

Registry Data Escrow Service



Data escrow services for achieving compliance with ICANN's Registry Data Escrow Agreements

ICANN AND IRON MOUNTAIN: DATA ESCROW FOR REGISTRIES

Full compliance with data escrow requirements and verification testing is part of the Internet Corporation for Assigned Names and Numbers' (ICANN) strategic plan. This plan is designed to ensure continuation of Domain Name System operations in the event of a physical or business failure of a registry.

As part of its Registry Agreement with ICANN, each registry operator must comply with provisions contained within a Registry Data Escrow Agreement. That agreement requires registries to periodically transfer registry data for their generic top-level domains (gTLD) to a reputable escrow agent to be held in escrow. As a trusted, neutral, third party, Iron Mountain works with registry operators to fulfill this requirement by safeguarding valuable registry data in secure, access-controlled escrow accounts.

Iron Mountain is the global leader in information protection, management, and storage services. In 2001, Iron Mountain was the first company ever selected to protect registry data via escrow agreements, and in 2007 ICANN selected Iron Mountain as its preferred provider of escrow services for registrars with its Registrar Data Escrow program.

THE BENEFITS OF IRON MOUNTAIN ESCROW FOR REGISTRY DATA

Data in escrow with Iron Mountain may be used to help ensure continuity of service in the event of a natural disaster, a technical failure of a registry, or a security breach within the DNS system.

Registry operators and ICANN rely on Iron Mountain to hold each deposit, and, upon certain events, release any retained deposits to ICANN. This ensures that the data associated with registered domain names is never at risk of being lost or inaccessible.

Iron Mountain has proven itself to be a safe, reliable choice for the escrow needs of registries, and we make it as simple as possible to comply with ICANN's escrow requirements. Iron Mountain has more experience with registry and registrar data escrow than any other provider, and our customers appreciate that they are working with an experienced team that understands the domain name industry.

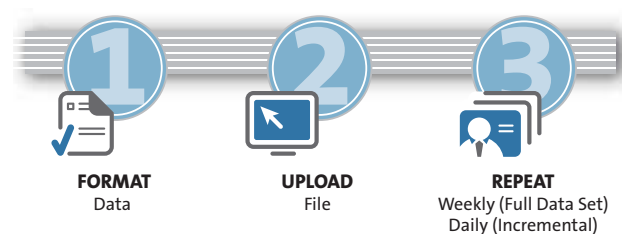
Depositing registry data into secure escrow accounts managed by a neutral third-party such as Iron Mountain helps safeguard the continuity of service across the Internet.

REGISTRY DATA ESCROW BASICS

ICANN established the Registry Data Escrow requirement to restore or continue operation of a registry due to either business or technical failures. Under the terms of the agreement, registries must regularly deposit registration data with an approved third-party provider of escrow services, such as Iron Mountain.

There are currently four different versions of the data escrow requirements in ICANN's gTLD registry agreements. Nearly all registry agreements signed since May 5, 2005 contain almost identical provisions that appear in Article 3.1(c)(i) of the gTLD Registry Agreement.

In essence, the Registry Data Escrow service works as follows. Upon receipt of registry data, Iron Mountain will verify that the data is complete, accurate, and delivered in the intended format. The escrow deposit verification process will validate completeness and integrity of the data, and also confirm that the file format sent is the format received. Complete, properly formatted data is deposited with Iron Mountain on a weekly basis with daily incremental deposits. That data is securely stored, and only accessed by ICANN if needed for business continuity reasons.



GETTING STARTED: 1 – 2 – 3

The data escrow process is uncomplicated. Data to be deposited must be formatted as specified by ICANN, and then encrypted and uploaded via secure FTP (SFTP) transmission. Iron Mountain provides model scripts and detailed setup instructions to aid implementation.

Registries must make one full deposit per week and daily incremental deposits during other days. Full deposits include the contents of all domain objects, host objects, contact objects, registrar objects, and, when applicable, DNSSEC-related key material.

Upon receiving a deposit, Iron Mountain verifies its format and completeness. Iron Mountain then moves the file to a non-public directory and notes the size and existence of the file. Files are decrypted and authenticated to verify that the files actually came from the registry operator. The decrypted file is then destroyed to maintain the security of the data.

Once registries complete the initial setup and establish an automated process, data transmission can be completed with very little time or effort. For security purposes, digital signatures, data encryption, and SFTP technologies are used.

WHY IRON MOUNTAIN?

Iron Mountain can safeguard the interests of registries by protecting and preserving information to help with compliance and continuity needs.

Iron Mountain created the technology escrow industry in 1982 to help companies protect source code and other intellectual property. Today, more than 90% of Fortune 500 companies turn to Iron Mountain for technology escrow protection.

Iron Mountain protects registry data through use of RAID storage and physical back-up tapes that are stored in geographically separated, secure, and environmentally safe facilities accessible only to authorized personnel. At least one of these storage facilities is located 200 feet below ground.

Recognized worldwide as the expert in securely storing vital records with over fifty years of experience, no other provider can approach the depth and experience offered by Iron Mountain. Today, ICANN—along with tens of thousands of customers worldwide—rely on Iron Mountain's technology escrow services to protect their intellectual property.

Iron Mountain looks forward to working with registries to safeguard critical data. Questions? Contact us by email at ipm-info@ironmountain.com or call (800) 962-0652.