# AWS SOPs

## Root Account Usage

* Avoid using the root account for regular workload activities.
* Create and use separate AWS Identity and Access Management (IAM) users with appropriate permissions.
* The root account should only be used for initial account setup and emergency access purposes.
* Do not share root account credentials with anyone.

## Contact Information

* Set the contact information for each AWS account to a corporate email address or phone number.
* Ensure that the contact information is accurate and up to date.
* Periodically review and update the contact information as required.

## Password & MFA

* Use strong, complex passwords that include a mix of upper- and lower-case letters, numbers, and special characters.
* Avoid using common passwords and personnel information in password.
* Enable Multi-Factor Authentication (MFA) for all AWS accounts, including the root account.
* Document the MFA device or service used for each account and store the relevant information securely.

## CloudTrail Logging:

* Enable CloudTrail logs in all regions for AWS account.
* Configure CloudTrail to send logs to a dedicated Amazon S3 bucket.
* Implement appropriate access controls to protect the CloudTrail logs from accidental deletion or unauthorized access.
* Regularly review and monitor CloudTrail logs for any suspicious activities or security incidents.

## Documentation and Communication:

* Maintain a centralized record or database of all created AWS accounts, including relevant details such as account names, responsible personnel, and creation dates.
* Communicate the account details and any specific instructions to the appropriate stakeholders.
* Ensure that all relevant teams, such as operations, security, and support, are aware of the new account and its associated requirements.

## IAM

* Dedicated user account must be created for each user. No 2 users should be using same account.
* Utilize temporary credentials, such as IAM roles, whenever possible instead of long-term access keys.
* Define and manage IAM roles that grant specific permissions required for individual tasks or functions.
* Assign IAM roles to users or applications based on the principle of least privilege.
* Access to account should be restricted if access is not required any more.
* Do not share your credentials with anyone.
* When creating IAM user provide full details of user for better understanding.
* Set standard password policy for IAM users.
* Use groups and roles to assign permissions instead of applying permissions to users.

## EC2

* Only open required ports on VM. Not additional or unused ports should be left open.
* Create VM of right size, not larger, not smaller.
* Select replication, multi AZ feature depending on the criticality of work / environment.
* Add necessary tags on all resources while creating.
* Check prices of resource before creating them. Take help of your lead with price confirmation.
* Enable termination protection for critical instances to prevent accidental termination.
* Isolate instances within Virtual Private Clouds (VPCs) for better network control and security. Keep all project / environment in their respective VPCs.
* Create unique username and password for all VMs. Prefer to use PEM key for authentication.
* Stop / Terminate unused or idle instances to optimize cost and prevent unnecessary resource usage.
* Use elastic IP address only when it is required. Avoid using it.

## S3

* Apply least privilege permissions to S3 bucket policies and IAM roles to restrict access to sensitive data.
* Enable server-side encryption for all S3 buckets storing sensitive information.
* Turn on versioning for S3 buckets to protect against accidental deletions or overwrites.
* Turn on Block Public Access at the bucket level to prevent accidental public access to sensitive data.
* Use S3 Object Lock to prevent deletion or modification of objects.
* Ensure versioning is enabled for all buckets storing critical or sensitive data to retain previous versions of objects. Define maximum versions to keep.
* Implement lifecycle policies to automatically transition objects to lower-cost storage tiers or delete them when no longer needed.