# The Playbook for Granting Third-Party Access to AWS S3

Amir Boroumand

Founder, Penguin Systems
penguinsys.com

# Avoid using IAM access keys which can be leaked

There are security risks associated with generating IAM access keys and secret keys for third-party vendors.

The keys could be mishandled or leaked, which would mean anyone with these credentials can gain unauthorized access to your bucket.

# Use cross account role if the third-party also has an AWS account

If the third-party vendor has their own AWS account, setting up cross-account access is a secure way to grant them access to your resources.

This can be done by creating an IAM role in your account that specifies what permissions the third party should have, and then allowing their AWS account to assume this role.

# Use AWS STS if they do not have an AWS account

For vendors without an AWS account, using AWS STS to generate temporary, limited-privilege credentials is an excellent approach.

It requires some integration work because the third party must authenticate into your system which then will request temporary credentials from STS by calling assumeRole on a role that has the requisite access.

The STS credentials can then be provided to the vendor.

## Need help setting up secure third-party access to your S3 buckets?

## Reach out today!

amir@penguinsys.com