केन्द्रीय कार्यालय
बालुवाटार, काठमाडौं
फोन नं. : ०१-५७१९६४१/४२/४३/४४
Website : www.nrb.org.np
पोष्ट बक्स : ७३

नेपाल राष्ट्र बैंक

बैंक तथा वित्तीय संस्था नियमन विभाग

पत्र संख्या : बै.वि.नि.वि./नीति/सूचना/१३/०८२/८३

मिति : २०८२/०८/२१

सूचना

सम्पूर्ण सरोकारवाला व्यक्ति तथा निकायहरु

विषयः राय/सुझाव उपलब्ध गराउने सम्बन्धमा ।

यस बैंकबाट तयार गरिएको **"Artificial Intelligence Guidelines"** मार्गदर्शन बैंकको वेवसाइट www.nrb.org.np/category/notices/ मा राखिएको व्यहोरा अनुरोध छ । उक्त मार्गदर्शन उपर कुनै राय/सुझाव भएमा २०८२ पुस १५ भित्र यस बैंकमा लिखित रुपमा अथवा इमेल मार्फत् **nrbbfirdppd@nrb.org.np** मा उपलब्ध गराइदिनुहुन अनुरोध छ ।

भवदीय,

२०८२/०८/२१

कार्यकारी निर्देशक

ARTIFICIAL INTELLIGENCE GUIDELINES

NEPAL RASTRA BANK

BANKS & FINANCIAL INSTITUTIONS

REGULATION DEPARTMENT

December, 2025

Contents

1. Definition & Acronyms

S.No.	Title	Description
1	Artificial Intelligence (AI)	The application of intelligent technologies and algorithms to perform tasks that typically require human intelligence. By analyzing data and recognizing patterns, AI enhances decision-making, improves operational efficiency, strengthens risk management and enhances overall user experience.
2	AI Model	A trained algorithm that analyzes data and recognizes patterns to perform specific intelligent tasks, enabling decision-making and problem-solving.
3	AI System	A complete solution that integrates one or more AI models with software and hardware components to perform intelligent tasks, improve operations and support decision-making.
4	AIG	Artificial Intelligence Guidelines
5	Algorithm	It is a set instructions or rules that enables a computer to learn from data, identify patterns and make decisions or predictions, forming the core logic behind AI models.
6	High-Risk	AI Systems that pose serious threats due to their potential to cause financial harm, operate with minimal oversight, and impact fundamental rights.
7	Human Oversight	The involvement of human judgment and intervention in the development, deployment and operation of artificial intelligence systems to ensure their decisions and actions are accurate, ethical and aligned with legal and societal standards.
8	LI(s)	Licensed Institution(s) by Nepal Rastra Bank
9	Life Cycle	It is the series of stages from defining the problem, collecting and preparing data, developing and testing the model, deploying it, monitoring performance, and continuously improving or retiring the system.
10	NRB	Nepal Rastra Bank
11	PSOs	Payment System Operators
12	PSPs	Payment Service Providers

2. Background

Artificial Intelligence (AI) is advancing at a remarkable pace, creating new possibilities while also introducing a range of risks and challenges for the financial sector. Given its potential to reshape the way financial institutions operate, Nepal Rastra Bank (NRB) has recognized the importance of providing clear direction on its use. These guidelines are intended to guide NRB-licensed institutions (LIs) in Nepal towards the responsible, transparent and ethical use of AI. The objective is to enable financial institutions to leverage the benefits of AI while safeguarding fairness, accountability, and stability within the financial system.

Nepal Rastra Bank has issued this Artificial Intelligence Guidelines following the announcement of Monetary Policy for fiscal year 2024/25. These guidelines follow international best practices and is tailored to the specific context of Nepal's financial system.

3. Objectives

These guidelines designed for NRB regulated LIs aim to:

3.1. Promote the adoption of AI technologies in a manner that enhances efficiency, innovation and customer experience while ensuring financial stability, integrity and operational resilience.

3.2. Ensure that AI applications in LIs are transparent, explainable, fair, and accountable, and that they uphold customer rights, protect data privacy, and do not result in discriminatory or unethical outcomes.

3.3. Mitigate risks associated with AI, including operational**,** ethical, systemic, model and cyber risks and ensure that LIs have adequate governance structures in place to manage these risks.

3.4. Foster a competitive and inclusive financial sector that leverages AI to provide accessible and affordable financial services to all segments of the population.

4. Scope

4.1. These guidelines are applicable to the institutions licensed by Nepal Rastra Bank, namely Commercial Banks (Class A), Development Banks (Class B), Finance Companies (Class C), Microfinance Institutions (Class D), Nepal Infrastructure Bank Limited, as well as Payment System Operators (PSOs) and Payment Service Providers (PSPs).

4.2. The guidelines cover the use of AI in various applications, including but not limited to credit scoring, fraud detection, customer service, risk management, and compliance monitoring.

5. Governance and Accountability

5.1 Board and Senior management oversight

The board of directors and senior management of LIs remain ultimately accountable for the outcomes and decisions generated by the institution's AI systems.

5.1.1. *Key responsibilities of board include but are not limited to:*

- Defines the LIs' AI-related risk tolerance within the overall risk management framework and sets the strategic direction for AI adoption and use.
- Establishes robust governance structures, including clear roles and responsibilities, to ensure effective oversight of AI systems.
- Ensures the implementation of ethical, transparent, and risk-aware practices for AI deployment through appropriate policies and frameworks.

5.1.2. Key responsibilities of senior management include but are not limited to:

- Ensures AI usage aligns with the institution's risk appetite, regulatory requirements and strategic goals, while also assessing, understanding, and continuously monitoring the institution's dependence on AI systems.
- Oversees the implementation and daily operation of AI systems within risk and compliance frameworks, including mechanisms for human oversight, auditability and remediation.

5.2. AI strategy & governance structure

5.2.1. *AI strategy & governance framework:* LIs should establish a comprehensive AI governance framework integrated with their overall risk management system. Guided by a clear AI strategy, the framework should define institutional objectives and ensure the secure development, deployment and use of AI technologies. It must include well-defined policies, procedures, and controls to manage AI-related risks, while also supporting business continuity, operational resilience, and regulatory compliance. The framework should ensure that AI systems are resilient enough to keep critical services running during disruptions, with well-defined measures in place to quickly detect issues, restore normal operations, and minimize the impact of failures.

5.2.2. *AI Governance Structure:* LIs should establish a cross-disciplinary AI steering committee, or assign this responsibility to an existing committee, comprising senior management and relevant staff from key units (e.g., business, risk, IT, legal, audit, HR). The committee should guide the development of an AI strategy and governance framework that addresses all aspects of people, processes, and technology. The AI strategy and governance framework must be approved by the LIs board. Senior management should include one or more members with sufficient expertise to oversee technology-related risks, particularly those associated with AI.

5.3. Outsourcing*:*

- **Internal Use of Third-Party AI:** LIs may use AI tools or ready-made models from third parties for internal purposes, such as drafting documents, creating summaries, or analyzing and processing information. This use will not be considered outsourcing, as the work remains within the institution. In such cases, the LIs' own governance, risk management and compliance policies apply, and these policies must be aligned with national regulations and regulatory requirements.
- **Outsourced AI Services:** When a LI outsources a service to a third-party provider that uses AI to deliver that service, it is considered outsourcing. In such cases, LIs must take appropriate steps to manage the associated risks and ensure regulatory compliance. This includes conducting thorough due diligence to confirm that the AI solution meets all regulatory requirements and that any risks are kept within acceptable limits. Contracts with the third-party provider should clearly address data security, compliance and

auditability. Additionally, LIs must obtain formal approval from their Board of Directors before outsourcing and notify the concerned supervision department of NRB.

6. Risk Management

6.1. Risk Identification and Assessment:

6.1.1. LIs are required to conduct an initial assessment of AI-enabled systems prior to their deployment or market launch to determine if they meet the criteria for classification as high-risk or not high-risk. For systems identified as high-risk, LIs should allocate sufficient resources to ensure comprehensive and effective risk management. The following criteria should be considered when identifying high-risk AI systems:

a) **Serious Harm**: The system has the potential to cause significant financial loss, legal liabilities, or denial of essential services.
b) **Broad Impact:** The system is deployed at large scale, increasing the possibility of systemic risk across institutions or sectors.
c) **Minimal Human Oversight:** The system functions with limited human supervision, increasing the likelihood of unchecked errors or misuse.
d) **Rights Risk:** The system poses risk to individual rights, including privacy, fairness, non-discrimination, and equality.
e) **Sensitive Data Use:** The system processes highly sensitive data, such as biometric information or large personal and financial datasets.

6.1.2. AI-related risk management should be embedded within the institution's existing risk management and internal control frameworks. LIs are required to identify and assess the risks associated with AI applications, including operational, data privacy, model, and reputational risks. All AI-related risks must be clearly documented in a dedicated section of the institution's risk register, with defined risk owners, mitigation measures, and monitoring mechanisms. Risk assessments should be conducted regularly and updated as necessary. LIs should also assess and mitigate risks from AI-generated synthetic media (e.g., deepfakes), including deploying detection tools and educating customers and other relevant stakeholders.

6.2. Model Risk Management: AI models used in decision-making processes are required to be rigorously tested and validated to ensure accuracy, reliability, and fairness. LIs should establish model risk management practices that include model development, validation, monitoring, decommissioning and unbiased algorithms throughout their entire life-cycle.

6.3. Data Quality and Integrity: AI systems rely heavily on data and LIs should ensure that the data used is accurate, complete and up-to-date. LIs should establish robust data governance policies to ensure data quality, integrity, and accountability throughout the AI lifecycle. This includes formulating a formal data retention policy that defines the collection, storage, usage, and disposal of data used in AI systems-such as training data, outputs, audit trails, and model documentation.

6.4. Cyber security: AI systems are required to be protected against cyber threats, including data breaches, hacking and other forms of cyber-attacks. LIs are required to implement robust cybersecurity measures, conduct regular security audits and ensure compliance with NRB's Cyber Resilience Guidelines. Additionally, measures such as regular penetration testing and AI-specific threat modeling should be adopted to strengthen security.

6.5. Ethical AI Use: LIs should ensure that AI systems are designed and operated in an ethical manner, with due consideration for fairness, transparency, and accountability. This includes avoiding biases in AI algorithms and ensuring that AI decisions do not discriminate against any individual or group.

7. Transparency and Explainability

7.1. *Explainable AI:* LIs should ensure that AI systems are transparent and that their decision-making processes can be explained in a manner that is understandable to stakeholders, customers, regulators, and auditors. AI-generated content must be clearly labeled.

7.2. *Customer Communication:* Customers are required to be informed whenever AI systems are used in decision-making processes that affect them. LIs should provide accessible explanations of how AI decisions are made and the factors influencing those decisions. Additionally, LIs must disclose AI usage during customer interactions.

7.3. *Audit Trails:* LIs are expected to maintain comprehensive audit logs of AI decision-making processes to ensure accountability and facilitate regulatory oversight. It is recommended that

these records align with international benchmarks, such as ISO/IEC 42001 (AI Management Systems), to support transparency, fairness, and responsible governance. Audit trails must be retained for the duration specified by NRB and provided upon request.

8. Data Privacy and Protection

8.1. Compliance with Data Protection Laws: LIs are required to comply with all applicable data protection laws and regulations, including the *Privacy Act, 2075 (2018).* AI systems are required to be designed to protect customer data and ensure privacy.

8.2. Data Minimization: LIs should adopt a data minimization approach, collecting only the data necessary for the intended AI application and retaining it only for as long as required.

*8.3. Consent and Opt-Ou*t: LIs are required to obtain explicit consent from customers before using their data in AI systems. Customers must also be provided with a clear option to opt out at any time, without it resulting in the denial of essential services.

9. Fairness and Non-Discrimination

9.1. Bias Mitigation: LIs should take proactive measures to identify and mitigate biases in AI algorithms that could lead to unfair or discriminatory outcomes. This includes regular testing and monitoring of AI systems for bias. For high-risk AI systems, it is recommended to have independent third-party validation of outcomes to ensure that decisions are fair, accurate and comply with applicable standards and regulatory requirements.

9.2. Inclusive AI: AI systems should be designed to serve all segments of the population, including marginalized and underserved groups. LIs should ensure that AI applications do not exacerbate financial exclusion or inequality.

10. Monitoring and Reporting

10.1. Regular Monitoring: LIs are required to continuously monitor the performance and impact of AI systems to ensure they operate as intended and do not pose undue risks. Monitoring should include both technical performance and customer outcomes. LIs should prepare AI system monitoring reports following a risk-based schedule.

High-risk AI systems should be monitored more frequently, while other systems must undergo regular reviews. LIs are required to develop dedicated monitoring plans to ensure effective oversight of high-risk AI systems. Additionally, LIs must conduct re-assessments of AI systems to identify and address new risks, particularly when there are significant changes in the system's functionality, operations or in the regulatory or technological environment.

10.2. Incident Reporting: LIs are required to report all AI-related incidents—whether critical or non-critical to the concerned supervision department of NRB in accordance with the IT Guidelines, 2012 and Cyber Resilience Guidelines, 2023. Critical incidents include major system failures, data breaches, or significant algorithmic bias that could harm customers or disrupt essential services. Non-critical incidents, including minor model errors or technical issues with minimal impact, must be documented internally and LIs should report them on a quarterly basis to NRB. Incident reports should clearly outline the nature of the event, its potential or actual impact on operations, customers, or data security, and the corrective measures taken to address the issue and prevent future occurrences.

10.3. Regulatory Reporting:

- LIs are required to submit annual reports to the concerned supervision department of NRB, outlining their AI activities, including the types of AI systems in use, their applications, risk management measures, and customer outcomes. These reports must be prepared using the standardized template provided by NRB (Annex A).
- LIs should maintain comprehensive documentation of AI systems, particularly those identified as high-risk, including details on data sources, algorithms, and decision-making processes. For AI systems not classified as high-risk, LIs must prepare a clear justification supporting this classification, which should be properly maintained and made readily available to regulatory authorities upon request.

11. Capacity Building

LIs should provide adequate training programs to keep their board members, senior management and other employees informed about the risks associated with using AI, the emerging technologies, and evolving regulations in the field of AI. This training should

cover everyone involved in overseeing, designing, developing, deploying or managing AI systems within the institution.

12. Customer Awareness and Grievance Handling

- LIs should take reasonable steps to educate customers about how AI is used in their products and services, as well as how it may influence decisions that affect them.
- LIs should establish or adapt their existing grievance mechanisms to properly handle complaints related to AI-driven decisions. LIs should also ensure that customers clearly understand how to raise concerns if they believe an AI-based decision has negatively affected them.

13. Compliance

In compliance with these guidelines, LIs must also adhere to the following secondary regulations, including any subsequent amendments:

a. Cyber Resilience Guidelines, 2023

b. IT Guidelines, 2012

c. The Privacy Act, 2075(2018)

d. Other relevant laws or regulations issued by the regulatory or governing bodies

Annex A: Reporting on Artificial Intelligence Activities

a) Reporting Period: [Insert Start Date] to [Insert End Date]
b) Reporting Entity (LIs Name): [Insert Name]
c) Submission Date: 2025-XX-XX

Section 1: Overview of AI Systems in Use

S.N.	AI System Name/ID	Type of AI Technology	Purpose / Use Case	Deployment Stage (Pilot/Live)	Developed In-house / Vendor	Date of Deployment
1						
2						
3						

Section 2: Application Details

a) Functionality and Application Area:
b) Target Segment (if any):
c) Benefits Achieved:

Section 3: Risk Management Measures

S.N.	AI System Name	Data Privacy Measures	Bias Monitoring	Model Validation	Explainability	Human Oversight	Other Controls
1							
2							
3							

Section 4: Governance & Compliance

a) AI Governance Framework in Place? (Yes/No):
b) Brief Description of AI Governance Structure:
c) Cybersecurity Measures in Place:
d) Compliance with NRB Guidelines:
e) AI-Related Training and Awareness Programs Conducted (Yes/No)
   If Yes, specify frequency,
   i. Target audience:
   ii. Last training date:

Section 5: Performance and Incidents

a) Performance Metrics Tracked:
b) Notable Outcomes:
c) Incidents/Concerns Identified:

Section 6: Future AI Initiatives

S.No	Planned Initiative	Expected Use Case	Timeline	Partner/Vendor (if any)	Remarks
1					
2					

Authorized Signatory:

Name:

Designation:

Contact:

Date: