# IRON MOUNTAIN®
# IMAGE ON DEMAND
# SECURITY DATASHEET

Iron Mountain Image on Demand service enables digital retrieval of the physical records and documents that you have stored in an Iron Mountain Record Centre. This pay-as-you-go solution enables fast, secure digital access to your documents whenever and wherever you need them.

With Image on Demand, you can rest easy with the knowledge that your information is secure throughout the entire process.

## Comprehensive Employee Training

All Iron Mountain employees that have electronic access are required annually to complete Security Awareness training provided by an internationally recognised leader in compliance training and education.

Every Iron Mountain employee also certifies annually to Iron Mountain's Code of Ethics & Business Conduct ("Code") training. Iron Mountain's Code covers the following information security areas:

> Data Privacy & Security
> Confidential & Proprietary Information
> Protecting Company Assets
> Appropriate Computer Use
> Employee Privacy
> Incident Reporting
> Confidential & Anonymous Helpline

Iron Mountain's Code in all the languages our employees speak around the globe can be accessed at www.ironmountain.com/code.

## Secure Imaging Workstations

Your original files never leave Iron Mountain's custody when you use Image on Demand. All imaging operations are physically located inside our secure facilities. Our Imaging operators undergo the same background checks and drug testing as all Iron Mountain employees, and no camera-enabled personal mobile devices are permitted in the scanning centre.

Access to the imaging workstations is restricted and requires username/password login information. All user activity is logged and monitored. Imaging workstations work on a single application for a single customer at a time. Each imaging application is processed by its own batch class and verified against the customer ID.

All imaging workstations are configured with hardening standards for both servers and networking equipment. In addition, each system is subjected to a vulnerability scan before being put into production. Workstations and servers are equipped with anti-virus software that is updated daily.

Image conversion is performed using dedicated image capture software and hardware connected to Iron Mountain's internal firewall-protected network. Iron Mountain maintains a three tier firewall architecture designed to support defense in depth. Multiple firewall vendors are also used. Perimeter firewalls terminate internet connections and Demilitarised Zone (DMZ) firewalls isolate those network segments. Firewalls are also used to separate layers of the application stack for additional security.

During the capture process, the capture software uses disk storage as cache, re-using and overwriting older information. The output images will be held for 30 days then purged.

## Encrypted Data Transfer

Digital files provided are implemented using Transport Layer Security (TLS), a protocol for transmitting documents via the Internet using encryption technology. This ensures an extremely high level of data transmission security through industry standard encryption technology. As information is transferred between the server and the Web clients, all data is encrypted. The solution uses server-side certificates to encrypt the data using TLS for the Web application. Any Internet traffic that lands on the clear text site using Hypertext Transfer Protocol (HTTP) will be redirected to the secure port for Hypertext Transfer Protocol Secure (HTTPS). When using Web services integration, a two-way authentication is employed using both client-and server-side certificates. All unauthorised requests are rejected. All data is securely and separately stored.

On request, Iron Mountain can set up a dedicated, encrypted communication link to transfer information to a customer

## Restricted User Access

To place an Image on Demand order, customers use Iron Mountain Connect™ , our web-based customer hub. Only authorised Iron Mountain Connect™ users can place an Image on Demand order or retrieve the requested images. All unauthorised requests are rejected. Customer super users are set up by Iron Mountain and can then manage their company's own internal users.

If a customer uses file transfer protocol (FTP) for ingesting assets/documents, access is provided through a secure FTP channel that assigns each customer a unique username and password.

Iron Mountain performs access control reviews for administrative users of the system on a quarterly basis and documents the results.

Learn more about Image on Demand.