**AWS ACCOUNT GOVERNANCE GUIDELINES AND PROCEDURES**

AWS customers look to move quickly and securely when launching new business innovations. The multi-account environment provides guidance to help customers plan their AWS environment.

This document covers guidelines and procedures for AWS accounts including Strategic and Tactical aspects.

**Strategic Points for AWS Account Governance:**

| **Sr. #** | **Description** | **References / Procedures** |
| --- | --- | --- |
| 1 | Implement AWS Organizations for Account Management: Use AWS Organizations to centralize and manage multiple AWS accounts under a single umbrella. This allows for better governance, security, and cost management across the organization. | [AWS Organizations User Guide](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_introduction.html) |
| 2 | Establish Clear Account Structure: Design and implement a well-defined account structure using AWS Organizations, including organizational units (OUs) and account hierarchies. This helps with account isolation, resource management, and centralized policy enforcement. | [AWS Organizations Best Practices](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_best-practices.html) |
| 3 | Leverage Service Control Policies (SCPs): Use SCPs to define fine-grained permissions and access controls for AWS accounts within an organization. SCPs help enforce security and compliance policies across accounts. | [Service Control Policies Overview](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scp.html) |
| 4 | Enable AWS Single Sign-On (SSO): Implement AWS SSO to centrally manage user access and authentication across AWS accounts. This simplifies user management, provides centralized control, and enhances security. | [AWS Single Sign-On User Guide](https://docs.aws.amazon.com/singlesignon/latest/userguide/what-is.html) |
| 5 | Implement Multi-Factor Authentication (MFA): Enable MFA for all user accounts to add an extra layer of security. This helps protect against unauthorized access to AWS resources. | [Activating and Deactivating AWS MFA Devices](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_enable_virtual.html) |

**Tactical Points for AWS Account Governance:**

| **Sr. #** | **Description** | **References / Procedures** |
| --- | --- | --- |
| 1 | Implement Least Privilege Principle: Follow the principle of least privilege when assigning IAM permissions to users, roles, and groups. Grant only the necessary permissions required to perform specific tasks. | [IAM Best Practices](https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html) |
| 2 | Regularly Rotate Access Keys: Regularly rotate access keys for IAM users and other AWS entities to minimize the risk of unauthorized access. Use AWS Secrets Manager or AWS CLI to automate key rotation. | [Rotating Access Keys](https://docs.aws.amazon.com/general/latest/gr/aws-access-keys-best-practices.html#rotate-access-keys) |
| 3 | Enable AWS CloudTrail for Logging and Monitoring: Enable AWS CloudTrail to capture API activity and monitor changes made to your AWS account. This provides valuable audit and compliance information. | [AWS CloudTrail User Guide](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/what_is_cloud_trail_top_level.html) |
| 4 | Implement VPC and Network Security Best Practices: Design and configure your Virtual Private Cloud (VPC) using best practices, including network segmentation, security groups, Network ACLs, and VPC flow logs. | [VPC Security Best Practices](https://docs.aws.amazon.com/vpc/latest/userguide/vpc-security-best-practices.html) |
| 5 | Follow the Well-Architected Framework: Adhere to the AWS Well-Architected Framework's five pillars (Operational Excellence, Security, Reliability, Performance Efficiency, and Cost Optimization) when designing and operating your AWS resources. | [AWS Well-Architected Framework](https://aws.amazon.com/architecture/well-architected/) |

**Example references for detailed procedures**-

| **AWS Account Governance** | **Example 1** | **Example 2** |
| --- | --- | --- |
| **Implement Least Privilege Principle** | **Create an IAM policy with granular permissions for a specific user.** | **Use IAM roles and permissions to restrict access to S3 buckets.** |
| Reference: [IAM Best Practices](https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html) | Reference: [Creating IAM Policies](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_create.html) | Reference: [Using IAM Roles to Delegate Permissions to Applications](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use.html) |
| **Regularly Rotate Access Keys** | **Enable automatic rotation of access keys for IAM users.** | **Use AWS Secrets Manager to automate the rotation of database credentials.** |
| Reference:[Best practices to protect your account's root user](https://docs.aws.amazon.com/accounts/latest/reference/best-practices-root-user.html)  [Best practices for managing AWS access keys](https://docs.aws.amazon.com/accounts/latest/reference/credentials-access-keys-best-practices.html) | Reference: [Rotating Access Keys](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html#Using_RotateAccessKey) | Reference: [Rotating Database Credentials Stored in Secrets Manager](https://docs.aws.amazon.com/secretsmanager/latest/userguide/rotating-secrets.html) |
| **Enable AWS CloudTrail for Logging and Monitoring** | **Create a CloudTrail trail to log API activity in all regions.** | **Configure CloudTrail to deliver logs to an S3 bucket and CloudWatch Logs.** |
| Reference: [AWS CloudTrail User Guide](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/what_is_cloud_trail_top_level.html) | Reference: [Creating a Trail in the CloudTrail Console](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-create-a-trail-using-the-console-first-time.html) | Reference: [Logging CloudTrail Events with CloudWatch Logs](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html) |
| **Implement VPC and Network Security Best Practices** | **Set up network segmentation using multiple VPCs and subnets.** | **Configure security groups and Network ACLs to control inbound/outbound traffic.** |
| Reference: [VPC Security Best Practices](https://docs.aws.amazon.com/vpc/latest/userguide/vpc-security-best-practices.html) | Reference: [Creating a VPC](https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html) | Reference: [Security Group Rules](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html#AddRemoveRules) |
| **Follow the Well-Architected Framework** | **Perform regular reviews of your architecture based on the pillars of the Well-Architected Framework.** | **Implement horizontal scaling to ensure reliability and performance.** |
| Reference: [AWS Well-Architected Framework](https://aws.amazon.com/architecture/well-architected/) | Reference: [Reviewing Your Architecture Using the Well-Architected Tool](https://docs.aws.amazon.com/wellarchitected/latest/userguide/intro-review-your-architecture.html) | Reference: [Auto Scaling Groups](https://docs.aws.amazon.com/autoscaling/ec2/userguide/AutoScalingGroup.html) |

Please note that the examples provided are simplified for example purposes. In actual implementation, the specific requirements and configurations may vary based on your organization's needs and policies