IAM Implementation

SOP: Securing Root Account and Setting Up IAM Roles and Policies

1. **Objective**: Secure the AWS root account and implement IAM roles and policies for team members.
2. **Procedure**:
   Secure Root Account:
   1. Enable Multi-Factor Authentication (MFA) on the root account:
      - Sign in to the AWS Management Console as the root user.
      - Navigate to the IAM dashboard.
      - Click on "Activate MFA on your root account" and follow the on-screen instructions to set up MFA using a virtual or hardware MFA device.
   2. Create a strong, unique password for the root account and store it securely.
3. **Set Up AWS Identity Center**:
   1. Navigate to the AWS Management Console.
   2. Open the **AWS Identity Center**.
   3. Configure AWS Identity Center:
      - Set up the identity source (e.g., AWS Managed Microsoft AD, AD Connector, or External IdP via SAML).
      - Define groups and assign users to these groups.
   4. Enable multi-factor authentication (MFA) for all users in Identity Center to add an additional layer of security.
4. **Create IAM Roles and Policies**:
   1. Define the roles and responsibilities of each team member.
   2. Create IAM roles for each team member:
      - Go to the IAM dashboard.
      - Click on "Roles" and then "Create role."
      - Select "AWS service" or "Another AWS account" based on the requirement.
      - Choose the appropriate service that the role will use.
      - Attach the necessary policies to the role (e.g., ReadOnlyAccess, AdministratorAccess).
      - Review and create the role.
   3. Create IAM policies with least privilege access for each role:
      - Go to the IAM dashboard.
      - Click on "Policies" and then "Create policy."
      - Define the policy using the policy editor or policy generator.
      - Review and create the policy.
   4. Attach policies to the corresponding IAM roles:

- Go to the IAM dashboard.
- Click on "Roles," select the role, and attach the required policies.

5. Assign IAM roles to users in AWS Identity Center:
    - Go to the AWS Identity Center console.
    - Select the user or group.
    - Assign the appropriate IAM roles to ensure users have the correct level of access.

Verification and Monitoring:

1. Regularly review and update IAM roles and policies to ensure they align with current security and access requirements.
2. Monitor IAM user activity using AWS CloudTrail and AWS Config to detect any unauthorized or unusual activity.
3. Conduct periodic audits to verify that MFA is enabled and enforced for all users, including the root account.
4. Use AWS IAM Access Analyzer to identify and mitigate any potential overly permissive access policies.

Training and Documentation:

1. Provide training for all team members on AWS Identity Center and IAM best practices.
2. Document all IAM roles, policies, and access controls for future reference and compliance purposes.