

## Vbrick™ Rev Encryption Key Management Introduction

### *Background*

Vbrick™ Rev is a cloud platform for live video streaming and video on-demand content management. Rev securely handles video storage at rest by leveraging Amazon Web Services (AWS) S3's built-in encryption. In addition to video files, Rev also stores and manages supplemental files of various types to aid and enhance the video management functionality.

Rev resides on Amazon's AWS cloud platform. The storage solution used by Rev for video storage is AWS S3 object storage.

AWS S3 includes encryption that Rev uses to offload all encryption, decryption and key management functions to S3 by default. AWS' S3 managed Server Side Encryption (SSE) uses a Master Encryption Key (MEK) and a Data Encryption Key (DEK) that is unique to each file/object that automatically encrypts all files within a Rev tenant. The Rev application never has knowledge of encryption keys nor does it execute the encryption.

### *Master Encryption Key Management Feature*

Rev offers a feature to allow customers to create and maintain their own Master Encryption Key to encrypt and decrypt files in their Rev tenant. With this feature, there are two options for MEK creation:

1. Rev customers may create their own AWS Key Management Service (KMS) account directly with AWS and use the AWS KMS features to create a MEK;
2. Rev customers may generate a MEK within their own third party Key Management solution and securely import the MEK into a Vbrick managed AWS KMS account or a customer managed AWS KMS account.

Rev then enables customers to rotate the active Master Key at a frequency of their choosing.

For more information on AWS' KMS see <https://aws.amazon.com/kms>.

### *Customer Responsibility*

#### **NOTE: CUSTOMERS SHOULD USE EXTREME CAUTION WHEN ROTATING MASTER KEYS.**

In cases where customers are creating and managing their own Master Keys, in order to prevent permanent loss of access to video and other files within the customer's Rev tenant, customers MUST:

1. Grant and ensure uninterrupted access to their Master Key within their KMS;
2. Ensure access to both **current** and **new** Master Keys during Master Key rotation. Access to the current key can be revoked **ONLY** after confirming that key rotation is 100% successful in Rev.

If access to the Master Key is lost at any time, then **REV, EITHER BY SOFTWARE OR MANUAL INTERVENTION, WILL NOT BE ABLE TO DECRYPT ANY FILE, VIDEO FILES OR ADDITIONAL FILES, AND THEREFORE THE DATA WILL BE CONSIDERED LOST AND IRRECOVERABLE.**

This feature requires customers to execute a contractual amendment to confirm their understanding of responsibilities as it relates to Master Encryption Key management. To enable this feature, contact Vbrick Customer Success at <https://vbrick.com/support>, who will provide the contractual amendment for execution by an authorized company official.