Homework 1: Designing an IAM Strategy for a Startup

Scenario:

You have just been hired as the first Security Engineer at **"HealthHive,"** a Series B startup building a mobile app for patient data tracking.

- **Workforce:** 50 Full-time employees (Remote), 10 Contractors (Global).
- **Tech Stack:** AWS (Infrastructure), GitHub (Code), Slack/Google Workspace (Productivity), Salesforce (Sales).
- **Constraint:** You handle sensitive medical data (HIPAA compliance required).
- **Current State:** Everyone shares passwords on Slack. There is no MFA.

Objective:

Design an Identity & Access Management (IAM) framework that secures the company without stopping the business from growing. Apply the **Principle of Least Privilege** and **Zero Trust**.

Part 1: Role-Based Access Control (RBAC) Matrix

Task: Identify the three critical user personas below and define their access levels. Do not give anyone "Admin" access unless absolutely necessary.

Persona	Systems Needed	Access Level (Read-Only, Editor, Admin)	Justification (Why?)
Junior Developer	AWS, GitHub, Slack		
Sales Director	Salesforce, Google Drive, Slack		
3rd Party Marketing Contractor	Google Drive, Slack		

Part 2: The Authentication Policy

Task: Define the rules for logging in. You must balance security with user friction.

1. **Password Policy:**
    - *Minimum Length:* _____ characters.
    - *Rotation Policy:* (e.g., Every 90 days? Never? Only on breach?) _____.
2. **Multi-Factor Authentication (MFA):**
    - Which factors will you require? (SMS, Authenticator App, Hardware Key).
    - *Policy for Admins:* _____.
    - *Policy for Contractors:* _____.
3. **Single Sign-On (SSO):**
    - Which application will act as your central "Source of Truth" (Identity Provider)? _____.

Part 3: The "Kill Switch" (Offboarding Protocol)

Task: A disgruntled Developer has been fired effective immediately. They have access to the source code and production database. Create a **5-step checklist** to revoke their access in the correct order to prevent data theft.

1.
2.
3.
4.
5.

Bonus Question: How do you handle a "Break Glass" scenario where the SSO system goes offline? How does the CEO get into their email?