AGREEMENT TO IMPLEMENT STANDARD CONTRACTUAL CLAUSES FOR THE TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES (CONTROLLER-TO-PROCESSOR TRANSFERS) FOR REGISTRAR DATA ESCROW SERVICES

This Agreement to Implement Standard Contractual Clauses for the Transfer of Personal Data to Third Countries (Controller-to-Processor) for Registrar Data Escrow Services (the "Agreement") is made and entered into by and among COREHUB, S.R.L.U, ("Registrar" or "data exporter") and Iron Mountain Intellectual Property Management, Inc., ("Escrow Agent" or "data importer"). Registrar and Escrow Agent are entering into this Agreement in furtherance of their respective obligations under the Registrar Data Escrow Agreement by and among Registrar, Escrow Agent and the Internet Corporation for Assigned Names and Numbers ("ICANN") with an effective date of April 21, 2008 ("Escrow Agreement") in order to address the protection of any personal data transferred from Registrar to Escrow Agent under the Escrow Agreement. Registrar and Escrow Agent may be referred to individually as a "party" or collectively as the "parties" throughout this Agreement. For the avoidance of doubt, ICANN is not a party to this Agreement and it shall not be bound by the terms of this Agreement.

WHEREAS the parties have executed the Escrow Agreement for the purpose of escrowing certain domain name registration data that may be released to ICANN upon the occurrence of certain events; and

WHEREAS the parties desire to enter this Agreement to add Standard Contractual Clauses to govern the transfer of personal data under the Escrow Agreement.

NOW THEREFORE, in consideration of the mutual promises herein, and other good and valuable consideration, the receipt and sufficiency of which is acknowledged, Registrar and Escrow Agent agree as follows:

1. The parties agree to implement and comply with the terms and conditions set forth in the attached Exhibit 1 (The Standard Contractual Clauses for the Transfer of Personal Data to Third Countries (Controller-to-Processor Transfers))(the "Clauses") for any "personal data," as defined in the Clauses, exchanged between the parties pursuant to the Escrow Agreement.

2. Notwithstanding anything to the contrary set forth herein or in Clause 12 of the Clauses, Registrar authorizes Escrow Agent to release the Deposits (as defined in the Escrow Agreement), including any personal data contained therein, to ICANN or transfer the Deposits, including any personal data contained therein, to a successor escrow agent, subject to the terms and conditions of the Escrow Agreement.

3. Notwithstanding anything to the contrary set forth herein, the parties hereby incorporate by reference Section 10 (Limitation of Liability and Consequential Damages Waiver) of the Escrow Agreement to govern each party's respective liability to the other under this Agreement. This Section 3 shall survive the termination of this Agreement.

4. This Agreement shall terminate upon the termination of the Escrow Agreement. For the avoidance of doubt, any terms and conditions of the Clauses that expressly survive the termination of the Clauses shall also survive the termination of this Agreement.

5. Except as otherwise set forth in this Agreement, in the event of a conflict between the terms of this Agreement and the terms of the Escrow Agreement, the terms of this Agreement shall control.

IN WITNESS WHEREOF, the parties hereto have executed and delivered this Agreement as of the last date set forth in the signature blocks below.

REGISTRAR: COREHUB S.R.L.U.	**Iron Mountain Intellectual Property Management, Inc.**
Individual Signing: AMADEU ABRIL I ABRIL **[print name]**	**Individual Signing:** Mary English **[print name]**
Signature: DocuSigned by: 2572A37992D24BA...	***Signature:*** DocuSigned by: Mary English 089DF59B1DCE41B...
Title: Representative of the sole administrator	**Title:** Vice President and General Manager
Signing Date: gener 15, 2016 | 07:47 PT	**Signing Date:** January 15, 2016 | 08:31 PT

EXHIBIT 1

STANDARD CONTRACTUAL CLAUSES FOR THE TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES (CONTROLLER-TO-PROCESSOR TRANSFERS)

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: COREHUB, S.R.L.U.

Address: CREU COBERTA,17 1-1, 08014 Barcelona

Tel: +34 935275235; fax: +34 935207834; e-mail: legal@corehub.net

Other information needed to identify the organisation

IANA # 15
(the data exporter)

And

Name of the data importing organisation: **Iron Mountain Intellectual Property Management, Inc.**

Address: **One Federal Street, Boston, MA 02110, USA**

Tel. 770 225 8176 **;** fax: **N/A** e-mail: rde@ironmountain.com

Other information needed to identify the organisation:

none
(the data importer)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1];

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer[2]

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a

[2] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia,* internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses[3]. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or

[3] This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full): AMADEU ABRIL I ABRIL

Position: Representative of the sole administrator

Name of the data exporting organisation: COREHUB, S.R.L.U.

Address: Creu Coberta 17, 1-1 08014 Barcelona

Other information necessary in order for the contract to be binding (if any):

DocuSigned by:

Signature...
2572A37992D24BA...

gener 15, 2016 | 07:47 PT

Date: ....

On behalf of the data importer:

Name (written out in full): Mary English

Position: Vice President and General Manager

Address: 2100 Norcross Parkway;Norcross, GA 30071

Name of the data importing organisation: **Iron Mountain Intellectual Property Management, Inc.**

Address:**, One Federal Street, Boston, MA 02110, USA**

Other information necessary in order for the contract to be binding (if any):

DocuSigned by:
Mary English
089DF59B1DCE41B...

Signature……………………………………………

January 15, 2016 | 08:31 PT

Date:...

.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

The data exporter is an Internet domain name registrar that manages the registration of Internet domain names for registrants.

Data importer

The data importer No. 1 is (please specify briefly activities relevant to the transfer):

Iron Mountain Intellectual Property Management, Inc. is the designated escrow agent for the Internet Corporation for Assigned Names and Numbers' (ICANN) registrar data escrow program. Iron Mountain Intellectual Property Management, Inc. holds in escrow certain Internet domain name information deposited by Internet domain name registrars that may be released to ICANN upon the occurrence of certain conditions.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

Internet domain name registrants.

Categories of data

Whois data including:

Name, address and contact information (i.e., telephone and fax number) for Internet domain name registrant
Name, address and contact information (i.e., telephone and fax number) for Internet domain name registrant's Administrative Contact
Name, address and contact information (i.e., telephone and fax number) for Internet domain name registrant's Technical Contact
Name, address and contact information (i.e., telephone and fax number) for Internet domain name registrant's Billing Contact

Special categories of data (if appropriate)

Not applicable.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

The data importer *will provide registrar data escrow services to the data exporter.*

DATA EXPORTER

Date: gener 15, 2016 | 07:47 PT

Name: COREHUB, S.R.L.U.

Authorised Signature …………………… DocuSigned by: 2572A37992D24BA...

DATA IMPORTER

Date: January 15, 2016 | 08:31 PT

Name: Mary English

Authorised Signature …………………… DocuSigned by: Mary English 089DF59B1DCE41B...

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

The data importer shall undertake appropriate technical and organizational measures to protect against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. The measures to be taken should take into account available technology and the cost of implementing the specific measures, and must ensure a level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected

Data importer

GENERAL INFORMATION SECURITY REQUIREMENTS

a) Information Security Requirements. Data importer maintains a formal, comprehensive information security program for the management of information security. The information security program shall include, but not be limited to:

1) Documentation, internal publication, and communication of data importer's information security policies, standards, and procedures;

2) Documented and clear assignment of responsibility and authority for establishment and maintenance of the information security program;

3) Documented permissions and authorizations included in this Appendix;

4) Regular testing of the key controls, systems and procedures of the information security program;

5) Administrative, technical and operational measures required in this Appendix which are designed to protect all personal data, to the extent they are applicable to the format in which the personal data is handled.

b) Minimum controls. In no event during the term of the Clauses shall data importer's security program use controls materially less protective than those provided in this Appendix.

c) Additional controls. Data importer agrees that it will adhere to any additional data exporter data security requirements that may be reasonably provided by data exporter to data importer.

d) Data importer Consultants. Data importer shall be liable for the compliance of its employees, third-party agents, service providers, temporary workers, contractors, subcontractors, representatives and assigns ("Data importer Consultants") that have access to Personal Data pursuant to the terms of this Appendix. Further, data importer shall impose on any Data importer Consultants that have access to Personal Data privacy and security obligations substantially similar to those in this Appendix prior to any such access taking place.

e) Industry Standard Safeguards. In no event shall data importer's security program incorporate less than Industry Standard Safeguards ("Industry Standard Safeguards").

Industry Standard Safeguards shall mean those safeguards widely accepted by information security professionals as necessary to reasonably protect data during storage, processing, and transmission; consistent with the sensitivity of and widely recognized threats to such data. Examples of Industry Standard Safeguards include those practices described in ISO/IEC 27002:2005, NIST 800-44, Microsoft Security Hardening Guides, OWASP Guide to Building Secure Web Applications, and the various Center for Internet Security Standards.

2. RISK ASSESSMENT REQUIREMENTS

a) Risk Assessment Program. Data importer shall maintain an information security risk assessment program designed to identify and assess reasonably foreseeable internal and external risks and vulnerabilities to the security, confidentiality, and/or integrity of Personal Data. Data importer shall further maintain an information security risk assessment program designed to identify any violation of law by data importer or Data importer Consultants. No less frequent than once every twelve (12) months, and upon a material change in risk or vulnerability to Personal Data, data importer shall evaluate and improve, as reasonable and appropriate, the effectiveness of data importer’s information security program for limiting any security risks.

3. INFORMATION PROCESSING ASSETS AND PHYSICAL MEDIA MANAGEMENT REQUIREMENTS

a) Program Requirements. Data importer shall maintain a program to manage information processing assets (such as computers, servers, storage devices, communications networks, personal computers, laptops and peripheral devices) that includes, but is not limited to, the following:

1) Assignment of asset ownership to ensure appropriate classification of information access, determination of access restrictions, and review of access controls;

2) Maintain an inventory of assets to facilitate asset lifecycle management and the identification of unauthorized assets accessing data importer systems, infrastructure or resources;

3) Sanitization of assets prior to their disposal; and

4) Require management authorization prior to removal of equipment or software from data importer premises that is not assigned to a specific individual.

b) Controls. Data importer shall maintain controls that include, but are not limited to, the following:

1) Operating procedures and technical controls designed to protect documents, computer media, input/output/backup data, and system documentation from unauthorized disclosure, modification and destruction.

2) Procedures for the secure disposal of electronic or physical media containing Personal Data.

3) An established process to track and maintain a chain of custody for all of data exporter’s electronic or physical media from initial data importer custody through to permanent removal or destruction.

4. WORKFORCE SECURITY MEASURE REQUIREMENTS

a) Confidentiality. Notwithstanding anything to the contrary, and in addition to any confidentiality terms in the Clauses, data importer shall (i) treat all Personal Data as confidential information and (2) strictly adhere to data importer's internal information security and acceptable use requirements. Data importer shall enter into confidentiality agreements with all Data importer Consultants with access to Personal Data which include confidentiality terms and conditions that are substantially similar to the terms of the Clauses and this Appendix.

b) Employees. To the extent permitted by applicable law and as required under the Agreement, data importer shall conduct background investigations for all employees and Data importer Consultants that perform any duties in connection with handling personal data.

c) Security Awareness Training. No less than once per twelve (12) months, data importer shall conduct general security awareness training and role-specific security training for all data importer employees handling personal data. Data importer shall maintain records identifying the names of such data importer employees in attendance and the date of each security awareness training. Data importer shall also routinely review and update its security awareness training program.

d) Violations. Data importer shall maintain a disciplinary process for all data importer employees who violate the security requirements contained herein. Data importer employees who commit intentional violations of the terms of this Appendix shall be immediately prohibited from providing services under the Clauses, and such employee's access to personal data shall be revoked within no more than twenty-four (24) hours from being removed from performing services.

5. PHYSICAL AND ENVIRONMENTAL SECURITY REQUIREMENTS

a) Physical Security Controls. Data importer's facilities shall utilize physical controls that reasonably restrict access to personal data, including, as data importer deems appropriate, access control protocols, physical barriers such as locked facilities and areas, employee access badges, visitor logs, visitor access badges, card readers, video surveillance cameras, and intrusion detection alarms. All visitors to data importer's facilities must sign in and be escorted at all times. Video surveillance recordings and other records of physical access shall be retained for a minimum of ninety (90) days.

b) Supporting Utilities. Data importer shall employ measures designed to protect its facilities and systems containing personal data from power, telecommunications, water supply, sewage, heating, ventilation and air-conditioning failures.

c) Transmission System Security. At no time shall data importer employ less than Industry Standard Safeguards designed to protect the physical security of its network infrastructure and telecommunication systems from transmission interception and damage.

d) Offsite Equipment. In the event that data importer outsources functions for handling personal data that use of offsite equipment, data importer shall require that the security measures for any such offsite equipment be substantially similar to measures required for on-site equipment used for the same purpose.

e) Physical Access to Information Processing Assets. Data importer shall retain records of data importer employees and Data Importer Consultants authorized to access data importer-controlled computer environment(s) used by data exporter for no less than three (3) years.

Upon data exporter's request, data importer shall permit data exporter to view all such records. Notwithstanding the foregoing, data exporter shall not be given access to the confidential information of other data importer customers or information which data importer is restricted from providing under applicable law.

f) Physical Access Restricted. Data importer shall limit physical access to data importer-controlled facilities that handle personal data to those data importer employees and Data importer Consultants who have a business need for such access. Data importer shall maintain a process for authorizing and tracking requests for physical access to such facilities.

g) Repairs and Modifications. Data importer shall record all security-related repairs and modifications to any physical components, including but not limited to hardware, walls, doors and locks for secure areas within facilities where personal data is handled.

h) Hardware and Software Records. Data importer shall maintain a record of the movement and storage of hardware and electronic media that handle personal data and the identity of any person responsible therefore.

6. <u>COMMUNICATIONS AND INFORMATION PROCESSING OPERATIONS MANAGEMENT REQUIREMENTS</u>

a) Device Configuration Standards. Data importer shall include Industry Standard Safeguards for security hardening procedures and standardized configurations for all devices such as servers, routers, switches and other network equipment used in handling personal data, or with network connectivity to those devices. Data importer shall regularly monitor devices for compliance with standardized configurations and take prompt remedial action to correct deviations from these standards when appropriate.

b) Information Processing Systems Change Control. Data importer shall maintain a formal change management request process for all communications network systems and any handling of personal data. Data importer shall ensure that all change requests are documented, tested, and approved by the asset owner, information owner, or management level personnel as appropriate prior to any new implementations for network communications capabilities, system patches, changes to existing systems or handling of information. Emergency changes required to maintain or restore service shall subsequently be reviewed, documented and appropriate approvals obtained for the change.

c) Segregation of Duties. Data importer shall segregate duties and areas of responsibility so that no one person has sole access to information processing systems that handle personal data. Data importer shall segregate the duties to limit the access of data importer employees or Data importer Consultants to personal data only to the extent necessary to perform their required job functions. Data importer shall prohibit personnel whose primary responsibility is software development shall from accessing production systems, resources, or environments, except when such access is specifically approved for a defined and documented period of time. Data importer shall terminate or specifically re-approve such access when the defined period of time has elapsed.

d) Separation of Development and Production Facilities. Data importer shall logically or physically separate all development, test and production environments for information processing systems.

e) Technical Architecture Management. Data importer shall establish a configuration management process to define, manage, and control the information processing system components utilized to provide the Services and the technical infrastructure of such components.

f) Intrusion Detection. Data importer shall continually monitor computer systems and processes for attempted or actual security intrusions or violations. Data importer shall notify data exporter within twenty-four (24) hours of any unauthorized access to personal data.

g) Network Security. Data importer shall ensure no less than the following measures are in place:

1) Maintain logs with daily reports for network intrusion detection system ("IDS")/ intrusion prevention sensors ("IPS") alert event for all data importer-hosted environment(s) used to handle personal data;

2) Install updates for all data importer-hosted environment(s) used to handle personal data and IDS/IPS systems no less frequently than once per week, or as soon as possible after the updates are received, including prompt deployment to production of the latest threat signatures or rules;

3) High-risk ports on externally-facing systems shall not be accessible from the internet;

4) Maintain log files of all data importer's network connections for no less than twelve (12) months;

5) Deploy firewall(s) designed to protect internal systems, inspect all inbound and outbound network traffic, limit such traffic to define protocols and ports, and specify source and destination hosts where possible;

6) Maintain hardening policies for defining inbound and outbound network ports or service traffic for all data importer-owned or managed systems and document such policies and any associated authorizations within the information security program;

7) Properly secure network and diagnostic ports; and

8) Implement policies, procedures and technical controls that are designed to prevent, detect and remove malicious code or known attacks on data importer's information systems.

h) Encrypted Authentication Credentials. Data importer shall ensure that authentication credentials transmitted over data importer's network devices are encrypted in transit.

i) Secure Network Administration. Data importer shall reasonably manage and control data importer's networks to protect such networks from known threats, and to maintain security for all data importer managed applications and data on or in transit over the network. Data importer shall implement technical controls and secure communication protocols consistent with Industry Standard Safeguards to prohibit unrestricted connections to untrusted networks or publicly accessible servers.

j) Virus Protection. Data importer shall maintain an anti-virus management program, including malware protection, up-to-date signature files, patches, and virus definitions, for data importer managed servers and workstations used to handle personal data.

k) Website – Client Encryption. Data importer shall ensure that for each of its websites Transport Layer Security (TLS) is enabled and contains a valid certificate requiring confidentiality, authentication or authorization controls.

l) Email Relaying. Data importer shall ensure that unauthenticated email relaying/forwarding in the data exporter-dedicated hosted environment(s) is disabled on data importer's Internet email servers.

m) Information Backup. Data importer shall create and securely store appropriate back-up copies of system files.

n) Electronic Information in Transit. Data importer shall utilize encryption using an industry standard algorithm with a minimum 128 bit key length to protect personal data transmitted over public networks when originating from data importer hosted infrastructure.

o) Cryptographic Controls. Data importer shall follow a documented policy on the use of cryptographic controls. Data importer's cryptographic controls shall:

1) Be designed to reasonably protect the confidentiality and integrity of personal data being handled by data importer in any shared network environments in accordance with the terms of this Appendix;

2) Be applied to data importer-hosted environment(s) used to transmit personal data across or to "untrusted" networks (i.e., networks that data importer does not legally control), including those environments or networks used for sending data to data exporter's corporate network from data importer's network, subject to data exporter's cooperation in management of encryption keys necessary to decrypt transmissions received by data exporter; and

3) Include documented encryption key management practices to support the security of cryptographic technologies.

4) Include encryption of all personal data on laptops and other portable devices.

p) Logging Requirements. Data importerw shall ensure the following:

1) Significant security and system events are logged and reviewed;

2) Audit logs for systems in data importer-hosted environments used to provide services are retained for a minimum of twelve (12) months;

3) System audit logs are reviewed for anomalies; and

4) Log facilities and systems information are reasonably protected against tampering and unauthorized access.

q) Network Time Synchronization. Data importer shall synchronize the system clocks of all information processing systems using a common authoritative time source.

r) Segregation on Networks. Data importer shall appropriately segregate related groups of information services, users, and information systems on networks. Internet facing systems and server systems handling data exporter data shall reside on a dedicated DMZ network segment segregated from corporate and user segments.

7. <u>ACCESS CONTROL REQUIREMENTS</u>

a) Access Control Policy. Data importer shall maintain an access control policy for all assets that handle personal data. Data importer shall formally approve, publish and implement such access control policy.

b) Logical Access Authorization. Data importer shall maintain an approval process for requests for logical access to personal data and requests for access to data importer systems used by data importer in providing services to data exporter.

1) Data importer shall maintain a user registration and deregistration procedure for granting and revoking access to data importer systems that handle personal data.

2) Data importer shall retain a record of access to data importer's information processing systems and Privileged Accounts (as defined below) in data importer-hosted environment(s) for no less than twelve (12) months. Upon data exporter's request, data importer shall provide such access records and reasonably cooperate with data exporter for all inquiries relating to such access records.

c) Privileged Access Control. A "Privileged Account" is an account that enables an individual to establish or modify identification credentials, access rules, production applications or operating systems or network parameters. Data importer shall ensure that Privileged Accounts are only provided by data importer to individual users that are expressly approved by data importer or data exporter, and data importer shall ensure that such Privileged Accounts are strictly limited to those individuals who have a legitimate business need to use a Privileged Account. Data importer shall maintain a process for obtaining approvals for Privileged Account users. Additionally, data importer shall maintain an audit trail of all approved individuals and actions performed by these Privileged Accounts.

d) Access Control and Access Review. Data importer shall grant access to personal data to current data importer employees or Data importer Consultants who need such access in order to perform their job function only. Every three (3) months, or on a quarterly basis, data importer shall review and confirm that all access to personal data or Privileged Accounts is only granted by data importer to individuals who require such access in the performance of their current job function. Data importer shall further maintain record of such access reviews and updates.

e) Control of Third Party Access. Prior to granting third parties access to data importer's information systems that handle personal data, data importer shall ensure that appropriate controls are in place including, but not limited to: restrictions on protocols and ports used to access information, encryption to protect sessions and information in transit, appropriate background checks for third party personnel as required herein, anti-virus software running current signatures on devices used to access personal data, and current patches on devices used to access personal data.

f) Operating Systems Access Control. Data importer shall control access to operating systems (both software and hardware based operating systems) by requiring a secure log-on process that uniquely identifies the individual who is accessing the operating system.

g) Mobile Computing Devices. Data importer shall maintain a program designed to protect data importer's mobile computing devices from unauthorized access. Such program shall address physical protection, access control and security controls such as encryption, virus protection and device backup.

h) Data exporter Systems Isolation. Data importer shall logically separate and segregate personal data from all other information in hosted environments used to handle personal data.

i) Accounts. Data importer shall require the following with respect to accounts:

1) Authentication of the identity of each data importer employee or Data importer Consultant who attempts to access data importer systems that handle personal data and prohibit the use of shared user accounts, or user accounts with generic credentials (i.e. IDs) for accessing such personal data or the associated systems.

2) That all user account IDs, including Privileged Accounts, be tied directly to an individual person (as opposed to a position) with the sole exception of service accounts required to run server software. Data importer shall ensure that (i) all service accounts are subject to at least the same password restrictions as Privileged Accounts, (ii) use of such services accounts is restricted to the specific servers required for the account and(iii) interactive logins are prohibited for any unusual activity and wherever possible.

3) The use of temporary passwords that meet or exceed the complexity requirements for individual accounts, check out IDs, or similar controls for default administration account access if default administration accounts are not disabled or removed.

4) That inactive accounts are locked or disabled after ninety (90) days of inactivity.

5) Access to an account is prohibited after no more than five (5) unsuccessful access attempts.

6) Unique identifiers and strong passwords with a required minimum number of characters that must be changed every ninety (90) days.

7) Employees are prohibited from sharing or writing down passwords.

j) Controls for Unattended Systems. Data importer shall utilize a password protected screensaver for any system that is inactive for thirty (30) minutes or longer.

8. <u>INFORMATION SYSTEMS ACQUISITION DEVELOPMENT AND MAINTENANCE REQUIREMENTS</u>

a) Systems Development Security. Data importer shall ensure that security measures are included in all information systems development and operations. Further, data importer shall publish and adhere to internal secure coding methodologies based on application development security standards.

1) Data importer shall include in the development process application functionality designed to prevent errors, losses, unauthorized modifications or misuse of information.

2) Data importer shall control access to system files and program source code. Data importer shall assign, document and conduct in a reasonably secure manner all information technology development, implementation and support project activities.

3) Data importer shall formally approve application changes and such changes will be controlled by a documented change control process.

b) Software Security Management. Data importer shall design its information systems (including operating systems, infrastructure, business applications, services and user-developed applications) to be in compliance with Industry Standard Safeguards.

1) Data importer shall maintain the security of production application system software and information.

2) Data importer shall appropriately supervise and monitor all outsourced software development activities.

3) Data importer shall maintain policies and technical controls designed to prevent non-administrative users from installing software on operations systems.

c) Network Diagrams. Data importer shall develop, document, and maintain physical and logical diagrams of networking devices and traffic.

d) Application Vulnerability Assessments/Ethical Hacking. No less frequently than once every twelve (12) months, data importer shall, perform vulnerability assessments on applications in its hosted environment(s) used to handle personal data.

e) If data importer does not permit data exporter or agents of data exporter to test or assess data importer infrastructure or applications in any capacity, upon data exporter's request data importer shall provide attestation to the security of its applications and infrastructure through independent certifications, third party application security testing, and internal security assurance processes. Additionally, data importer shall make available to data exporter all executive summaries of the results of independent security tests. Data importer shall not be required to provide detailed results that are the confidential and proprietary information of data importer.

f) Change Testing and Review. Data importer shall review and test changes to applications and operating systems prior to deployment to ensure there is no adverse effect on personal data or systems and to negative impact to functionality required by data exporter to consume the scoped services.

9. <u>DATA SECURITY BREACHES AND INCIDENT RESPONSE REQUIREMENTS</u>

a) Notification. Data importer shall notify data exporter promptly upon learning of a Data Security Incident. For purposes of this Addendum, a "Data Security Incident" shall mean (a) the actual unauthorized access to or use of personal data, or (b) the unauthorized disclosure, loss, theft or manipulation of unencrypted personal data (or encrypted personal data where unauthorized decryption has or is likely to occur) or other information under control of data importer that has the potential to cause harm to data exporter's business, clients, employees, systems, or reputation. This notification obligation also applies to major disruptions of the operations or other violations of regulations for the protection of personal data or other irregularities in the handling of personal data. The data importer shall, in consultation with the data exporter, take appropriate measures to secure the personal data and to mitigate possible negative consequences for those affected.

Notification must include a phone call to the data exporter. In the event data importer is unable to reach such contact promptly, data importer must contact globalsecurity@ironmountain.com and global.privacy@ironmountain.com. Notification shall include at a minimum (a) a detailed description of the Incident, (b) the expected resolution time (if it has not already been resolved), and (c) the name and phone number of the data importer representative that data exporter may contact to obtain further information and updates.

b) Updates. Data importer agrees to keep data exporter informed of progress and actions taken to address the Security Incident, and to provide data exporter with all facts about the Security Incident as appropriate for data exporter to conduct its own assessment of the risk to personal data and of data exporter's overall exposure to such Security Incident.

c) Disclosure. Unless such disclosure is mandated by law, data exporter in its sole discretion will determine whether to provide notification to data exporter's customers or employees concerning incidents involving personal data.

d) Remediation. Notwithstanding any other provisions of the Clauses, in the event of a Security Incident involving unencrypted personal data, data importer agrees to provide all service(s) required by applicable law or even if not so required which are customarily provided to individuals impacted by a breach in confidentiality of their personal data in their jurisdiction. For purposes of this Appendix, personal data shall mean any data related to or associated with an identified or identifiable natural person, including, but not limited to, any data exporter employee information, or data exporter customer information. A natural person is identifiable if, with reasonable effort, the individual could be identified from the data or a grouping of data.

Certificate Of Completion

Envelope Id: D9BF3082F10E407C959E1B6400AAA585		Status: Completed
Subject: Please DocuSign this document: IANA 15 STANDALONE MODEL CLAUSE AGREEMENT IMIPM.pdf		
Source Envelope:		
Document Pages: 24	Signatures: 6	Envelope Originator:
Certificate Pages: 3	Initials: 0	David Jones
AutoNav: Enabled		745 Atlantic Ave.
EnvelopeId Stamping: Enabled		Boston , MA 02111
Time Zone: (UTC-08:00) Pacific Time (US & Canada)		david.jones@ironmountain.com
		IP Address: 216.229.152.50

Record Tracking

Status: Original 1/13/2016 6:49:12 AM	Holder: David Jones david.jones@ironmountain.com	Location: DocuSign

Signer Events	Signature	Timestamp
Amadeu Abril i Abril legal@corehub.net Security Level: Email, Account Authentication (None) Electronic Record and Signature Disclosure: Not Offered ID:	DocuSigned by: 2572A37992D24BA... Using IP Address: 80.39.220.15	Sent: 1/13/2016 6:56:22 AM Viewed: 1/15/2016 7:40:44 AM Signed: 1/15/2016 7:47:59 AM
Mary English mary.english@ironmountain.com Vice President and General Manager Iron Mountain Inc. Security Level: Email, Account Authentication (None) Electronic Record and Signature Disclosure: Accepted: 7/8/2015 10:53:18 AM ID: 66fe5012-dedf-4e70-ab18-c3b0ba779e9d	DocuSigned by: Mary English 089DF59B1DCE41B... Using IP Address: 216.229.152.50	Sent: 1/15/2016 7:48:01 AM Viewed: 1/15/2016 8:30:53 AM Signed: 1/15/2016 8:31:06 AM

In Person Signer Events	Signature	Timestamp

Editor Delivery Events	Status	Timestamp

Agent Delivery Events	Status	Timestamp

Intermediary Delivery Events	Status	Timestamp

Certified Delivery Events	Status	Timestamp

Carbon Copy Events	Status	Timestamp

Notary Events		Timestamp

Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	1/15/2016 7:48:01 AM
Certified Delivered	Security Checked	1/15/2016 8:30:53 AM
Signing Complete	Security Checked	1/15/2016 8:31:07 AM
Completed	Security Checked	1/15/2016 8:31:07 AM

Electronic Record and Signature Disclosure

Electronic Record and Signature Disclosure created on: 11/25/2009 3:01:43 PM
Parties agreed to: Mary English

Consumer Disclosure NOT Required