情報管理・秘密保持規定

第1章　総論

第１条目的

本規定は、一般社団法人認知症高齢者研究所（以下「当所」という）が取り扱う情報の適正管理の方法を定めると共に、重要な秘密情報の保持に関する各種義務等を明示することにより、もって、当所における情報管理が適正厳格に行われ、顧客、取引先より預かり保管し、あるいは当所社自身が有する各種機密情報等を保護することを目的とする。

第２条 適用範囲

本件規定が適用される範囲は次の通りとする。

1 場所的適用範囲

（１）当所事務所の敷地内、専用通信回線で結ばれた範囲、インターネット回線により結ばれた各研究室，現地研究事務所，出張研究所，あるいはサーバー保管場所、その他主に当所の情報を取り扱うことを主たる目的とする物的設備の範囲

（２）但し，遠隔操作により，出張先，外出先，自宅，宿泊施設などにおいて，前記（１）の施設にアクセスし，保管された情報を利用する場合には，例外的にその出張先，外出先，自宅，宿泊施設等が適用範囲に含まれるものとする。

2 人的範囲

（１）本件規定が適用となるのは、理事・監事・相談役などの役員、研究員、臨時雇用者(アルバイト・パート雇用者)、派遣研究員など、当所と雇用契約関係を持つものにして、情報に接する可能性のある者を対象とする。

（２）当所が外部事業者等との間で，委託契約などを締結し，情報の処理などを行わせる場合には，当所の機密情報に限り本規定を準用するものとする。準用にあたっては本規定の条件に加え、当所を外部事業者に置き換えて適用するものとする。

3 時間的適用範囲

本件規定は、入所ないし各種契約の成立と同時に各自に適用となり、原則として，退職後も当所情報に関する限り適用されるものとする。退職後の秘密保持に関しては、別途「秘密保持に関する誓約書」を作成し，保護義務等に関する取り決めを行う。

第 3 条 定義

1 情報

当所および当所に関連する一切の当事者に関わる、一切の事実、評価、データ(電気的・磁気的信号類の一切を含む)で、伝達可能なもの

2 秘密の指定

上記 1 の情報の中から、代表理事、理事、監事、その他担当責任者が特に指定した情報につき、次の通りの区分を行う。

極秘情報　代表理事、理事、監査役らが特に指定した情報であって，情報の表示において「極秘」と表示のあるもの。

機密情報　理事及び担当責任者が特に指定した情報であって，情報の表示において「機密」と表示のあるもの。

秘密情報　重要情報で、担当者責任者以上のものが指定した情報で，情報の表示において「秘密」と表示のあるもの。

取扱注意　秘密ではないが、著作権情報を含むなど、実質的に公開、広範な流布を避けるべき情報で、担当者が指定した情報であって，情報の表示において「取り扱い注意」乃至「部外秘」と表示のあるもの。

第 4 条 各種秘密の取扱いの原則

情報管理のために，情報のセキュリティのランクに従って，下記のとおり情報管理者を定め，情報を管理するものとする。

① 極秘情報　代表取締役、取締役、監事らが特に「極秘情報」と指定しだ情報は、情報担当理事がこれを管理するものとし，上記指定権者以外の閲覧を禁止する。また、閲覧に際しては、閲覧許可の申請と情報担当理事の承認を経た上で、期限を定めて閲覧を許可するものとする。また、いかなる理由においてもこれの複製、配布、持ち出しを行うことを禁止する。

② 機密情報　理事及び担当責任者が特に「機密情報」と指定した情報は、情報担当理事がこれを管理し，理事、担当部門の責任者以外の閲覧を禁止する。また、閲覧に際しては、閲覧許可の申請と情報担当理事の承認を経た上で、期限を定めて閲覧を許可するものとする。また、いかなる理由においてもこれの複製、配布、持ち出しを行うことを禁止する。

③ 秘密情報　重要情報で、担当者責任者が「秘密情報」と指定した情報は各情報の担当者がこれを管理するものとし，理事・指定権者のほか、特に許可を取った研究員が、定められた方法に従って閲覧することのみが許される。各情報の担当者は閲覧許可を与えた対象を記録する。また、担当者は閲覧する許可を得た対象に提供する目的に限り、担当者の責任により複製、配布、持ち出しを許可する。

④ 取扱注意　秘密ではないが、著作権情報を含むなど、実質的に公開、広範な流布を避

けるべき物で、担当者が「取扱い注意」と指定した情報は、担当者においてこれを管理するものとし，担当者において社外持ち出しを制限するとともに，複製，配布，保管において十分な注意を払うことが義務付けられる。

第 5 条 秘密漏洩の禁止

1 一般禁止規定

理事、研究員、契約所員、派遣所員、臨時雇用者等本件規定の対象者は，前条に定める情報についてその指定された方法に従い、利用するものとし、その方法に違反し、業務目的外に使用してはならない。

いかなる情報であっても、第三者(配偶者・両親・親戚等の血縁者及び友人・知人を含む。以下同じ)に開示・提供してはならない。なお退職後も、在職中に知り得た社内情報を第三者に開示・提供してはならない。

2 パスワード発行管理義務

各情報の情報管理者は，利用が必要であり，かつ利用可能なものに対して，パスワード発行規則に基づいて，一人に対し，１つに限りパスワードを発行することができる。パスワード発行後は，定期的にパスワードの変更を行うものとし，変更後のパスワードもこれを管理するものとする。

３パスワード保持義務

各人に付与されたパスワードは、各自において厳重に管理しなければならず、第三者(配偶者・両親・親戚等の血縁者及び友人・知人を含む。以下同じ)に開示・提供してはならない。また，パスワードを，容易に観取される可能性のある手帳やメモ類に書き入れるなどしてはならない。

なお退職，職場の異動，担当変えなどの変更のあった場合には，直ちに与えられたパスワードを破棄し，使用を停止し，管理者に対し，その抹消を請求しなければならない。

また，在職中に知り得たパスワードを第三者に開示・提供してはならない。

４　退職後の秘密保持義務

退職後の秘密保持義務については、別途「退職時秘密管理義務に関する誓約書」の定めに従うものとする。

第２章 内部的管理・規制

第１　施設等物的規制

第６条　私的利用スペースと，作業施設との峻別

１　個人の私的所有物，私的情報端末，私的携帯電話などを収納するロッカールームを明確にし，作業施設に入る前に通過できるようにすること。

２　本件規則の対象者は，すべての私的利用にかかる情報端末等を，指定されたロッカーに収納するものとし，作業施設内に持ち込んではならない。

第７条　通信施設の区分

１　所内 LAN の敷設制限

情報担当理事は，所内の LAN の敷設につき，明確な指針の元，担当者の意見を聞いた上で，情報流通の仕組み明確にし，LAN 回線，および情報流通システムを管理することとする。

２　回線配置の明確化と安全性確保

所内 LAN 回線の敷設は，重要性に準じて色分けし，かつ，安全な形態で敷設するものとする。

研究員等は，LAN 回線に接触してはならず，かつ干渉となるような行為をしてはならない。回線の敷設などを変更する必要のある場合は，情報担当理事に対し，敷設状況を変更すべき理由と，新たな敷設の要望を図示した書面にて，変更申請して，担当者による変更を実施するものとする。

３　配線図の保管

情報担当理事は，社内 LAN 回線の配線図面を厳格に管理するものとする。回線の一部変更を行った場合も，その変更を正確に反映し，履歴とともに厳重に保管するものとする。

第２情報取り扱い規制

第８条 秘密の指定

１ 入手情報の取扱い

当所が新たに作成し，分析し，取得し、あるいは保管管理を始めた各種情報については、秘密分類の判断を行うべき指定権者が確定し、指定行為を行うか，指定行為を行わないことを明示するに至るまでは、担当者において厳重に秘密を守る取扱いをしなければならない。

2 秘密の指定時期

指定者は、指定者において情報入手後、その重要性を直ちに判断し、必要な指定行為を行うものとする。

3 秘密の指定方法

指定者が秘密の判断をした時には、直ちに情報そのものに，指定された秘密のレベルに従った表示を、誰が見ても分かる位置と大きさで、明確に表示し，指定対象情報のホルダー等保管場所に、確実に保管し，情報リストに登録しなければならない。

第９条 秘密情報の管理方法

1 管理場所の確保

	文書の場合	データの場合
a 極秘情報、機密情報について	利用者を情報管理理事に制限した複数の方法による施錠を施した部屋ないしキャビネットないしロッカーにて文書管理可能な場所を確保すること	直接インターネットなどの外部への接続を許可しない PC に保管し、厳重に保管する。
b 秘密情報について	担当責任者が指定した施錠可能な部屋ないしキャビネットないしロッカーにて文書管理可能な場所を確保すること。	担当責任者が指定した所定の情報管理フォルダを作成し、パスワードによるアクセス制限をかけて保管する。

2 管理場所の管理方法

文書情報の場合	データの場合
1 入退室者の全員の氏名・利用目的・利用対象情報の記入を義務づけること	1 アクセスログをすべて取るようにすること
2 利用情報の種類を明記させ、一回につき 1 情報に制限すること	2 一回のアクセスで、1 情報しか利用できない仕組みを採用する
3 原則として持ち出しは認めない。	3 読み出し専用とし、書き込み、削除、複写など禁止する

3 管理責任者の設置

管理責任者を設け、その氏名を明示し、管理を厳正に実施できるようにする。

4 取扱い記録（利用ログ）の保管

情報利用に関して記録した情報(利用者名簿、利用情報の表記、利用目的表記など)も、対象情報と同様のレベルで保管するものとする。

5 契約交渉，セールス，見学者、来訪者対応

極秘情報、機密情報、秘密情報の管理室、管理場所は、来訪者等の目に付くところに設置しない。構造上、必要以上に接近させないように配置すること。

第１０条情報記録媒体利用の制限

1 ノート型 PC 及び情報記憶媒体の制限

① 読み書き可能な外部記憶媒体（FDD、MO、ZIP、CD-RW、DVD-RW、USB メモリ、外付け HDD など）については原則として利用を禁止する。
② 読み込み可能な外部記憶媒体については、情報管理取締役が内容を確認し許可したもののみ利用可能とする。
③ ノート PC は情報管理取締役が許可したもの以外は原則として施設内に持ち込んではならない。また、施設内で利用しているノート PC は原則として外部に持ち出してはならない。
④ 当所の付与した携帯電話機を除いて、データを記録することのできる端末は原則として施設内に持ち込んではならない。また、施設内で利用している端末は原則として外部に持ち出してはならない。

2 例外

（1） 所外持出し用記憶媒体の取り扱い
所外に送信し，携帯する必要のある各種の学術学会資料,プレゼンテーション資料，PR 情報などに関しては，指定された所外持出し用記憶媒体を利用するものとし，持ち出しの際に事前にウイルスチェック，機密制限チェックを受け，チェック済みとの表示を受けたもののみ持ち出すことができる。

（2） 来客者、見学者、取引先、その他情報管理理事が特に認めたものについては、会議室、応接室、研究室、打ち合わせ場所、その他情報管理理事が特に認めた場所においてのみ例外的に持ち込んだノートパソコンを利用することができる。

（3） ただし、無線を利用する機器類である時は、当所の機器類に支障の無いことを確認した上で、利用を許可するものとする。

第１１条 メールの利用制限

1 メールの利用制限

当所内では、外部とのメールの利用は，当所の付与したメールアドレスのみの利用を認め，私的アドレスの利用は禁止する。

2 例外

当所の付与したメールアドレスであっても，所内で特に機密性を重視するために指定された PC 端末，あるいは重要回線として指定された LAN 回線に接続された PC 端末においては，理由の如何を問わず，利用を禁止する。

第１２条バックアップ

1 バックアップ体制の確保

管理対象の情報については、原本のバックアップを必ず取り、原本と同じ程度の厳重度となるように管理する。

ただし、バックアップの保管場所は原本とは離れた場所に保管するものとする。

2 事故対策

何らかの不測の事故により、重要な情報や、秘密に管理された情報が漏洩され、流用された場合を想定して、緊急の対策をあらかじめ準備しておくこと。

① 回復のための作業手順の確認

② 漏洩した場合にはその原因追求と、対策の明確化をする。

③ 流出・漏洩の場合に損害賠償などを請求する手順を明確にすること。

第３章　対外的規制

第１３条 セキュリティ対策指針

1 セキュリティ指針

当所においては、次のセキュリティ指針を確立し、実行する。

① 安定、適正、確実なシステムの構築により未然抑止効果の確保

② セキュリティに関する研究、教育、啓蒙を行い、万全の予防を行う

③ 外部からの不正侵入を警戒し、常時監視し、異常事態の把握と、侵入者摘発を確実に行う

④ 不正侵入を受けた時は、その手口・原因を研究し、万全の対策を立て、直ちに実施し、

同じ手口での再度の侵入を防止する。同時に、所定の機関や組織に速やかに報告を行う。

⑤ 損害を受けた時は、その内容を明確に把握し、顧客情報、取引き情報など当所以外の第三者に損害を与え、もしくは影響があると判断される場合は、直ちに関係当事者に通知し、正確な事実関係の告知と、それに対する当所の対策を説明する。

2 セキュリティの実施

① 常時警戒、常時点検、防止

ア 常時点検の義務

情報管理担当者においては、回線の区分のほか、各端末の状況を確認し、異常事態の発生していないことを確認する義務がある。

イ 常時警戒の義務

インターネットをはじめとして、外部ネットワークと接続して、外部からのアクセスを可能としている場合には、常にそのアクセスを監視するアプリケーションを稼動させ、常時監視を行うものとする。

ウ 各種監視、防止装置の整備

ファイアーウオールなど、侵入を制限する装置を採用し、常時侵入を防止するように努力する。

② 最新情報の取得、スキルアップ

ア 最新情報の入手

情報管理担当者は、ウイルス情報や、不正アクセス侵入方法、アプリケーションのセキュリティホールの最新の報告、などに注意し、常に最先端の情報を取ること。

イ スキルアップ

最新の情報に基づいて、自らボートスキャンを実施するなどして、セキュリティホールの発見に勤め、すべてのセキュリティホールに対して、十分な対策を施すこと。

ウ セキュリティに関する研究会などに積極的に参加して、常にスキルアップを行うように努力すること。

③不正なアクセスに対する対策

ア ウイルスなど

常にウイルス情報に注意し、特にメール添付のファイルを開かないようにすること。

常時、ウイルススキャンを実施して、情報のチェックを行う。

イ クラッキングの危険性を事前に察知する

ボートスキャンを稼動させてし)など、侵入を試みているような形跡が無いか常に注意し、早期発見を行うように努力する。

第４章 契約における情報管理

第１４条 契約行為における情報管理義務

1　契約内容の検討

当所が締結する一切の契約は、契約担当者の判断に加え、理事、代表理事の検討を経ることとし、情報の流出などが無いように十分な配慮を行う。

2　秘密保持規定の設定

当所が第三者と契約行為を行う場合で、当所の情報が利用される場合に関しては、その情報の重要性にかんがみ、十分な「秘密保持条項」及び「秘密遵守システムの確立」「罰則」「対抗措置」 を明記させること。

3　契約の実施状況の確認

契約に定めた秘密保持関連事項の遵守がなされているかにつき、契約相手方に対し、常時確認し、あるいは監視し、調査すること。

第１５条契約前秘密管理

１　契約を締結するに際して，事前に一定の情報を開示する場合には，情報開示の前に「秘密保持契約書」を締結するものとする。

２　秘密保持契約を締結するにあたって，次の点に留保し，実行することとする。

（１） 当所の定める秘密保持契約実施要綱に従って，契約を立案し，締結すること

（２） 当所の定める要綱に従って，開示する情報につき，改ざんできない仕組みを利用した特定番号を附すこと

（３） 提供する必要のある情報につき，事前に上長の承諾を得ること

（４） 提供する情報のすべてを特定した上で登録しなければならない

３　秘密保持契約を締結した後においては，常時提供した情報の保管状況，担当者の変更の有無，変更した場合は新たに秘密保持義務の確認を実施し，かつ現実の管理状況を把握し，管理するものとする。

４　契約締結後，すべての動向をメモし，かつ相手方との情報交流，話し合いについては常にこれらを記録するものとし，面談した際には必ず協議書を作成し，両者が保持するものとする。

第１６条外注制限

情報の処理などを外注する場合には，厳格にこれを処理管理しなければならない。

第１７条(罰則)

研究員が本規程に違反した場合は、就業規則に基づき処分を行うものとする。また本規程に違反する故意または重大な過失によって当所に損害を与えた場合は、一切の賠償責任を

負うこととする。なお当該損害賠償の責任は、在職中はもちろん退職後も免れることはできない。

付則

1.この規程は平成 28 年 8 月 1 日より施行する。
2.この規程を改廃する場合は、研究員を代表する者の意見を聴いて行うものとする。