Task #3 - IAM

What to do

Sub-task 1 – Create 3 User Groups

Let's imagine that we have created AWS Account that will use all members of our AWS program (Coordinator, Mentees, Mentors (Experts)). For all these users it will be better to create different groups with different permissions because, for example: Coordinator has more permissions that Mentee. Please create 3 user groups:

1. CoordinatorsGroup
2. MentorsGroup
3. MenteesGroup

Sub-task 2 – Create policies and roles

1. Create a policy named FullAccessPolicyEC2.
2. Configure the FullAccessPolicyEC2 to allow any actions on the EC2 resources.
3. Similarly, create policies for S3:
   a. FullAccessPolicyS3 – everything's allowed.
   b. ReadAccessPolicyS3 – only get and list actions.
4. Create one role of **EC2 Type** (Trusted Entity) per each policy configured so far (note – these roles won't be used right now, but might be reused in upcoming EC2 module):
   a. FullAccessRoleEC2
   b. FullAccessRoleS3
   c. ReadAccessRoleS3
5. Create one group per each policy configured so far:
   a. FullAccessGroupEC2
   b. FullAccessGroupS3
   c. ReadAccessGroupS3
6. Create 1 user from the 1st group, 1 user from the 2nd group, and 1 user from the 3rd group.
7. Configure named profiles for each user from the previous step to be used with AWS CLI in the subsequent modules. For more info please see https://docs.aws.amazon.com/cli/latest/userguide/cli-configure-profiles.html

What should I remember?

1. **Once you create AWS Account -> Setup Multi-factor Authentication**
2. **Do NOT share your account**
3. **Do NOT commit your account Credentials into the Git**
4. **Terminate/Remove all created resources/services once you finishe Module**
5. **Please Do not forget to delete NAT Gateway if you used it.**
6. **Do NOT keep instance running if you don't use it**
7. **Carefully keep track of billing and working instances so you don't exceed limits**