために必要な措置を検討し、実施するものとする。

(システム障害時への対応)

第24条 当社は、システム障害の発生に備え、顧客管理システム等の基幹システムについて、定期的にバックアップを取り、システム障害が発生した場合でも速やかに復旧させる体制を整備するものとする。なお、バックアップの方法は、バックアップ対象であるシステム環境とは別の場所にて設置・運営されるバックアップ（オフサイトバ

ックアップ)を基本とする。

- 2 当社は、第26条に定める教育訓練において、システム障害が発生した場合を想定した訓練を実施することで、システム障害に備えるものとする。
- 3 当社は、システム障害等が発生した場合は、別に定める「危機管理規定」に従って対応し、障害発生経緯等の状況を記録するとともに、再発防止策を講じるものとする。
- 4 当社は、一定のシステム障害が発生した場合は、監督官庁宛に報告を行うものとする。

## 第7章 その他の安全管理措置

(非開示契約の締結)

第25条 当社は、この規定に定める情報管理業務に従事する役職員との間で、非開示契約等を締結し、当該役職員の退職後においても適切な情報の管理を行うものとする。

(教育訓練)

第26条 情報システム管理責任者は、役職員が情報等を取扱うにあたり、必要かつ適切な指導・監督を行わなければならない。

- 2 情報システム管理責任者は、必要に応じて、役職員に対して以下の内容を含む研修を実施するものとする。
  - (1) 個人情報保護法その他情報管理に関する各種法規制の内容
  - (2) 当社の情報管理に関する各種規定及び方針の内容
  - (3) 情報セキュリティ管理に関する事項
  - (4) 情報漏えい等が生じた場合の対応
  - (5) システム障害が発生した場合の対応(特に、クーリング・オフ等の解約時におけるシステム障害の発生に留意すること)

## 第8章 その他

(外部委託先の管理)

第27条 顧客情報の取扱いの全部又は一部を外部委託する場合は、その取扱いを委託した顧客情報の安全管理が図られるよう、委託先に対する必要かつ適切な監督を行わなければならないものとする。

- 2 顧客情報の取扱いの外部委託は、別に定める「外部委託先管理規定」に従って行う。

(リスク管理)

第28条 当社は、当社の事業に内在する種々のリスクを把握し適切に管理するために、当社のリスク管理を行う。特に、情報システム管理に伴うリスクについては、この規定に基づき作成した台帳等の記録類を活用し、リスクの検証を行うものとする。

(自己点検)

第29条 情報システム管理責任者は、必要に応じて、各部門の責任者(情報管理者)及び役

- 職員に対して、情報等の管理に係る自主点検の実施を指示することができる。
- 2 前項の指示を受けた各部門の責任者（情報管理者）及び役職員は、情報等の管理に係る自主点検を実施し、その結果を、情報システム管理責任者に報告しなければならない。
  - 3 前項に掲げる報告を受けた情報システム管理責任者は、当該報告を受けて経営に重大な影響を与える可能性があると判断した場合には、当該問題について取締役会に報告しなければならない。
  - 4 役職員は、本条に掲げる自主点検に、できる限り協力するものとする。

（内部監査）

第30条 財務部（内部監査）は、当社の顧客情報の取扱い等の管理状況についてその実施状況や適切性を判断・検証する為、内部監査を実施する。

- 2 内部監査は、別に定める「内部監査規定」に従って行う。

（改廃）

第31条 この規定の改廃は、取締役会において行うものとする。

附 則

第1条 この規定は、2022年1月27日より施行する。