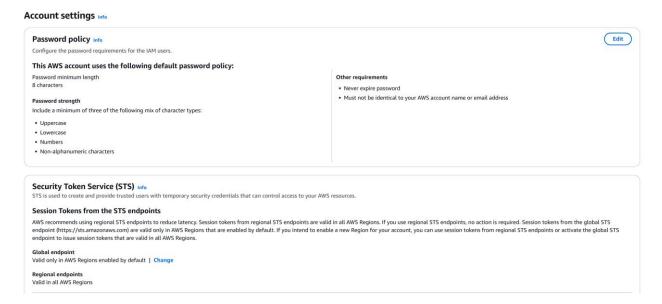




## ACCT-002 - Define identity security best practice on how to access customer environment by leveraging IAM

Depending on the user access permission configuration, we present best practices for maintaining user identity security. We maintain the minimum required roles or permissions, setting temporary credentials where applicable for accessing IAM roles. Each Partner administrator user must have dedicated credentials.

## **Policy**



## **Grant least privileges**

IAM users are defined and classified based on the role or activities they can run in the console for the management and operation of current Infinity Gifts Souvenirs workloads.

This definition is done similarly to the on-premises environment, although the use of IAM policies achieves greater control over the privileges assigned.

Since we manage the environment through terraform, only the user assigned for those purposes has administrative permissions on the account.

In addition to that, the client requested a single user for administrative access, was assigned the minimum permissions allowed, and there was no need to create user groups.

For example, one of the resources assigned to the management of this account only has access to the management of the EC2s within the account.





