**IAM – Identity and Access Management**

1. **Authentication**
   1. Ability to log into an aws account
      1. Username/Password
   2. Verifies that you say you are who you are.
2. **Authorization** 
   1. These is the ability to access resources once logged in the aws account
3. **Groups**
   1. To organize users in one location.
   2. Only need to grant group policy which applies to all user in same group
      1. **Use cases** 
         1. Administrators in Admin folder
         2. Developers in Dev folder
         3. Engineers in AWSEng folder
4. **IAM Users**
   1. Programmatic Access/Service Account
      1. Access Key ID
      2. Secret Access Key
         1. Log into Aws account using command line interface (CLI) or powershell
         2. SDK – Software development kit
         3. APIs – Application Programming interface
      3. To perform application task.
      4. No MFA
   2. AWS Management Console Access
      1. Log into our aws management console using the internet browser (safari, chrome, IE. etc)
      2. Enable MFA
5. IAM Roles
   1. An IAM role is an IAM entity that defines a set of [permissions](https://aws.amazon.com/iam/details/manage-permissions/) for making AWS service requests. IAM roles are not associated with a specific user or group. Instead, trusted entities assume roles, such as IAM users, applications, or AWS services such as EC2.**Policies**
   2. A policy is a JSON format document that contains rules **granting** or **denying** access to a service in AWS
6. Account Password policy
   1. Policy governing rule around setting up user passwords