AWS IAM Permissions Risk Assessment & Remediation Report

1. **Executive Summary**

StartupCo, a rapidly growing startup, recently launched their first offer, a fitness tracking application. In order to meet launch deadlines they bypassed foundational cloud security practices including, a lack of IAM configuration, no MFA, shared root access and inadequate credential management.

This report identifies key security risks and outlines remediation efforts to bring the company's environment up to industry standards while still supporting future scalability.

2. **Scope**

This assessment focused on StartupCo's primary AWS account used to host their production and development environments. Items in scope:

AWS Root Account – Evaluation of usage practices, access management and credential handling.

IAM Configuration – Review of user and group roles and their associated policies.

Key AWS Services in Use – EC2 instances used to host their application, S3 buckets where customer and application data is stored, RDS instance where user information is stored, and CloudWatch – used for application and infrastructure monitoring.

User Groups Assessed – Developers (4 members), Operations (2 members), Finance (1 member), and Data Analyst (3 members).

This report does not include third-party integrations, CI/CD pipelines, or non-AWS systems unless they directly impact IAM configurations or access controls within the AWS environment.

3. **Findings**

High Risk/Critical	Caution/Moderate	Good/Acceptable
Root account used by everyone	No separate permissions for different teams	CloudWatch in use for monitoring
No MFA or password policy	No dev/ prod seperation	X
AWS credentials shared via teams chat	EC2/S3/RDS usage without security details specified	X

The table above is a traffic light risk assessment used to plainly represent the severity of each vulnerability present in StartupCo's environment. The root account provides a major attack surface, the lack of MFA puts credentials at risk of compromise, and the overly permissive IAM policies go against the principle of least privilege. This lack of policies also represents a lack of configuration concerning AWS services such as S3,

EC2, and RDS. CloudWatch is helpful in providing visibility into these environments and understanding what happened, where, and how.

4. **Remediation Actions**

Mapped out current infrastructure (See Appendix A1: StartupCo Infrastructure)

Secured Root Account – Enabled MFA on root account (See Appendix A2: MFA Configuration), root account now used only for critical administrative tasks.

Created IAM Groups and Users – Created 4 groups; data analyst, finance, developer, and operations. Assigned users to the appropriate group. (See Appendix A8: Users)

Applied Least Privilege Permissions:

- *Developers:* EC2, S3, CloudWatch (See Appendix A3: Developer Permissions)

- Operations: EC2, RDS, SSM, CloudWatch (See Appendix A4: Operations Permissions)

- Finance: Billing and Budgets (See Appendix A5: Finance Permissions)

- Data Analyst: RDS and S3 (See Appendix A6: Data Analyst Permissions)

Implemented Industry Standard Security – Enforced MFA for all IAM users, enabled IAM password policy: minimum 12 characters, complexity (See Appendix A7: Password Policy)

5. **Benefits Impact and Benefits**

Reduced attack surface – Eliminated high-risk practices (shared use of root account, lack of MFA)

Improved compliance – Alignment with ISO 27001, and AWS Well-Architected best practices.

Scalable model – New users can be onboarded securely and consistently due to appropriate group permissions.

6. **Recommendations**

Automate key and password rotation using AWS Secrets Manager.

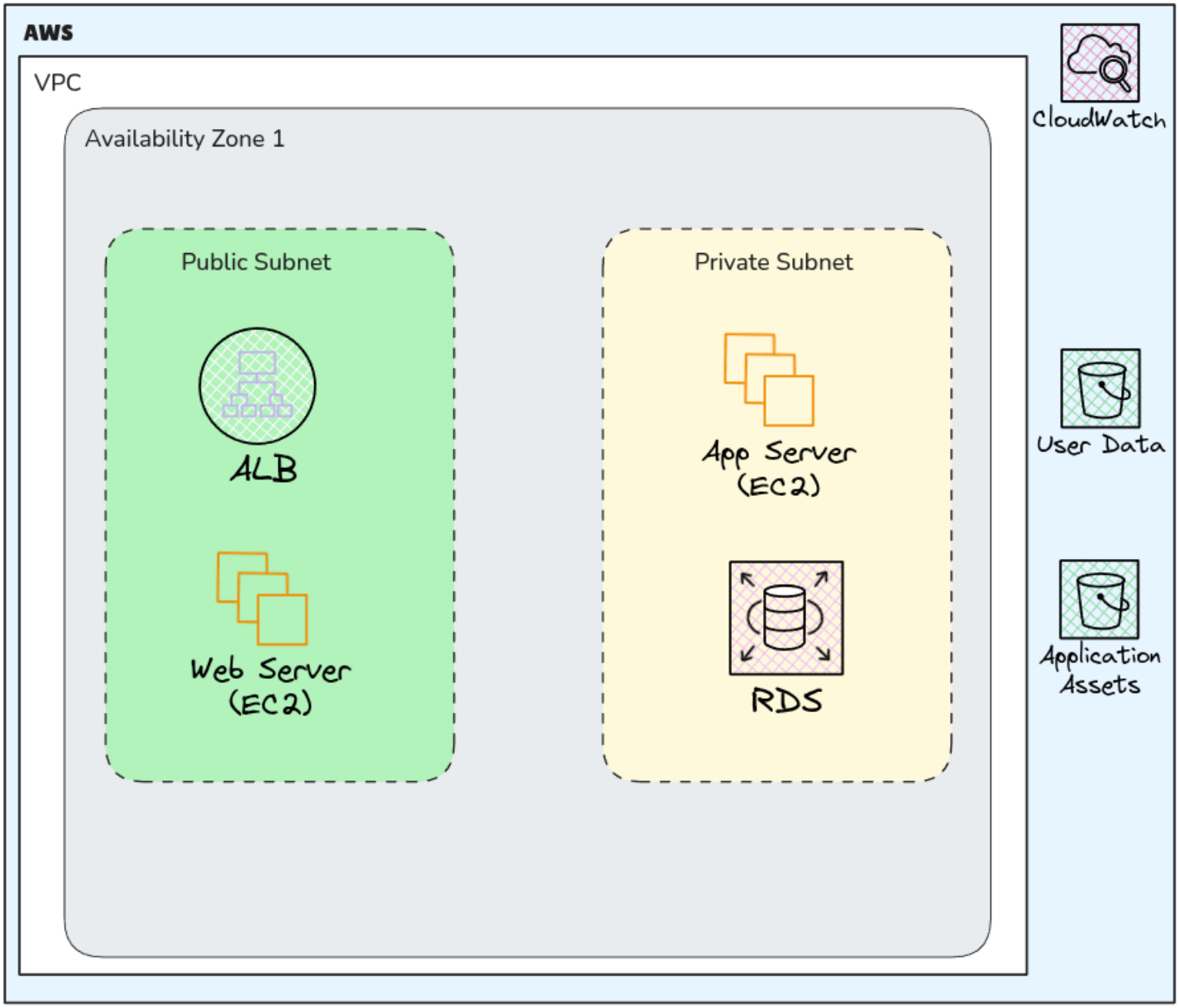
Enable CloudTrail with organization-wide logging for auditing IAM changes.

Regularly review and refine IAM policies based on industry best practices such as those listed in the ISO 27001 and NIST SP 800-63B.

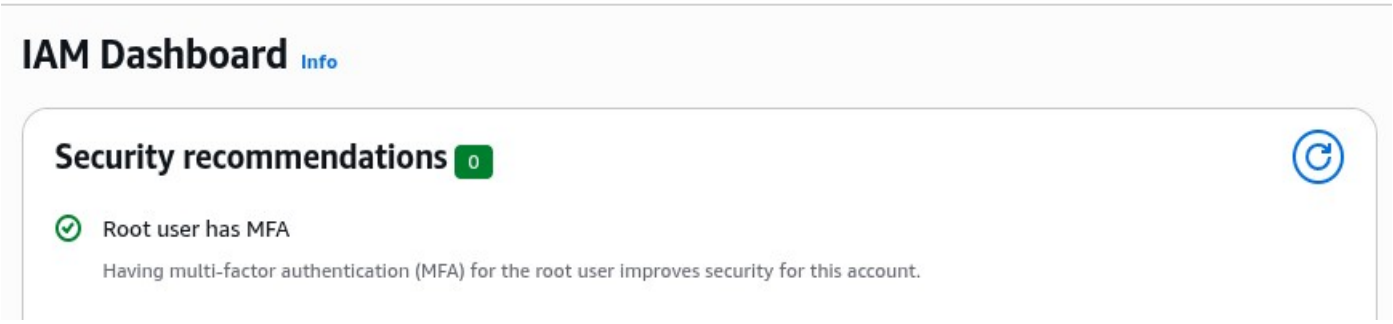
The password policy was configured based off recommendations in NIST SP 800-63B Section 3.1.1.2. All other changes were made to be aligned with the principle of least privilege.

7. **Appendix**

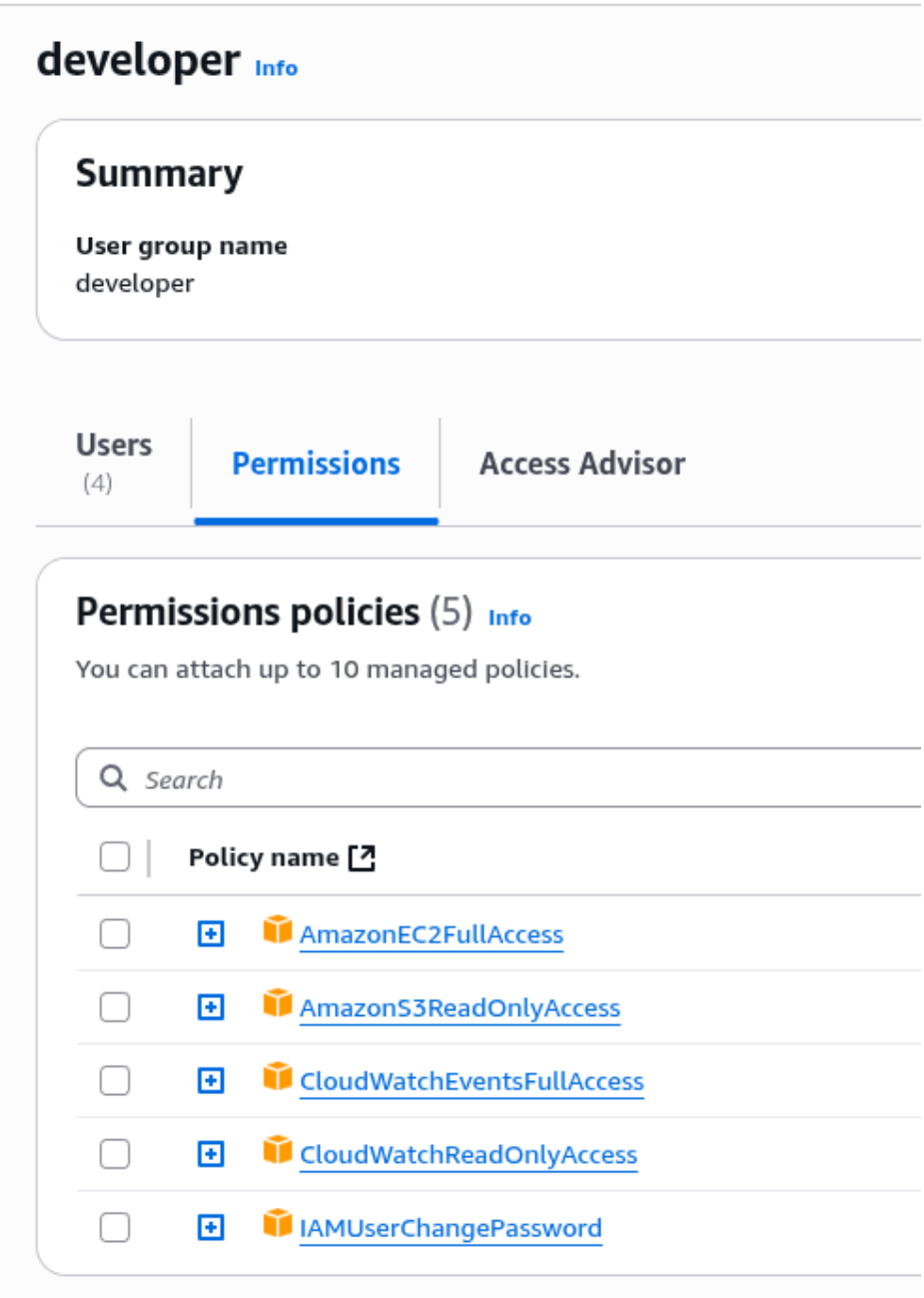
Appendix A1: StartupCo Infrastructure



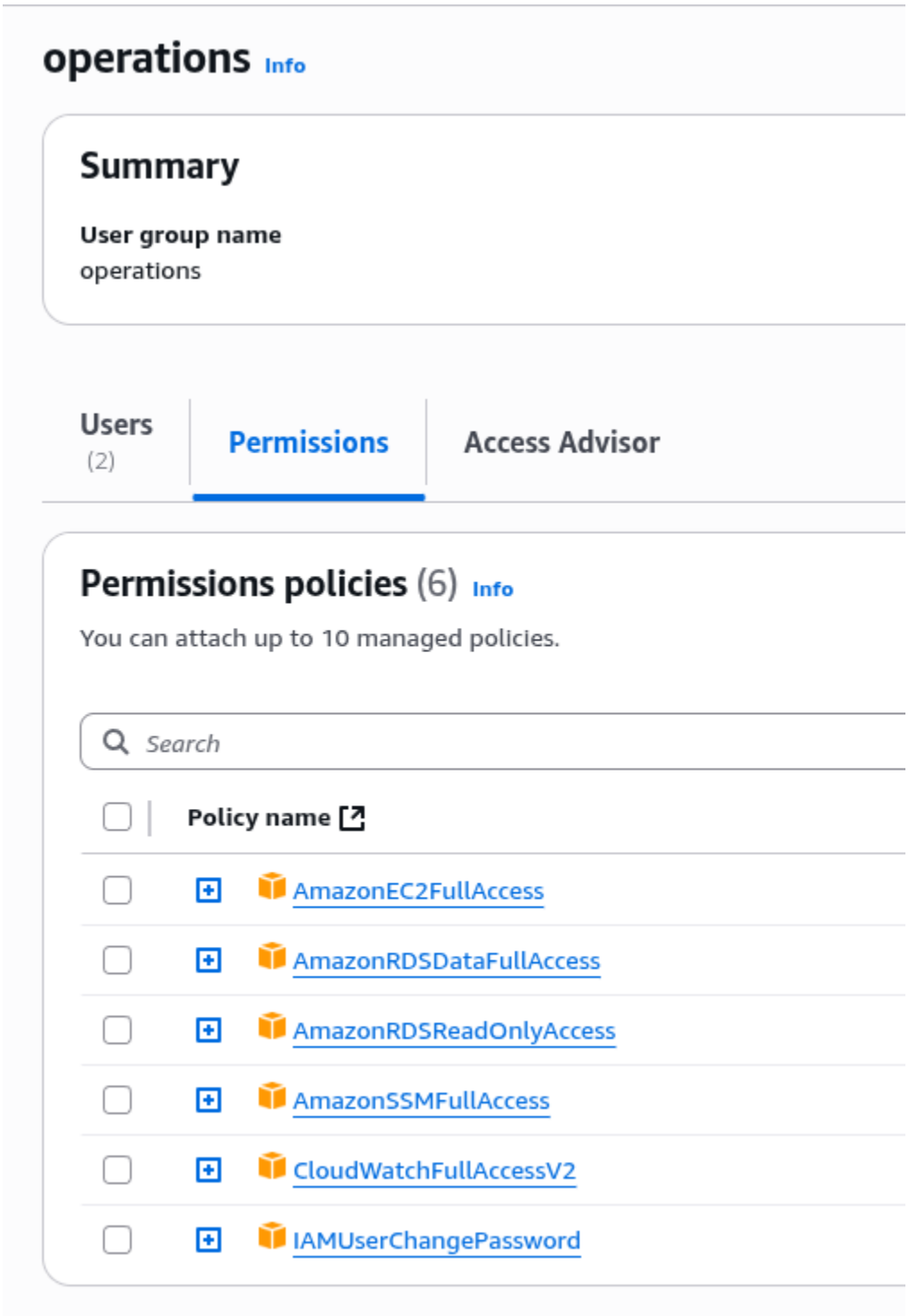
Appendix A2: MFA Configuration



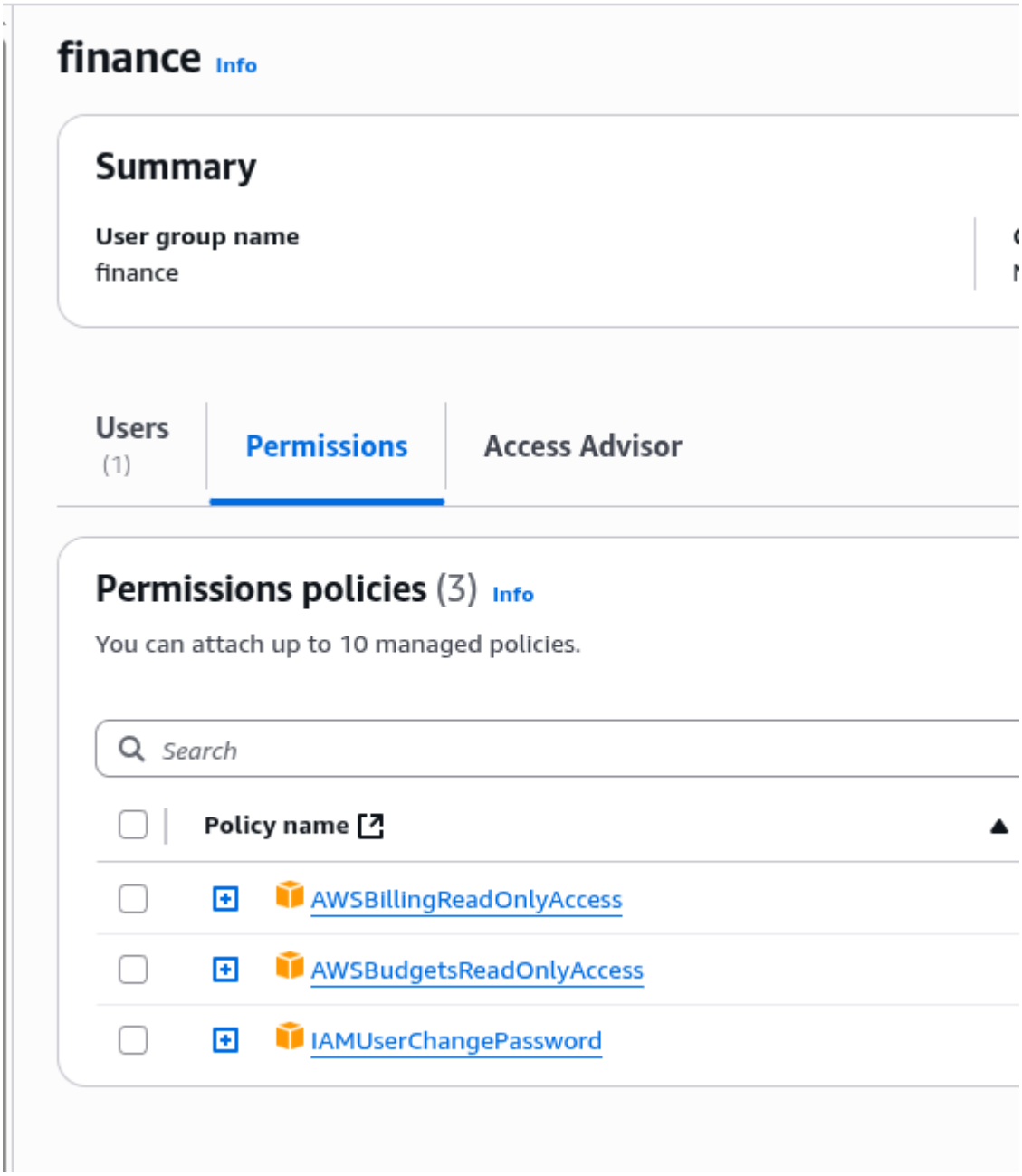
Appendix A3: Developer Permissions



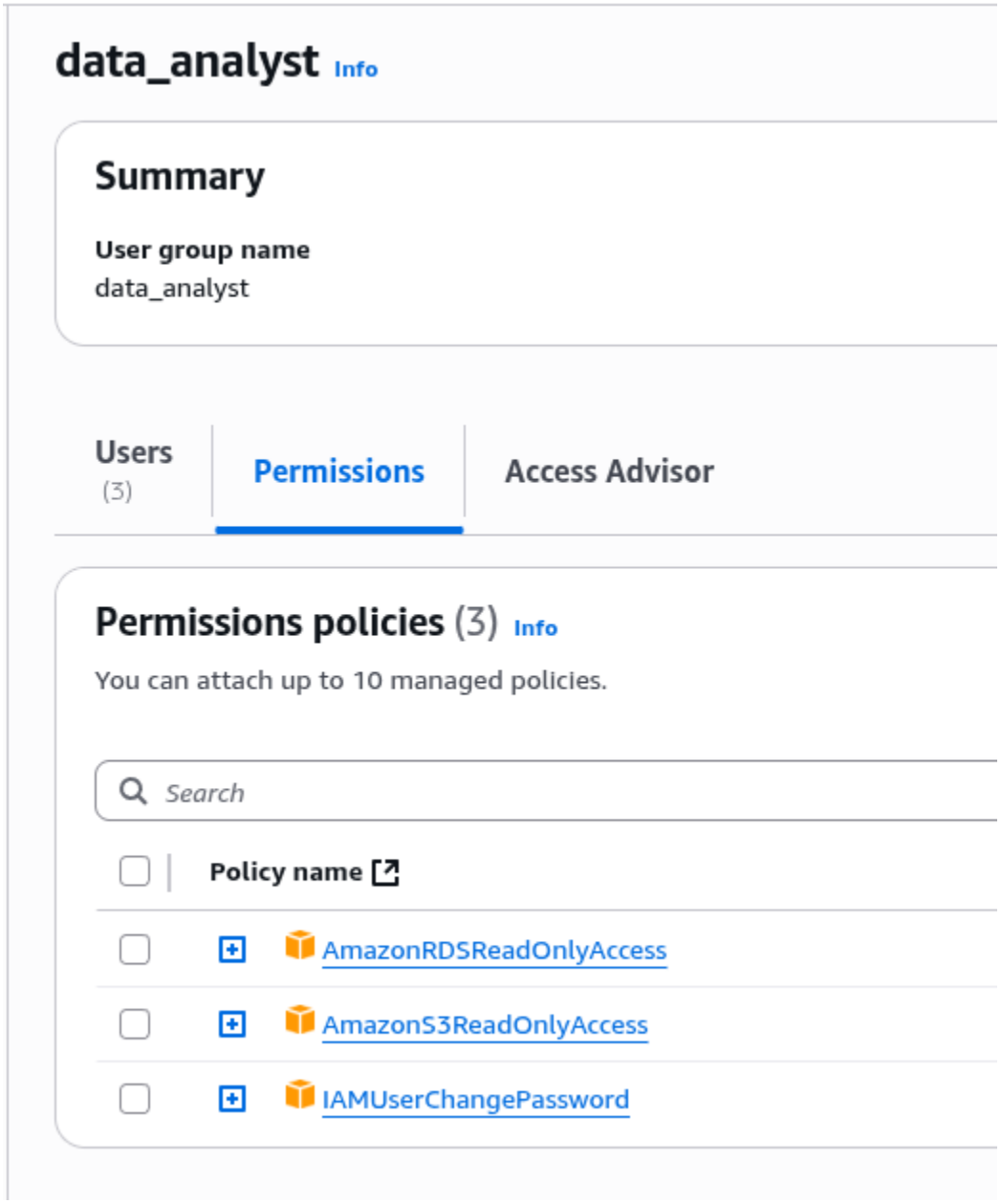
Appendix A4: Operations Permissions



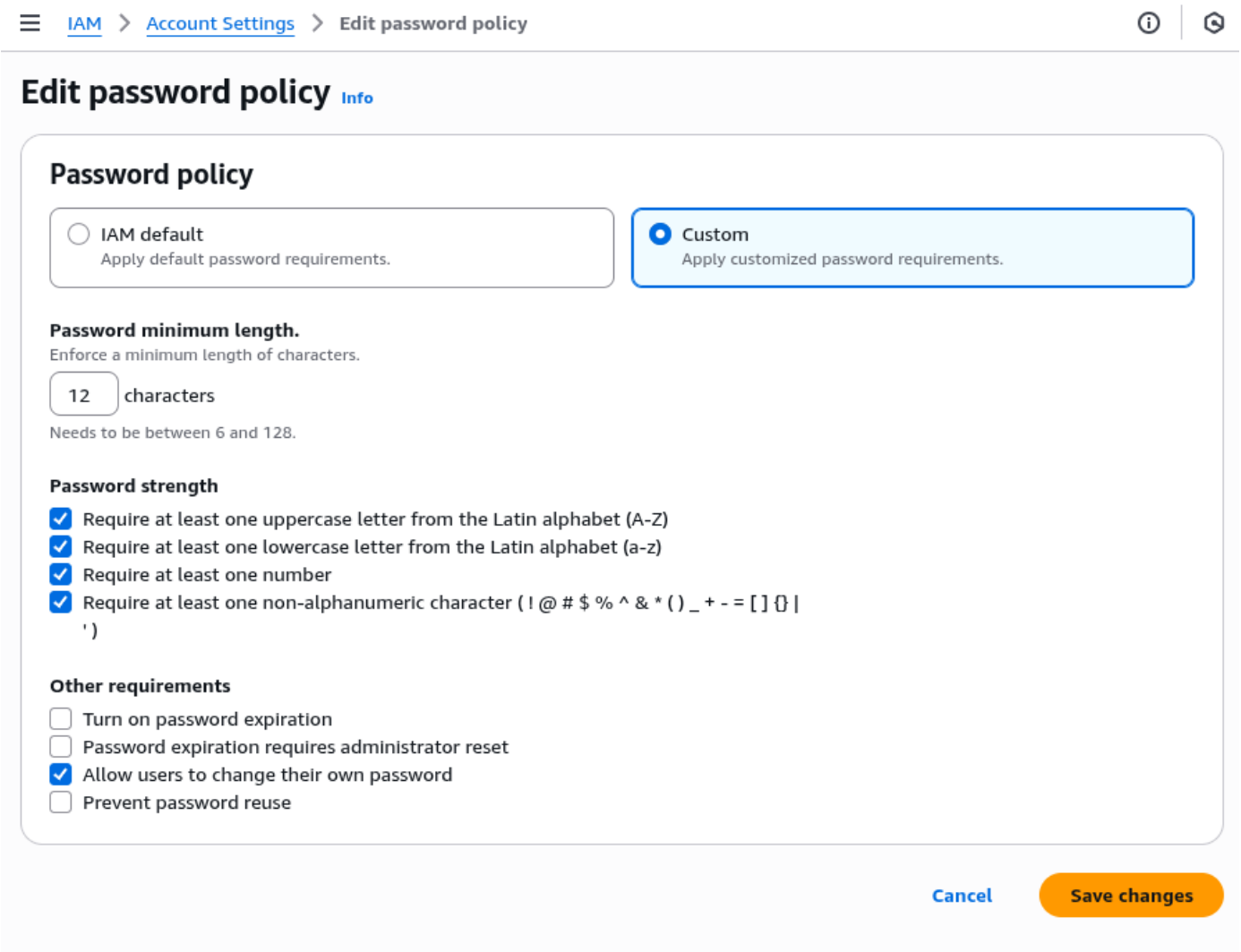
Appendix A5: Finance Permissions



Appendix A6: Data Analyst Permissions



Appendix A7: Password Policy



Appendix A8: Users

☐	harry_analyst	/	1
☐	luke_developer	/	1
☐	mei_operations	/	1
☐	michael_developer	/	1
☐	norman_analyst	/	1
☐	octavius_analyst	/	1
☐	peter_operations	/	1
☐	RogerSterling	/	0
☐	sally_developer	/	1
☐	sylvan_developer	/	1