



CREDITACCESS GRAMEEN LIMITED

Artificial Intelligence Governance Policy
Published in Public Domain

Extracted from: Artificial Intelligence Governance Policy, Version 1.0

1.0

Classification: *Public*

Purpose of this Document

This document extracts the clauses from CreditAccess Grameen Limited's Artificial Intelligence Governance Policy (Version 1.0) that are recommended for publication in the public domain. Internal governance, committee composition, vendor/LLM details, and risk-register content have been excluded as they are for internal use only. All extracted text below is reproduced verbatim, without modification, from the original policy document.

Reference Table

Clause No.	Clause Title	Page in Original Policy
1	Introduction	4
2	Working Definition	4
3	Scope	4
4	Out of Scope	5
6	Guiding Principles	5
6.1	Encourage Responsible AI Innovation	5
6.2	Ensure Regulatory Compliance and Risk Management	5
6.3	Build Sustainable AI Infrastructure and Talent	6
6.4	Ensure Ethical AI, Fairness, and Transparency	6
6.5	Strengthening Customer Trust and Protection	6
12	Data Security and Privacy Guidelines	13
13	Regulatory and Legal Compliance	13
13.1	Data Privacy and Protection	14
13.2	Data Management	14
13.3	Authentication & Access Control	14
13.4	Fairness, Explainability, and Non-Discrimination	14
13.5	Compliance Audit and Reporting	14

Extracted Clauses

1. Introduction

Adopting AI technologies has become critical in today's rapidly evolving business environment, as it enables organizations to make faster, data-driven decisions and respond dynamically to market changes. It is well understood that AI enhances operational efficiency, customer experience, and risk management, particularly in data-intensive sectors. Organizations that leverage AI effectively can unlock new revenue opportunities and gain a sustainable competitive advantage, while those that delay adoption risk falling behind. Increasingly, AI is not just an innovation lever, but a core capability for long-term business resilience and growth. AI use cases can be explored across various functions of the company leading to efficiency/cost saving, better customer service, credit cost control or improved revenue generation.

While the importance of AI technology is well understood, the policy framed stresses the balance between innovation and overriding importance of ethics, regulation and customer trust on today's fast evolving digital ecosystem.

This policy establishes the governance framework, risk management standards, and operational guidelines for the use of Artificial Intelligence (AI) across the organization. As a mid-size Non-Banking Finance Corporation

(NBFC) operating in the Indian financial services sector, CreditAccess Grameen recognizes both the transformative potential and inherent risks associated with AI technologies.

The purpose of this policy is to:

- Define a clear and practical working definition of AI applicable to the organization.
- Classify AI integrated applications by type and risk profile.
- Establish governance mechanisms to ensure responsible safe, ethical, and compliant AI systems.
- Define roles and responsibilities across technology, risk, and business functions.
- Ensure compliance with applicable regulatory guidelines including RBI directions on IT governance and outsourcing.

2. Working Definition

For the purposes of this policy, Artificial Intelligence (AI) refers to systems that use large language models (LLMs) and generative AI technologies to generate, summarize, analyze, or act upon text, code, data, or business processes.

3. Scope

This policy applies to all CAGL employees, contractors, vendors, and third-party service providers involved in the design, development, deployment, management, or use of AI systems and platforms across all business units at CreditAccess Grameen Ltd.

4. Out of Scope

This policy does not cover traditional rule-based automation (RPA), statistical models (scorecard, regression), or deterministic algorithms that do not involve generative AI or LLM-based components.

6. Guiding Principles

This section lists the overarching aims of this policy which includes responsible innovation, inclusion, compliance, risk reduction and sustained capability to serve as foundational principles of all subsequent guidelines

6.1 Encourage Responsible AI Innovation

AI must be explored actively which can contribute to enhanced productivity, improved process enhancement, innovation in product design & risk management and reduced time to market.

6.2 Ensure Regulatory Compliance and Risk Management

AI must be designed / used with appropriate risk management in place.

- There shall be appropriate safety guidelines for day-to-day productivity related use
- Appropriate data security measures shall be adopted while using AI
- Black-box AI models (i.e. explainability is non-existent or weak) may not be used for credit decisions. Overrides (human-in-the-loop) are required where explainability is weak.
- Cyber-resilience controls are regularly penetration-tested in AI-enabled applications.

- Vendor due diligence for AI SaaS providers; all must comply with Indian data localization laws
- Company shall adhere to all applicable regulations while using AI

6.3 Build Sustainable AI Infrastructure and Talent

Long-term AI success depends on reliable technology, robust processes, and internal expertise.

CA Grameen may

- Investment in infrastructure either in public cloud or on-prem
- Build AI talent in-house or through partnership
- AI assets must be treated with the same accountability as IT assets, with clear ownership, documentation and visibility before deployment

6.4 Ensure Ethical AI, Fairness, and Transparency

The company shall strive to design AI with safeguards against bias and discrimination to the extent possible. Regular model audits to identify unintended discriminatory outcomes (e.g., gender, geography, ethnicity) shall be carried out for the same.

- Red teaming to test for manipulation or bias in high-stakes models
- Engagement with external reviewers for fairness checks

6.5 Strengthening Customer Trust and Protection

All AI-powered functions shall also consider building customer trust as an important consideration

- Mechanisms for customers to escalate queries about AI-generated outcomes
- Options for a human override where required
- "AI used here" badges or notices in digital channels where feasible

12. Data Security and Privacy Guidelines

The CISO shall issue periodic safety guideline with respect to AI usage. It would also be the responsibility of CISO to monitor adherence to the guideline and report any deviation to CRO.

13. Regulatory and Legal Compliance

This section ensures the policy aligns with prevailing and forthcoming Indian data, digital, and AI regulatory frameworks.

13.1 Data Privacy and Protection

- All the AI Implementations shall follow the stipulated Information Security guidelines of the organization, as applicable.

13.2 Data Management

- Data must reside within authorized geographic locations per regulatory and corporate requirements
- Cloud and on-premises environments must enforce controls to prevent unauthorized data access

13.3 Authentication & Access Control

- Role-based access control (RBAC) must be enforced for all AI/ML development, deployment, and operational environments
- Access logs must be maintained and regularly audited

13.4 Fairness, Explainability, and Non-Discrimination

- AI critical models (e.g., credit scoring, claim denials, fraud alerts) shall be tested for fairness using outcome analysis
- Audit trails maintained for decision-making logic and results

13.5 Compliance Audit and Reporting

- Periodic audits of Critical Type 2 AI systems shall be conducted by Internal Audit as part of the independent assurance framework, while ongoing compliance monitoring and reporting shall be the responsibility of respective business and control functions. Incident and exception reports for all AI failures, adverse impacts, or customer grievances

Note: This is an extract derived from CreditAccess Grameen Limited's board approved Artificial Intelligence Governance Policy, Version 1.0 (Classification: Internal use only). Only the clauses listed in the Reference Table above have been reproduced here for public disclosure; all other sections of the original policy remain internal.