AWS IAM User Creation with Terraform – Runbook

■ Purpose

This runbook describes the standard operational procedure to create AWS IAM users using Terraform. It covers authentication, least-privilege permissions, execution steps, and verification.

■ Prerequisites

- Terraform installed
- AWS CLI installed and configured
- IAM user with least-privilege permissions
- Access to AWS account 735339531099
- Region: eu-west-1

■ Authentication

Terraform authenticates using AWS CLI credentials. No credentials are stored in Terraform code. The IAM user terraform-selam is used for execution.

```
aws sts get-caller-identity
```

■ Least-Privilege Permissions

The IAM user is added to a dedicated group with a custom least-privilege policy. The policy allows only IAM user lifecycle actions required by Terraform.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:CreateUser",
        "iam:GetUser",
        "iam:ListUsers",
        "iam:DeleteUser",
        "iam:TagUser"
      ],
      "Resource": "arn:aws:iam::735339531099:user/tf-*"
    }
  ]
}
```

■ Terraform Configuration

```
provider "aws" {
  region = "eu-west-1"
}

resource "aws_iam_user" "example" {
```

```
    name = "tf-selamboss"
}
```

■ Execution Steps

```
terraform init
terraform plan
terraform apply
```

■ Verification

Confirm successful execution by reviewing Terraform output and verifying the user exists in AWS Console under IAM → Users.

■ Conclusion

This runbook ensures secure, auditable, and repeatable IAM user creation using Terraform while following least-privilege principles.