. com Registry Agreement Appendix 1A
Data Escrow Specification

(Effective as of the Updated Data Escrow Effective Date)

Registry Operator will engage an independent entity to act as data escrow agent (the "Escrow Agent") for the provision of data escrow services related to the Agreement pursuant to an agreement substantially in the form of Appendix 2A, as the same may be revised from time to time, among ICANN, Registry Operator and the Escrow Agent.

Changes to the schedule, content, format, and procedure set forth herein may be made only with the mutual written consent of ICANN and Registry Operator (which neither party shall unreasonably withhold) or through the establishment of a Consensus Policy as outlined in Section 3.1(b) of the Agreement.

TECHNICAL SPECIFICATIONS

1 **Deposits**. There will be two types of Deposits: Full and Differential. For both types, the universe of Registry objects to be considered for data escrow are those objects necessary in order to offer all of the approved Registry Services.

1.1 "**Full Deposit**" will consist of data in the registry through 00:00:00 UTC (Coordinated Universal Time) on the day that such Full Deposit is submitted to Escrow Agent.

1.2 "**Differential Deposit**" means data that reflects all transactions that were not reflected in the last previous Full or Differential Deposit, as the case may be. Each Differential Deposit will contain all database transactions since the previous Deposit was completed including data through 00:00:00 UTC of each day, but Monday. Differential Deposits must include complete escrow records as specified below that were not included or changed since the most recent Full or Differential Deposit (i.e., all additions, modifications or removals of data since the last deposit).

2 **Schedule for Deposits**. Registry Operator will submit a set of escrow files on a daily basis as follows:

2.1 Each Monday, a Full Deposit must be submitted to the Escrow Agent by 23:59 UTC.

2.2 The other six (6) days of the week, a Full Deposit or the corresponding Differential Deposit must be submitted to Escrow Agent by 23:59 UTC.

3 **Escrow Format Specification**.

3.1 **Deposit's Format**. Registry objects, such as domains, contacts, name servers, registrars, etc. will be compiled into a file constructed as described in https://datatracker.ietf.org/doc/draft-ietf-regext-data-escrow/, see Section 9, reference 1 of this Appendix and https://datatracker.ietf.org/doc/draft-ietf-regext-dnrd-objects-

mapping/, see Section 9, reference 2 of this Appendix (collectively, the "DNDE Specification"). The DNDE Specification describes some elements as optional; Registry Operator will include those elements in the Deposits if they are available. If not already an RFC, Registry Operator will use the most recent draft version of the DNDE Specification available as of the Updated Data Escrow Effective Date. Registry Operator may at its election use newer versions of the DNDE Specification after the Updated Data Escrow Effective Date. Once the DNDE Specification is published as an RFC, Registry Operator will implement that version of the DNDE Specification, no later than one hundred eighty (180) calendar days after. UTF-8 character encoding will be used.

3.2 **Extensions**. If Registry Operator offers additional Registry Services that require submission of additional data, not included above, additional "extension schemas" shall be defined in a case by case basis to represent that data. These "extension schemas" will be specified as described in Section 9, reference 2 of this Appendix. Data related to the "extensions schemas" will be included in the deposit file described in Section 3.1 of this Appendix. ICANN and Registry Operator shall work together to agree on such new objects' data escrow specifications.

4. <u>Processing of Deposit files</u>. The use of compression is recommended in order to reduce electronic data transfer times, and storage capacity requirements. Data encryption will be used to ensure the privacy of registry escrow data. Files processed for compression and encryption will be in the binary OpenPGP format as per OpenPGP Message Format - RFC 4880, see Section 9, reference 3 of this Appendix. Acceptable algorithms for Public-key cryptography, Symmetric-key cryptography, Hash and Compression are those enumerated in RFC 4880, not marked as deprecated in OpenPGP IANA Registry, see Section 9, reference 4 of this Appendix, that are also royalty-free. The process to follow for the data file in original text format is:

1) The XML file of the deposit as described in Section 9, reference 1 of this Appendix must be named as the containing file as specified in Section 5 but with the extension xml.

2) The data file(s) are aggregated in a tarball file named the same as (1) but with extension tar.

3) A compressed and encrypted OpenPGP Message is created using the tarball file as sole input. The suggested algorithm for compression is ZIP as per RFC 4880. The compressed data will be encrypted using the escrow agent's public key. The suggested algorithms for Public-key encryption are Elgamal and RSA as per RFC 4880. The suggested algorithms for Symmetric-key encryption are TripleDES, AES128 and CAST5 as per RFC 4880.

4) The file may be split as necessary if, once compressed and encrypted, it is larger than the file size limit agreed with the Escrow Agent. Every part of a

split file, or the whole file if not split, will be called a processed file in this section.

5) A digital signature file will be generated for every processed file using the Registry Operator's private key. The digital signature file will be in binary OpenPGP format as per RFC 4880 Section 9, reference 3, and will not be compressed or encrypted. The suggested algorithms for Digital signatures are DSA and RSA as per RFC 4880. The suggested algorithm for Hashes in Digital signatures is SHA256.

6) The processed files and digital signature files will then be transferred to the Escrow Agent through secure electronic mechanisms, such as, SFTP, SCP, HTTPS file upload, etc. as agreed between the Escrow Agent and the Registry Operator. Non-electronic delivery through a physical medium such as CD-ROMs, DVD-ROMs, or USB storage devices may be used if authorized by ICANN.

7) The Escrow Agent will then validate every (processed) transferred data file using the procedure described in Section 8 of this Appendix.

5. **File Naming Conventions**. Files will be named according to the following convention: {gTLD}_{YYYY-MM-DD}_{type}_S{#}_R{rev}.{ext} where:

5.1 {gTLD} is replaced with the gTLD name; in case of an IDN-TLD, the ASCII-compatible form (A-Label) must be used;

5.2 {YYYY-MM-DD} is replaced by the date corresponding to the time used as a timeline watermark for the transactions; i.e. for the Full Deposit corresponding to 2009-08-02T00:00Z, the string to be used would be "2009-08-02";

5.3 {type} is replaced by:

1) "full", if the data represents a Full Deposit;
2) "diff", if the data represents a Differential Deposit;
3) "thin", if the data represents a Bulk Registration Data Access file, as specified in Section 2.1 of Appendix 5A;
4) "thick-{gurid}", if the data represents Thick Registration Data from a specific registrar, as defined in Section 2.2 of Appendix 5A. The {gurid} element must be replaced with the IANA Registrar ID associated with the data.

5.4 {#} is replaced by the position of the file in a series of files, beginning with "1"; in case of a lone file, this must be replaced by "1";

5.5 {rev} is replaced by the number of revision (or resend) of the file beginning with "0": and

5.6 {ext} is replaced by "sig" if it is a digital signature file of the quasi-homonymous file. Otherwise it is replaced by "ryde".

6. **Distribution of Public Keys**. Each of Registry Operator and Escrow Agent will distribute its public key to the other party (Registry Operator or Escrow Agent, as the case may be) via email to an email address to be specified. Each party will confirm receipt of the other party's public key with a reply email, and the distributing party will subsequently reconfirm the authenticity of the key transmitted via offline methods, like in person meeting, telephone, etc. In this way, public key transmission is authenticated to a user able to send and receive mail via a mail server operated by the distributing party. Escrow Agent, Registry Operator and ICANN will exchange public keys by the same procedure.

7. **Notification of Deposits**. Along with the delivery of each Deposit, Registry Operator will deliver to Escrow Agent and to ICANN (using the API described in draft-lozano-icann-registry-interfaces, see Section 9, reference 5 of this Appendix (the "Interface Specification")) a written statement from Registry Operator (which may be by authenticated e-mail) that includes a copy of the report generated upon creation of the Deposit and states that the Deposit has been inspected by Registry Operator and is complete and accurate. The preparation and submission of this statement must be performed by Registry Operator or its designee, provided that such designee may not be the Escrow Agent or any of Escrow Agent's affiliates. Registry Operator will include the Deposit's "id" and "resend" attributes in its statement. The attributes are explained in Section 9, reference 1 of this Appendix.

If not already an RFC, Registry Operator will use the most recent draft version of the Interface Specification at the Updated Data Escrow Effective Date. Registry Operator may at its election use newer versions of the Interface Specification after the Updated Data Escrow Effective Date. Once the Interface Specification is published as an RFC, Registry Operator will implement that version of the Interface Specification, no later than one hundred eighty (180) calendar days after such publishing.

8. **Verification Procedure**.

1) The signature file of each processed file is validated.

2) If processed files are pieces of a bigger file, the latter is put together.

3) Each file obtained in the previous step is then decrypted and uncompressed.

4) Each data file contained in the previous step is then validated against the format defined in Section 9, reference 1 of this Appendix.

5) The data escrow agent extended verification process, as defined below in Section 9, reference 2 of this Appendix, as well as any other data escrow verification process contained in such reference.

If any discrepancy is found in any of the steps, the Deposit will be considered incomplete.

9. **References**.

1) Domain Name Data Escrow Specification (work in progress), https://datatracker.ietf.org/doc/draft-ietf-regext-data-escrow/

2) Domain Name Registration Data (DNRD) Objects Mapping, https://datatracker.ietf.org/doc/draft-ietf-regext-dnrd-objects-mapping/

3) OpenPGP Message Format, http://www.rfc-editor.org/rfc/rfc4880.txt

4) OpenPGP parameters, http://www.iana.org/assignments/pgp-parameters/pgp-parameters.xhtml

5) ICANN interfaces for registries and data escrow agents, https://tools.ietf.org/html/draft-lozano-icann-registry-interfaces