**SOP for AWS root account usage**

**Objective**: The objective of this document is to provide **guidelines** for establishing internal processes for creating AWS accounts on behalf of Basik Marketing. These processes ensure security, best practices, and effective management of customer accounts within the AWS environment. This document also provides the **procedural steps** to implement important aspects for the AWS root account usage.

1. **When to Use Root Account for Workload Activities**:  
   1.1. The root account should only be used for initial setup and administrative tasks, such as creating and managing AWS accounts for customers.   
   1.2. Discourage the use of the root account for day-to-day workload activities to minimize the risk of unauthorized access or accidental misconfiguration.   
   1.3. Emphasize the importance of using IAM (Identity and Access Management) roles and users for regular workload activities

1.4 Using the root AWS account for **workload activities should be avoided** as much as possible.

1. **Enable Multi-Factor Authentication (MFA) on Root Account**:  
    2.1. Enable MFA on the root account to add an extra layer of security.  
    2.2. Educate staff on how to properly set up and use MFA, including the recommended MFA device options.  
    2.3. Clearly communicate the MFA policy to employees and ensure compliance.
2. **Set Contact Information to Corporate Email Address or Phone Number**:  
    3.1. Set the contact information for the AWS account to the customer's corporate email address or a designated phone number.   
   3.2. Regularly review and update contact information to ensure it remains accurate and up to date.   
   3.3. Establish a process for verifying and validating contact information changes to prevent unauthorized modifications.
3. **Enable CloudTrail Logs in All Regions**:  
    4.1. Enable AWS CloudTrail in all regions to capture API activity logs for security and auditing purposes.   
   4.2. Ensure that the CloudTrail service is active and properly configured in each AWS region.   
   4.3. Regularly review and analyze CloudTrail logs for any suspicious activity or potential security breaches.
4. **Protect CloudTrail Logs from Accidental Deletion with a Dedicated S3 Bucket**:  
    5.1. Create a dedicated Amazon S3 bucket to store CloudTrail logs.  
    5.2. Implement appropriate access controls and permissions to restrict modification or deletion of the CloudTrail logs.   
   5.3. Regularly review and monitor the access logs of the S3 bucket for any unauthorized access attempts.

**General Best Practices:**

1. **Documented Processes**:   
   6.1. Maintain clear and well-documented processes for creating and managing AWS accounts on behalf of customers.  
   6.2. Document steps to follow, including required approvals, permissions, and security checks.   
   6.3. Regularly review and update the documentation to reflect any changes in policies or procedures.
2. **Role-Based Access Control (RBAC)**:   
   7.1. Implement a role-based access control system using AWS IAM.   
   7.2. Assign appropriate permissions to users and groups based on their roles and responsibilities.   
   7.3. Regularly review and update permissions to align with changes in personnel or responsibilities.
3. **Regular Auditing and Review**:   
   8.1. Conduct regular audits and reviews of AWS accounts and associated resources to identify potential security vulnerabilities or misconfigurations.  
    8.2. Use AWS Trusted Advisor and other AWS-native tools to assess account security and compliance.   
   8.3. Establish a process for addressing and remediating any identified issues promptly.
4. **Ongoing Training and Awareness**:  
    9.1. Provide regular training and awareness programs to educate employees about AWS security best practices.   
   9.2. Promote a culture of security awareness and responsibility within the organization. 9.3. Stay updated on AWS security announcements and best practices to ensure continuous improvement.
5. **Incident Response and Disaster Recovery**:  
    10.1. Develop and maintain an incident response plan specific to AWS accounts and resources.  
    10.2. Establish backup and disaster recovery mechanisms to ensure business continuity in case of data loss or system failures.  
    10.3. Regularly test the incident response plan and backup mechanisms to validate their effectiveness.

Below table details the **SOP’s / Procedural Steps** to implement key aspects for AWS root account in Basik Marketing-

| **Process** | **Detailed SOP Steps** |
| --- | --- |
| When to Use Root Account for Workload Activities | 1. Using the **root AWS account for workload activities should be avoided as much as possible**. The root account has unrestricted access to all resources and controls within an AWS account, making it a high-security risk if compromised. It is generally recommended to follow the principle of least privilege and use IAM (Identity and Access Management) users or roles with specific permissions for workload activities.  2. Determine if the activity requires root account access. Managing account-level settings. Typical use cases for root account recommended are for below tasks:-   * Creating and managing IAM users: Although it's recommended to delegate user management to IAM administrators, creating and managing IAM users initially requires root account access. * Managing AWS Organizations: Root account access is necessary to create, manage, and delete AWS Organizations, which help you manage multiple AWS accounts. * Managing cross-account access: Configuring cross-account access using IAM roles, setting up roles for AWS Single Sign-On (SSO), and establishing trust relationships between accounts usually requires root account access. * Recovering deleted resources: In certain cases, the root account may be required to restore accidentally deleted resources, such as S3 buckets, EC2 instances, or RDS databases. * Managing AWS Support cases: Root account holders can interact directly with AWS Support and manage support cases related to their account. * Deactivating and closing an AWS account: When closing an AWS account, the root account must initiate the process and confirm the closure.   3. If not, instruct the user to use an appropriate IAM role or user.  4. If root account access is necessary, document the justification and obtain necessary approvals.  5. Perform the required activity using the root account.  6. Once the task is completed, disable root account access and revert to IAM roles or users. |
| Enable Multi-Factor Authentication (MFA) on Root Account | 1. Access the AWS Management Console using the root account.  2. Navigate to the IAM service and select the root account.  3. Enable MFA by following the provided instructions.  4. Configure the MFA device, either physical or virtual.  5. Test MFA to ensure it is working correctly.  6. Communicate the MFA policy and instructions to all relevant personnel. |
| Set Contact Information to Corporate Email Address or Phone Number | 1. Access the AWS Management Console using the root account.  2. Navigate to the "My Account" page in the account settings.  3. Update the contact information with the corporate email address or designated phone number.  4. Verify the changes through the verification process, if applicable.  5. Document the updated contact information for future reference.  6. Regularly review and update contact information as needed. |
| Enable CloudTrail Logs in All Regions | 1. Access the AWS Management Console using the root account.  2. Navigate to the AWS CloudTrail service.  3. Enable CloudTrail in all regions by selecting the desired settings.  4. Configure the log file integrity validation settings and log file encryption options.  5. Review the CloudTrail settings and ensure they align with the organization's requirements.  6. Regularly monitor the CloudTrail status and troubleshoot any issues. |
| Protect CloudTrail Logs from Accidental Deletion with a Dedicated S3 Bucket | 1. Create a dedicated S3 bucket for storing CloudTrail logs.  2. Define a naming convention and encryption options for the bucket.  3. Implement IAM policies to restrict access to the bucket and allow only authorized users or roles.  4. Enable versioning and MFA delete capabilities for the bucket.  5. Test the access controls and verify that CloudTrail logs are properly stored in the dedicated bucket.  6. Regularly review the bucket's access logs and monitor for any unauthorized access attempts. |