**Technology & security modules**

**IAM Section:**

**IAM: Users & Groups**

• IAM = Identity and Access Management, Global service

• Root account created by default, shouldn’t be used or shared

• Users are people within your organization, and can be grouped

• Groups only contain users, not other groups

• Users don’t have to belong to a group, and user can belong to multiple groups

IAM: Permissions

• Users or Groups can be assigned JSON documents called policies

• These policies define the permissions of the users

• In AWS you apply the least privilege principle: don’t give more permissions than a user needs

**IAM – Password Policy**

• Strong passwords = higher security for your account

• In AWS, you can setup a password policy:

• Set a minimum password length

• Require specific character types:

• including uppercase letters

• lowercase letters

• numbers

• non-alphanumeric characters

• Allow all IAM users to change their own passwords

• Require users to change their password after some time (password expiration)

• Prevent password re-use

**Multi Factor Authentication – MFA**

• Users have access to your account and can possibly change configurations or delete resources in your AWS account

• You want to protect your Root Accounts and IAM users

• MFA = password you know + security device you own

• Main benefit of MFA: if a password is stolen or hacked, the account is not compromised

**How can users access AWS ?**

• To access AWS, you have three options:

• AWS Management Console (protected by password + MFA)

• AWS Command Line Interface (CLI): protected by access keys

• AWS Software Developer Kit (SDK) - for code: protected by access keys

• Access Keys are generated through the AWS Console

• Users manage their own access keys

• Access Keys are secret, just like a password. Don’t share them

• Access Key ID ~= username

• Secret Access Key ~= password

**IAM Roles for Services**

• Some AWS service will need to perform actions on your behalf

• To do so, we will assign permissions to AWS services with IAM Roles

• Common roles:

• EC2 Instance Roles

• Lambda Function Roles

• Roles for CloudFormation

**IAM Security Tools**

• IAM Credentials Report (account-level)

• a report that lists all your account's users and the status of their various credentials

• IAM Access Advisor (user-level)

• Access advisor shows the service permissions granted to a user and when those services were last accessed.

• You can use this information to revise your policies.