

# IRON MOUNTAIN® SERVER BACKUP ADVANCED SECURITY

No IT professional would ever question the necessity of data backup. However, as a professional, you want to know your data is absolutely secure before, during, and after the backup process. Unlike legacy tape-based solutions – which are vulnerable to theft, disappearance, and deterioration – the powerful, reliable security model employed by Iron Mountain Server Backup solutions can guard against data loss from backup beginning to end.

## END-TO-END ENCRYPTION

With Iron Mountain Server Backup solutions, your data is encrypted through every step of the backup process.

- **Start at the source.** Before your data leaves your server, the information is protected at any of the following levels you choose: 256-bit AES (Advanced Encryption Standard), 128-bit AES, 112-bit 3DES, or 128-bit Blowfish encryption.
- **Over-the-wire encryption.** As your data travels over the Internet to the vault, you can rest easy knowing your information is protected by 128-bit AES encryption. Because Iron Mountain Server Backup deduplication ensures back up of only new or changed blocks, much less data is exposed during backup processes.
- **At-rest encryption.** Your data stays safely encrypted in one of Iron Mountain Server Backup's top-tier rated and ISO-certified or SSAE (Statement on Standards for Attestation Engagements) 16-compliant data centers.

## FIPS-APPROVED AES ENCRYPTION

Iron Mountain Server Backup encryption is certified by NIST (National Institute of Standards and Technology) as specified by FIPS (Federal Information Processing Standards) Publication 197. FIPS 197 designates AES as the standard for encrypting data used by federal departments and agencies, and all FIPS-approved encryption modules comply with that standard. We're committed to meeting or exceeding regulations that enable us to deliver the high level of security you expect and require.



# YOU ALONE CONTROL THE ENCRYPTION KEY

Iron Mountain Server Backup solutions have no “back door” decryption keys. Once you establish your encryption password and settings, no one else can access or decrypt your backup data – not even the Iron Mountain Server Backup employees who manage your information.

## AUTHENTICATION AND AUTHORIZATION

You are in control from the moment you initiate your backup through to communications and management. Both authorization and authentication are required to begin every backup and restoration session and your Iron Mountain Server Backup solution will identify and validate the system, the account, the username and password used to access the vault. What’s more, the authentication information itself is encrypted for added security, and any interaction between your systems and the vault must be initiated on your end.

## STAY IN CONTROL WITH IRON MOUNTAIN SERVER BACKUP SECURITY

Iron Mountain Server Backup offers:

- ✓ Authentication between your systems and our remote vaults
- ✓ Encrypted communications while managing backup processes
- ✓ Flexible, role-based security

Iron Mountain Server Backup solutions encrypt any interactions with the management portal, so you can configure your backup jobs and policies without compromising the security of your systems.

Iron Mountain Server Backup’s role-based security model likewise enables you to flexibly control access to the system. Various security options let you choose who has the power to restore, encrypt, and decrypt data, or perform other backup or restoration-related functions.

## SSAE 16 COMPLIANCE:

As an added layer of protection and assurance, Iron Mountain Server Backup maintains SSAE 16 (Statement on Standards for Attestation Engagements No. 16) compliance. SSAE 16 addresses service organization and is comprised of guidelines for trusted data security, confidentiality, integrity, availability, and privacy controls. In today’s regulated business environment, SSAE 16 compliance is an excellent way to demonstrate good faith when hosting or processing customer data.

Iron Mountain Server Backup systems also undergo annual SSAE 16 audits, which include compliance reports issued by independent auditors.

## OPERATIONAL SECURITY:

With Iron Mountain Server Backup, you can easily track backup and restoration using detailed logs that create auditable paper trails. In addition, procedural, electronic, mechanical, and physical controls safeguard the security of every Iron Mountain Server Backup data center. These controls include:

- Key-card and/or biometric access
- 24/7 surveillance cameras
- Background checks on all employees
- Data center access limited to authorized employees