

# ACHIEVING SECURITY WITH CLOUD PC BACKUP

CONNECTED®  
BACKUP FOR PC

## EXECUTIVE SUMMARY

Today, more organizations than ever recognize the value and convenience of using cloud backup to protect their data. Organizations considering cloud backup face these security concerns:

- Could an unauthorized individual gain access to backed-up data?
- Could backed-up data be altered?
- Will necessary data be available when needed?
- Is data safe from fire, floods, and human error?

Iron Mountain offers hosted data storage that enables customers to reduce the costs, risks, and complexity of storing and protecting their enterprise information. With our heightened focus on security, privacy, and cost savings, Iron Mountain goes beyond simple cloud storage to enterprise cloud security.

### TRANSFER SECURITY

- Outbound connections only
- SSL encryption (TLS 1.0)
- Authentication by user encryption key and digital certificate
- 128-bit Advanced Encryption Standard (AES)

### STORAGE SECURITY

- 128-bit Advanced Encryption Standard (AES)
- Unique encryption keys

### FACILITY SECURITY

- All data replicated to mirrored facility
- Extensive underground sites
- Gated entrances with 24x7 security guards
- Clean Agent Fire Extinguishing System and on-site firefighting apparatus and personnel
- Internal and external 24x7 monitoring
- External accreditation by the Uptime Institute

### GOVERNMENT COMPLIANCE

- FIPS 140-2 Level 1 validated cryptographic module
- Section 508 of the (U.S.) Rehabilitation Act

## **CONNECTED® BACKUP FOR PC SECURITY OVERVIEW**

Most organization data originates with PC users, whether in the office, or on laptops or home computers. Iron Mountain's Connected® Backup for PC solution can capture and store this vital information regardless of its source – inside or outside the firewall – while dramatically reducing storage costs.

However, it's not enough to back up the data: stored backups must also be secure from outside threats. Iron Mountain meets this need with a cloud-based solution that truly and comprehensively protects the PC data that belongs to your organization. Iron Mountain follows rigorous standards to keep this data safe, including security best practices and Iron Mountain-developed practices.

The bottom line: Iron Mountain takes data protection seriously, and goes to great lengths to protect customer data from all credible threats. The Connected Backup for PC solution provides security at every level, from backup through storage through data retrieval.

This document introduces the many security measures currently in place within the Iron Mountain data protection architecture to prevent unauthorized access or damage to customer data.

## **WHAT IS CONNECTED BACKUP FOR PC CLOUD SERVICE?**

Iron Mountain's Connected Backup for PC cloud solution is a client-server system for file backup from personal computers, over any TCP/IP network, to ultra-secure offsite facilities. The Connected Backup for PC solution is available internationally.

## **CONNECTED BACKUP FOR PC CLOUD SERVICE: SECURITY**

The Connected Backup for PC solution provides a level of security for the customer's data that is better than alternative practices for handling computer data. The following sections show how Iron Mountain creates a secure environment for data transfer, data storage, and account management.

Iron Mountain's security objectives have four aspects:

- 1. DATA TRANSFER SECURITY:** Prevents access to customer's data during transfer for backup or retrieval.
- 2. STORAGE SECURITY:** Prevents unauthorized access to backed up data stored on the server.
- 3. MANAGEMENT SECURITY:** Prevents unauthorized access while providing client account management.
- 4. FACILITY SECURITY:** Iron Mountain's physical security practices and facility hardening.

## KEY SECURITY ASPECTS OF CONNECTED BACKUP FOR PC CLOUD SERVICE

### 1. DATA TRANSFER SECURITY

The Agent is a Connected Backup for PC application that runs on every PC to manage all backup and retrieval activities at the client level. For example, the Agent scans the PC's disk, and determines what data to send to the Data Center servers at Iron Mountain's offsite, highly available, mirrored facilities.

Data transfer security features include:

- The Agent always initiates contact with the Data Center.
- SSL encryption (TLS 1.0) protects all customer information during transmission between Agent and Data Center.
- The Data Center server authenticates the Agent connection using the user encryption key, while the Agent authenticates the server using a digital certificate embedded in the Agent installation package.
- After authentication, the Agent encrypts every file flagged for backup with 128-bit Advanced Encryption Standard (AES) and sends the encrypted data to the Data Center. If organizations use third-party encryption products, such as Microsoft's Encrypting File System (EFS), to encrypt files on PCs, the Agent backs up the encrypted files.

### 2. STORAGE SECURITY

Iron Mountain stores all backup data in secure, offsite facilities. Storage security features include:

- The Data Center stores the 128-bit AES-encrypted files without decrypting them.
- Every account has a unique encryption key, used to encrypt and decrypt each file that the Agent backs up. Only the Agent that encrypted the file can decrypt it. The Agent uses 112-bit Triple DES encryption to send the encryption key to the Data Center securely. The Data Center escrows the encryption key on its secure server.
- Facility servers do not provide a view to customer data. In the highly unlikely event that an individual were able to gain access to data files on the server, that individual would not be able to view the data.

- The Agent requires a valid password, or a valid technician ID and password, when a user tries to retrieve files. This can prevent unauthorized individuals with physical access to another person's client from performing retrieves.
- Changing the account status can temporarily or permanently prevent an Agent from backing up or retrieving files from stolen or unused clients. For example, when an employee leaves the organization, canceling their account prevents unauthorized individuals from accessing files that the former employee backed up.

The Account Management Website is an administration tool that allows users to modify their own profile information, such as their password. The user must enter a valid password to access the Account Management Website. The optional MyRoam® administration tool allows users to retrieve backed-up files using a Web browser instead of the Agent user interface. Only specified users and communities can access MyRoam.

### 3. MANAGEMENT SECURITY

Support Center technicians must possess a valid Technician ID and an associated password. Technician accounts can have varying levels of access to Support Center's features, based on the permissions granted to the technician ID. For example, a given technician might have access only to specific communities.

Staff security features include:

- Access to Data Center areas is restricted to facility administrators only.
- Only Iron Mountain employees and signed-in escorted guests can enter Iron Mountain facilities.
- Iron Mountain employees must display Iron Mountain picture ID/card-key badges at all times. Card key use logs are reported and reviewed regularly.

## 4. FACILITY SECURITY

Iron Mountain protects over 3 petabytes of PC data for some 3 million users in its secure offsite facilities worldwide. Iron Mountain has achieved 99.99 percent uptime for ten years, with most months 100 percent.

Facility security features include:

- All data received by either mirrored facility is replicated at once to its mirror by high-speed links.
- Outages or disasters at either facility do not interfere with the availability of the data.
- All Iron Mountain servers run a hardened version of Microsoft® Windows® Server, using Microsoft best practices and security patches and service packs.
- Up-to-date virus protection: we have never had a mission interruption due to viruses.

Protecting the security of your data is central to Iron Mountain's values. Iron Mountain owns or leases offsite Data Bunkers that provide high-security, environmentally-controlled storage for media, and includes data centers with redundant infrastructure.

These Data Bunkers include the following security measures:

- Extensive multi-acre underground sites.
- Gated entrances with 24x7 security guards.

- Restricted access requiring photo ID and visitor escort.
- Real-time closed circuit TV monitoring.
- Commercial power feeds with full backup generators.
- Clean Agent Fire Extinguishing System (CAFES) and on-site firefighting apparatus and personnel.
- Internal and external 24x7 monitoring for temperature, "waterbug" leaks, smoke, fire, and motion detection.
- External accreditation by the Uptime Institute according to their Tier Classification and Performance Standard.



*Entrance to Iron Mountain underground facility.*

### CONNECTED BACKUP FOR PC LICENSED PRODUCT: SECURITY

Client-side security for the Connected Backup for PC licensed product is similar to client-side security for the cloud Service. However, with the licensed version, server-side security is not provided by Iron Mountain's secure offsite facilities, but is the responsibility of the customer, including server-side networks, servers, firewalls, passwords, and physical facilities.

### GOVERNMENT COMPLIANCE

Connected® Backup uses an embedded Federal Information Processing Standard (FIPS) 140-2 Level 1 validated cryptographic module for Windows XP and Windows 7 personal

computers, and Windows 2003 servers, per the FIPS 140-2 Implementation Guidance section G.5 guidelines.

The Connected® Backup end-user interfaces comply with the requirements for clause 1194.21 of Section 508 of the U.S. Rehabilitation Act (<http://www.access-board.gov/sec508/standards.htm>).

### SUMMARY

Iron Mountain is managing more than 3 petabytes (12 billion backup files) of data at its facilities. Iron Mountain has been backing up PC data since 1995, from the largest enterprises to small businesses. Iron Mountain delivers the expertise customers need to reduce the costs and risks of data protection and storage.



120 Turnpike Road, Southborough, MA 01772

Iron Mountain Digital is the world's leading provider of Storage-as-a-Service solutions for data protection and recovery, archiving, eDiscovery, and intellectual property management. The technology arm of Iron Mountain offers a comprehensive suite of solutions to thousands of companies around the world, directly and through a worldwide network of channel partners.

© 2010 Iron Mountain Incorporated. All rights reserved. Iron Mountain, the design of the mountain, Connected, LiveVault, Delta Block and SendOnce are registered trademarks of Iron Mountain Incorporated in the U.S. and other countries. All other trademarks and registered trademarks are property of their respective owners.