AWS Cloud Security for Nuvepro

## 1.Secure your Password and Access key & Secret key

The two main types of credentials used for accessing your account are **Password** and **Access key & Secret key**. Both types of credentials can be applied to the root account or to individual IAM users.

You should safeguard passwords and access keys & secret keys as you would any other confidential personal data, and never embed them in **publicly accessible code (i.e. a public Git repository).** For added security, frequently rotate or update all security credentials.

**Note**:

* **Please do not share/upload your access key to anyone or Github/Gitlab/Bitbucket or any other public network with internet access.**
* **Change the Nuvepro dashboard password frequently or After 20 days.**

## 2. Delete the access key once your work is finished.

**Note:**

* **If you use GitHub for document or code versioning and sharing, consider using** [**git-secrets**](https://github.com/awslabs/git-secrets)**, which can scan for AWS credentials and other sensitive information, helping you avoid committing code or documents that contain any sensitive information.**
* **If you suspect that a password or access key pair has been exposed, immediately rotate and delete the exposed credentials.**
* **upGrad will not be liable for any additional charges consumed due to this.In case any such deductions take place due to this, the learner would be required to recharge their credits.**