AWS S3 Bucket Policy - Read-Only Public Access with Security Conditions

This document explains the AWS S3 bucket policy created for read-only public access with security considerations and conditions.

Policy Overview

The policy provides: 1. Read-only public access to objects in your S3 bucket 2. Security through HTTPS-only access requirement 3. Template format that can be customized for your specific bucket

How to Use This Policy

1. Replace `BUCKET-NAME` in the policy with your actual bucket name
2. Apply this policy in the AWS S3 console:
3. Go to your S3 bucket in the AWS Management Console
4. Select the "Permissions" tab
5. Under "Bucket Policy", click "Edit" and paste the modified policy

6. Click "Save changes"

7. Ensure your bucket's Block Public Access settings are configured appropriately:

8. Some settings may need to be disabled to allow public read access
9. Review AWS documentation on Block Public Access for security best practices

Security Implications

This policy implements the following security measures:

1. **Read-Only Access**: Only allows `s3:GetObject` operations, preventing write or delete operations
2. **HTTPS Requirement**: All requests must use HTTPS (SSL/TLS), protecting data in transit
3. **Scope Limitation**: Access is limited to objects within the specified bucket

Additional Considerations

- Monitor your bucket access logs regularly
- Consider implementing additional security measures like IP restrictions if needed
- Review AWS documentation for the latest security best practices

Policy Customization

You can further customize this policy by: - Adding IP address restrictions - Limiting access to specific object prefixes - Adding time-based conditions - Implementing AWS KMS encryption requirements