Baseline for all AWS accounts (v1.1 w.e.f 20SEP2022):

1. IAM Account:

DO:	a) Root account must enable MFA, and no root access key should be created. b) MFA must be enabled for all users who have write permission to any AWS services. c) Enable AWS console audit log (e.g. Access Analyzer). d) Password policy should follow the following default rules: i) Minimum length of 8 characters and maximum length of 64 characters. ii) Allow usage of ASCII and Unicode characters. iii) Cannot be identical to AWS account or email address. e) Regular clean up of old/not in use resources (at least quarterly): i) Users ii) Roles iii) Policies
DO NOT:	a) Share account details with others.

2. EC2:

DO:	a) SSH access must be restricted, no source of 0.0.0.0/0. b) Disable all ports that are not in use. c) Internet facing ports opened must be audited. d) EBS has to be encrypted with at least default encryption. e) Inbound traffic must be encrypted, with at least TLS v1.2 and HTTPS f) System logs must be enabled, stored for minimum 1 year i) Auth/secure logs ii) Web server logs iii) Rsyslogs g) ELB, SSL and all resources must use safe ciphers, Key Algorithms and MAC protocols. Refer to this list: https://infosec.mozilla.org/guidelines/openssh h) Regular clean up of old/not in user resources (at least quarterly): i) Security groups ii) SSH key pairs. i) Patch, update and secure operating system in instance regularly or when major security vulnerability is found.

	i) Keep patch/update log(s) for at least 1 year. j) Install anti-virus program with latest signatures to protect against malicious programs. E.g. ClamAV.
DO NOT:	a) Use 0.0.0.0/0 if the instance is not to be public facing. b) Use “All traffic” where all ports are opened whenever possible. c) Share any accounts / credentials, specifically keypairs, username, password d) Use default security groups

3. S3:

DO:	a) S3 bucket must be encrypted, at least with default SSE-S3. b) Block public access should be enabled, unless approval for public access is granted via form.

4. VPC

DO:	a) Enable flow logs. b) Implement Web Application Firewall (WAF) c) Enable AWS Guardduty for intra-VPC network traffic.
DO NOT:	a) Use the default VPC provided by AWS.

5. Others:

5.1. RDS:

DO:	a) Access should be restricted if placed in a public subnet, else set up in a private subnet. b) If passwords are stored in a database, they should be encrypted. No storing of clear passwords.

5.2. Cloudtrail:

DO:	a) Must be enabled. b) Turn on Cloudtrail log file validation so changes made to the file can be tracked to ensure log file integrity.

	c) Enable access logging for Cloudtrail log S3 bucket to track access requests and identify potentially unauthorized or unwarranted access attempts.

5.3. Guardduty:

DO:	a) Must be enabled in all regions that have AWS services running.