Group : Data Tech - Developer

AWS Account :

1. LGI_BBR_Prod
2. LGI_BBR_DEV
3. LGI_Dataplatform_Dev
4. LGI_Dataplatform_Prod

Permession Set Name : DT-Developer

Permission hanya memberikan akses ke lambda, ec2, s3, athena, & Glue

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Allow",
      "Action": [
        "lambda:*",
        "ec2:*",
        "s3:*",
        "athena:*",
        "glue:*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Group : Data Tech - Root

AWS Account :

1. LGI_BBR_Prod
2. LGI_BBR_DEV

3. LGI_Dataplatform_Dev
4. LGI_Dataplatform_Prod

Permession Set Name : MfaForce

Permission untuk block semua service jika tidak diaktifkan mfa nya

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowViewAccountInfo",
      "Effect": "Allow",
      "Action": "iam:ListVirtualMFADevices",
      "Resource": "*"
    },
    {
      "Sid": "AllowManageOwnVirtualMFADevice",
      "Effect": "Allow",
      "Action": [
        "iam:CreateVirtualMFADevice"
      ],
      "Resource": "arn:aws:iam::*:mfa/*"
    },
    {
      "Sid": "AllowManageOwnUserMFA",
      "Effect": "Allow",
      "Action": [
        "iam:DeactivateMFADevice",
        "iam:EnableMFADevice",
        "iam:GetUser",
        "iam:GetMFADevice",
        "iam:ListMFADevices",
        "iam:ResyncMFADevice"
      ],
      "Resource": "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid": "DenyAllExceptListedIfNoMFA",
      "Effect": "Deny",
      "NotAction": [
        "iam:CreateVirtualMFADevice",
        "iam:EnableMFADevice",
        "iam:GetUser",
```

```
          "iam:ListMFADevices",
          "iam:ListVirtualMFADevices",
          "iam:ResyncMFADevice",
          "sts:GetSessionToken"
        ],
        "Resource": "*",
        "Condition": {
          "BoolIfExists": {
            "aws:MultiFactorAuthPresent": "false"
          }
        }
      }
    ]
}
```

Group: Data Tech - Administrator

AWS Account :

1. LGI_BBR_Prod
2. LGI_BBR_DEV
3. LGI_Dataplatform_Dev
4. LGI_Dataplatform_Prod

Permession Set Name : Administrator

1. AdministratorAccess

Group: Data Tech - Power User

AWS Account :

1. LGI_BBR_Prod
2. LGI_BBR_DEV
3. LGI_Dataplatform_Dev
4. LGI_Dataplatform_Prod

Permession Set Name : PowerUser

1. PowerUserAccess

Group: Data Tech - ReadOnly

AWS Account :

1. LGI_BBR_Prod
2. LGI_BBR_DEV
3. LGI_Dataplatform_Dev
4. LGI_Dataplatform_Prod

Permession Set Name : ReadOnlyAccess

1. ReadOnlyAccess

Group: Data Tech - Custom Permission

AWS Account :

1. LGI_Dataplatform_Prod

Permession Set Name : CustomPolicy

Permission hanya spesifik bisa akse ke s3 saja ke bucket raw-data, bronze, silver, gold, & pointsystem di account LGI_Dataplatform_Prod

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::carrot-prod-raw-data-bucket",
```

```
        "arn:aws:s3:::carrot-prod-bronze-data-bucket",
        "arn:aws:s3:::carrot-prod-gold-data-bucket",
        "arn:aws:s3:::carrot-prod-silver-data-bucket",
        "arn:aws:s3:::carrot-prod-pointsystem-data-bucket"
      ]
    },
    {
      "Sid": "Statement1",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:ListBucketVersions",
        "s3:GetObject"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```