

Terms of Reference of Developing a

Claude AI Deployment

Scope of Work

Claude AI Deployment

Background

Pakistan Microfinance Investment Company Limited (PMIC) intends to introduce secure access to **Claude** to support employee productivity and improve the efficiency of approved business activities. Potential applications include document analysis, report drafting, policy review, summarization, research assistance and technical support.

1. Purpose

PMIC aims to hire a software development firm to develop Web Portal via PMIC staff will access Claude through a private, company-branded chat interface. All processing happens inside PMIC's own **Cloud platform** account and private network. A custom confidentiality filter screens every query before it reaches Claude, blocking anything that contains customer-identifiable or regulated financial data.

The vendor shall evaluate and recommend the most suitable cloud platform for securely integrating Anthropic Claude. The assessment should include AWS Bedrock, Microsoft Azure, Google Cloud, and any other appropriate platform supporting Claude integration.

2. Deliverables

The system has five components, all operating inside PMIC's private **Cloud platform** network:

User Layer: PMIC employees access the assistant via browser through a company-branded internal URL (e.g., ai.pmic.pk).

Interface Layer: Open WebUI a secure, self-hosted chat interface, handles login, chat history, and user management.

Confidentiality Filter: A custom-built screening service checks every query before it reaches Claude, based on rules provided by PMIC (see Section 4 for details).

Network Layer: A Virtual Private Cloud (VPC) with a private endpoint (**Cloud platform**) ensures all traffic stays within **Cloud platform** private backbone, never touching the public internet.

Model Layer: **Cloud platform** Bedrock routes approved requests to Claude (Sonnet 5), with Zero Data Retention enabled so no prompt or response is stored after the request completes.

*Data Flow: User → Open WebUI → Confidentiality Filter (block or allow) → Private Network Endpoint → **Cloud platform** Bedrock → Claude → Response returns via the same private path.*

3 Confidentiality Filter

PMIC will provide a set of rules/policy defining what counts as confidential data. The filter is built around this list:

1. Pattern Matching (default, all cases): Instantly detects structured sensitive data, CNIC numbers, account numbers, phone numbers, and using rule-based scanning. This runs before every request reaches Claude, with no added delay.
2. AI-Based Context Check (only if required): If PMIC's rules include non-pattern-based confidential content e.g., customer names, or specific case details that don't follow a fixed format, a secondary AI-based check will be added. This step adds a small amount of processing time per query, since it runs an extra check before Claude responds.

4.1 Model Configuration at PMIC Premises

Item	Details
Cloud platform Account	Active Cloud platform account under PMIC's ownership and billing.
Domain/Subdomain	A subdomain (e.g., ai.pmic.pk) for internal access.
Confidentiality Rules	A written list of what counts as confidential/regulated data, provided before filter development begins (Section 4.1).

4.2 Cloud Model Configuration at Cloud Model

Item	Details
Cloud platform Architecture	VPC, private network endpoint, security groups, IAM roles.
Bedrock Configuration	Model access, region selection, Zero Data Retention.
Confidentiality Filter	Custom-built screening service based on PMIC's confidentiality rules.
Open WebUI Deployment	Installed, configured, connected, hosted within the VPC.
Branding & Access	Company branding, login setup, user access configuration.
Testing	Functional, security, and load testing.
Documentation	This document plus handover notes for PMIC's IT team.
Go-Live Support	Support through launch and initial stabilization.

4.3 Reports and Dashboard

The solution shall provide:

- User activity and audit reports.
- User wise usage Claude activity
- User wise Input and output token

5. Technical Aspects

The solution shall:

- Solution will give access to Full Claude functionality like project, agent etc
- Solution should be SECP compliance
- Maintain detailed system, transaction, and user audit logs.
- Support data backup, restoration, and disaster recovery.
- Cybersecurity

6. Testing and Acceptance

The service provider shall conduct:

- Unit testing.
- System and integration testing.
- Security and vulnerability testing.
- Performance testing.
- User Acceptance Testing.

7. Additional Documents/Reports Required

The service provider shall deliver:

1. Business Requirements Document.
2. Functional and technical design documents.
3. Deployment and configuration documents.
4. User, administrator, and technical manuals.
5. Training for business, risk, and IT users.

8. Support

The service provider shall provide an agreed warranty period after go-live, including:

- Correction of application defects.
- Technical and operational support.
- Performance monitoring and optimization.
- Knowledge transfer to PMIC's IT team.

9. Duration

The service provider will be required to complete the assignment in max 3 months after awarding.

10. Qualification and experience of firm

The firm with the following qualifications is invited to design the Claude AI interface

1. A software house/firm which has expertise in designing Cloud based managed server, AI, Front end application development
2. At least 5 Years of experience in software development.
3. Demonstrate a strong understanding of AI, Claude Integration, Cloud managed services configuration