Reference Material

CORPORATE AI USAGE, GOVERNANCE & RESPONSIBLE AI HANDBOOK

Authored By: AMEET B. NAIK & SAAKAR S. YADAV

Lexlegis.ai
YOUR TRUSTED LEGAL AID

Digital Publication – No Physical Print Copies

DOCUMENT INFORMATION

Version: 1.0
Document Type: Corporate AI Governance & Responsible AI Handbook
Prepared By: Ameet Naik and Saakar S. Yadav
Reviewed & Compiled By: LexLegis.ai (Reference & Guidance Material)
Date of Issue: 13th November 2025
Supersedes: All previous versions of the AI Policy & Governance Framework
Intended Audience: All employees, contractors, partners, and Corporate users
Document Status: Active – Under Continuous Review
Confidentiality Classification: Public Use – General Circulation
Distribution Permission: May be shared, distributed, and referenced openly.

DISCLAIMER:

This document has been prepared by LexLegis solely for reference and guidance purposes. It is intended to provide general information on corporate Artificial Intelligence governance and responsible usage practices. While every effort has been taken to compile accurate, relevant, and up-to-date content, inadvertent errors or omissions may have occurred. LexLegis does not assume any responsibility or liability for such inaccuracies or for any consequences arising from the use, reliance, or interpretation of this material.

This document is not legal advice, nor is it a substitute for professional consultation, statutory interpretation, or organization-specific policy decisions. Users are advised to evaluate the content in the context of their own operational, legal, and regulatory frameworks. LexLegis shall not be held responsible for any loss, damage, or adverse outcome resulting from the direct or indirect application of this document.

Use of this material is entirely at the discretion of the reader, who bears full responsibility for ensuring compliance with applicable laws, internal governance standards, and organizational protocols.

ABOUT THE AUTHORS

Ameet B. Naik is the founding partner at Naik Naik & Co. and with over three decades of experience in the field of law. He carries several important reported judgments and landmark decisions to his credit.

Ameet has spear-headed the legal recourse in a number of matters and has built a distinguished career in dispute resolution, white-collar crime, corporate commercial disputes, international arbitration, insolvency law, intellectual property, and corporate and commercial practice, with recognized expertise in handling complex commercial arbitral proceedings. He continues to maintain a dominant position as an accomplished litigator across various sectors and has been at the fore-front of several high stake litigations. He is at the forefront of the country's top disputes in the media and entertainment sector and has represented celebrities, artists, broadcasters, production houses, top business houses, industrialists, and conglomerates across all forums, including the Apex Court. Ameet has authored two books and is regularly ranked by leading global and domestic publications.

Saakar S. Yadav is a seasoned technologist and platform architect with over two decades of hands-on experience designing and scaling large, high-impact digital systems. He has played a pivotal role in national technology initiatives—including building the Central Data Processing Centre for the National Judicial Reference System (NJRS), one of India's largest judicial-appeal repositories—demonstrating mastery in complex data handling, high-volume processing, and mission-critical system design.

As the founder of LexLegis.ai, Saakar brings deep expertise in robust architecture development, compliance-driven platform engineering, and real-world digital governance. His experience spans tax-tech, legal-tech, enterprise systems, and government-grade technology—making him uniquely positioned to define AI usage standards that are scalable, secure, compliant, and technically sound.

His contributions ensure the handbook is grounded not only in theoretical governance principles but also in practical, technologically executable guidelines that reflect the realities of modern platform ecosystems.

TABLE OF CONTENTS

1. PURPOSE

The purpose of this handbook is to establish a clear and comprehensive standard for the responsible, ethical, secure, and legally compliant use of artificial intelligence within the organization. Artificial intelligence has the potential to significantly improve productivity, enhance decision-making, and streamline operations; however, it also introduces risks related to data privacy, misinformation, bias, ethical misuse, and operational inconsistency.

This document ensures that every individual interacting with AI understands their responsibilities, adheres to established guidelines, and exercises judgment consistent with the organization's values and obligations. The policy emphasizes that AI must always be used in a manner that respects privacy, maintains confidentiality, avoids discrimination or harm, and promotes professional integrity.

Compliance with this policy is verified through periodic audits, logging reviews, and training assessments. If any misuse or non-compliance is identified, corrective action will be taken, which may include retraining, revocation of AI tool access, or other disciplinary measures in line with corporate governance protocols.

2. SCOPE

This handbook applies to all individuals who work with or interact with AI systems on behalf of the organization. This includes full-time employees, part-time staff, interns, consultants, contractors, and external vendors who have been granted access to any corporate systems that use or expose AI capabilities.

The systems governed by this policy cover the entire range of AI applications, including but not limited to content-generation tools, predictive analytics platforms, automation tools, natural-language processing engines, recommendation systems, internal chatbots, and third-party AI services accessed through APIs.

Because AI usage is inherently tied to data access and business workflows, the organization performs routine comparisons of system activity logs against the list of

approved tools. Any evidence of unapproved AI usage is immediately investigated. Unauthorized systems are blocked at the network level to protect corporate and personal data.

3. DEFINITIONS

For clarity and consistency, several key terms require detailed explanation.

Artificial intelligence refers to technological systems that are capable of learning patterns, identifying relationships, generating content, or making predictions and recommendations based on data inputs. These systems may vary from simple automation tools to complex machine-learning models, and they may be hosted internally or by external vendors.

Generative AI refers to AI systems capable of producing original or synthetic content such as text, images, audio, code, or analytical summaries. These systems often operate by predicting likely outputs based on patterns learned during training.

Personal data refers to any information about an identifiable individual. This includes names, contact numbers, identification numbers, financial details, health information, location details, behavioral attributes, or any data that can either directly or indirectly be linked to an identifiable person.

Sensitive personal data refers to categories of information that, if misused, could cause harm or risk to an individual—such as financial data, government IDs, biometric identifiers, health information, data of children, or information relating to protected characteristics.

All personal data must be treated as regulated material. This means that employees cannot assume an item is "non-sensitive" unless explicitly defined as such. Logs, prompt monitoring, and random audits ensure that personal or sensitive data does not appear in AI prompts or unapproved workflows. If such data is found, the breach protocol is immediately activated.

4. AI GOVERNANCE STRUCTURE

A structured governance system ensures that AI operations remain safe, transparent, and aligned with organizational values. A dedicated AI Governance Board oversees the approval of new AI tools, evaluates risks, and conducts periodic audits across departments. This board functions as the primary authority ensuring that AI deployments align with the organization's risk appetite, business goals, and ethical commitments.

Each deployed AI system is assigned a System Owner responsible for monitoring its performance, maintaining lifecycle documentation, approving updates, and ensuring the system continues to operate within defined boundaries. The System Owner acts as the single point of accountability for that system.

A Data Protection Lead ensures that all data processed by AI—especially personal and sensitive personal data—is handled in full compliance with applicable law and internal standards. This includes reviewing data flow diagrams, assessing privacy risks, and verifying that data is processed only for its intended purpose.

The Security Team ensures AI systems are accessed securely, monitors system behavior, detects anomalies, and ensures all APIs, credentials, and model endpoints are protected from misuse or unauthorized access.

No AI-related system or significant modification may be released into production unless it has passed through this formal governance structure.

5. RISK CLASSIFICATION FRAMEWORK

Every AI system carries a different potential impact on individuals, business operations, and legal compliance. The organization therefore uses a structured risk classification method to determine whether a system requires minimal oversight, elevated oversight, extensive human monitoring, or complete prohibition.

Minimal-risk systems include tools used for drafting content, generating summaries, performing brainstorming tasks, and other low-impact processes where the output can easily be corrected by a human.

Limited-risk systems may support internal decision processes or perform generalized analysis. They require oversight to ensure that their outputs remain reliable and that no personal data is exposed to unnecessary processing.

High-risk systems include any AI that influences decisions about individuals' rights, financial well-being, employment status, access to healthcare, or legal or ethical treatment. These systems must undergo the highest level of scrutiny, testing, documentation, and human oversight.

Certain types of AI are strictly prohibited—such as systems designed for manipulation, deception, discriminatory profiling, or invasive monitoring of individuals.

Risk classification must be performed before deployment and revisited periodically. Any system without classification is automatically prevented from deployment.

6. ACCEPTABLE USE OF AI

AI may be used as an augmenting tool rather than a decision-maker. Employees may rely on AI for research support, initial drafting of emails, creation of first-draft documents, development of content outlines, or generation of suggestions. However, the employee remains fully accountable for the accuracy and appropriateness of the final output. AI-generated content must be reviewed line by line, corrected where necessary, and contextualized before being shared internally or externally.

The organization treats AI output as an unverified suggestion. Employees must cross-check facts, validate numbers, avoid quoting AI as an authoritative source, and ensure no sensitive content is inadvertently introduced. The responsibility for accuracy always rests with the human user, not the AI system.

Audits and supervisory reviews help ensure that employees consistently follow these guidelines.

7. PROHIBITED USE OF AI

There are categories of actions that employees must never perform using AI systems. The organization forbids entering personal, financial, medical, or confidential data into unapproved AI tools under any circumstances. This includes customer information, employee records, business strategies, vendor details, contract text, or confidential intellectual property.

The organization also prohibits prompting AI to create content that is harmful, illegal, sexually explicit, discriminatory, abusive, or deceptive. AI must never be used to bypass legal processes, manipulate individuals, interfere with protected groups, or generate content intended to mislead stakeholders.

Using AI through personal accounts for business purposes is strictly prohibited. Attempting to override safety controls or exploit system vulnerabilities is a serious violation subject to disciplinary review.

If prohibited usage is detected, the issue is escalated to the Data Protection Lead and the Information Security Team immediately.

8. DATA PRIVACY & CONFIDENTIALITY

All personal data processed through or around AI must be handled with the utmost care and respect for individual privacy. Employees must adhere to principles such as purpose limitation, meaning data must only be used for specific, legitimate business functions that have been clearly documented. Consent must be obtained where required, including when working with minors' data or sensitive categories of personal data. Individuals have the right to withdraw consent, correct inaccurate information, and request deletion of their data.

Employees may not input personal or sensitive data into generative AI systems unless the tool has been explicitly approved for such processing and appropriate data-protection measures are in place. Even in approved environments, only the minimum amount of data required for the workflow should be used. Unnecessary information must be avoided.

Data must be anonymized, masked, or pseudonymized wherever possible. If a data breach occurs, whether accidental or deliberate, the Data Protection Lead initiates the required remediation steps, which may include logging the breach, determining impact, notifying affected individuals, and preventing further misuse.

9. SECURITY REQUIREMENTS

AI systems must be protected through robust digital security protocols. Users must access AI platforms using secure corporate accounts, protected with multi-factor authentication. Sensitive data passing through AI pipelines must be encrypted both during transmission and while stored.

Credentials, including API keys, must never be shared or hardcoded into code repositories. Access must be granted on a strictly need-to-know basis, with continuous audits ensuring that permissions are appropriate and that no unauthorized individuals have gained access.

Security teams regularly monitor logs and system behaviors to detect anomalies such as unusual traffic patterns, improper data uploads, or repeated system misuse. Any suspicious activity triggers an immediate security review.

Employees involved in a security breach may have their access revoked until the issue is resolved.

10. ETHICAL & RESPONSIBLE AI USE

AI must always be used in a manner that reflects fairness, respect, and ethical conduct. This includes ensuring that outputs are free from prejudice, discriminatory implications, or harmful stereotypes. Employees must never encourage AI to produce content that targets or disadvantages any individual or group based on attributes such as race, gender, disability, age, socioeconomic status, or other protected characteristics.

AI-generated content must uphold corporate values of dignity, accuracy, and professionalism. Employees should be aware that AI systems may inadvertently reflect bias present in training data. Because of this, regular fairness testing is necessary. If any biased or harmful output is detected, it must be reported and investigated immediately.

11. HUMAN OVERSIGHT & ACCOUNTABILITY

AI must never replace human judgment in areas where decisions carry meaningful consequences. For decisions involving hiring, promotions, disciplinary action, insurance, creditworthiness, healthcare guidance, or legal recommendations, AI may assist through pattern analysis or data summarization, but the final decision must always be made and documented by a qualified human professional.

Human oversight includes reviewing AI outputs, contextualizing recommendations, and ensuring that decisions are fair, well-reasoned, and compliant with organizational and legal standards. Any decision found to have bypassed required human oversight must be reviewed, corrected if necessary, and logged for future governance analysis.

12. TRANSPARENCY REQUIREMENTS

When AI is involved in producing customer-facing content, internal reports, or automated responses, this involvement must be disclosed clearly. Transparency is necessary to maintain trust and ensure that stakeholders understand the nature of the information they are receiving.

Communication templates, chatbot scripts, automated messages, and support responses are periodically inspected to ensure they include appropriate notices indicating AI involvement. If a disclosure is missing, the employee responsible must correct the content and ensure that future communications follow transparency expectations.

13. AI MODEL LIFECYCLE MANAGEMENT

The organization maintains comprehensive documentation for every AI system deployed. This documentation includes the system's purpose, how it was trained, what datasets were used, what assumptions were made, and what limitations exist. It also includes technical metrics such as accuracy, drift sensitivity, operational boundaries, and any identified risks.

Documentation must be actively maintained and updated whenever the model or associated workflows are modified. Outdated documentation can result in misunderstandings or misapplications of the system, and therefore, no system may remain in production without current documentation.

14. VENDOR & THIRD-PARTY AI GOVERNANCE

Before a third-party AI tool or service is approved for use, the organization conducts a thorough evaluation of the vendor's capabilities, infrastructure, policies, and data-handling practices. This includes reviewing how the vendor stores data,

whether they share information with third parties, what security mechanisms they use, and whether their contractual obligations align with the organization’s requirements.

If a vendor’s practices do not meet the organization's security, privacy, and ethical standards, the integration is not approved. Vendor partnerships are re-evaluated periodically to ensure ongoing compliance.

15. PERFORMANCE MONITORING & DRIFT MANAGEMENT

Over time, AI models may degrade in performance due to changes in data patterns, market conditions, or user behavior. This phenomenon, known as drift, can cause a model to become less accurate or behave unpredictably. To prevent this, continuous performance monitoring is mandatory.

Metrics such as accuracy, precision, recall, response quality, safety event frequency, and operational consistency are measured and recorded. If these metrics show deviations, the model may be recalibrated, retrained, or rolled back to a previous stable version.

16. INCIDENT REPORTING & RESPONSE

Any anomaly in AI outputs or behavior must be reported immediately. This includes unsafe, biased, inaccurate, offensive, or unexpected outputs. Incidents may arise from misuse, flawed prompts, incorrect configurations, data leaks, or model failures.

A prompt reporting culture ensures that potential harm is prevented. Once an incident is reported, the organization conducts an investigation to identify the cause and implement necessary corrective measures. Failure to report incidents promptly may be treated as a governance violation.

17. TRAINING & AWARENESS

AI is a powerful tool that requires knowledgeable and responsible handling. All users must complete annual training that covers AI safety, responsible usage, data privacy, legal responsibilities, security practices, and organizational values.

Specialized training is mandatory for employees who work directly with high-risk systems or sensitive data. Training completion is tracked, and access to AI tools may be restricted until all required learning modules have been completed.

18. COMPLIANCE, AUDIT & PENALTIES

To ensure the sustained integrity of AI operations, the organization performs regular audits of systems, workflows, logs, and data-handling practices. Compliance teams review prompts, outputs, decision records, classification forms, and vendor evaluations.

Non-compliance may lead to formal warnings, corrective training, suspension of access, or other disciplinary actions depending on severity. Repeated or serious violations may result in employment or contract termination.

19. MODEL & PROMPT CHANGE MANAGEMENT

AI systems evolve over time. Whether a model upgrade, prompt change, vendor update, parameter adjustment, or dataset replacement occurs, the system must undergo complete revalidation. This involves repeating all safety, bias, accuracy, privacy, and rejection-behavior tests that were performed during the initial deployment phase.

Any change—no matter how small—can impact behavior. Therefore, approval must be obtained again before reintroducing the updated version into production.

Unauthorized changes must be reversed immediately until the updated system passes all required checks.

20. MANDATORY AI VALIDATION TEST SUITE

Every AI system must undergo rigorous evaluation before deployment or redeployment. These validations examine whether the system produces accurate information, avoids harmful or biased content, respects confidentiality, rejects inappropriate prompts, upholds privacy principles, and responds consistently across repeated tests.

The test suite includes scenarios for factual accuracy, safety, ethics, refusal behavior, bias detection, language tone stability, and operational reliability. If the model fails any part of the validation, deployment is blocked until rectified.

21. DEPLOYMENT, LOGGING & CONTINUOUS MONITORING

Once deployed, AI systems must maintain detailed logs of user interactions, data flows, system responses, and technical errors. These logs are vital for auditing compliance, identifying misuse, and detecting anomalous behaviors.

Monitoring tools continuously assess the performance and safety of the system, alerting designated personnel to potential issues. If any pattern suggests instability or risk, the system may be paused for immediate evaluation.

22. DOCUMENT CONTROL

This handbook is reviewed regularly to ensure it reflects current laws, industry standards, and corporate objectives. Every employee must acknowledge updated

versions. Version history is maintained for accountability, and any changes are clearly documented.

23. MASTER CHECKLISTS

To ensure practical implementation, the organization maintains detailed operational checklists for daily AI usage, privacy and security compliance, lifecycle management, vendor assessments, deployment readiness, and monitoring workflows. These checklists guide employees and teams in consistently applying required procedures and ensuring no step is overlooked.

APPENDIX: AI GOVERNANCE CHECKLIST

ORGANIZATIONAL GOVERNANCE

☐ AI Governance Board is formally established.
☐ Roles and responsibilities (System Owner, DPO, Security Lead) are assigned.
☐ Every AI system has an accountable owner documented.
☐ Governance workflows are documented and accessible.
☐ AI Usage Policy is reviewed annually.
☐ Updates to the policy are communicated to all employees.
☐ Employees acknowledge receiving the latest policy version.
☐ AI usage logs are monitored for compliance.
☐ Periodic audits are scheduled and performed.
☐ Audit findings are documented and resolved.

RISK CLASSIFICATION

☐ Each AI tool has undergone a risk assessment.
☐ Risk level (Minimal/Limited/High/Prohibited) is documented.
☐ Basis for classification is recorded.
☐ Risk classifications are reviewed periodically.
☐ High-risk tools have received governance approval.
☐ Prohibited AI tools are blocked across systems.

DATA PROTECTION

☐ Personal data usage for each system has been reviewed.
☐ Data minimization principles are followed.
☐ Sensitive personal data is not processed unless approved.
☐ Data flow diagrams are documented.
☐ Consent (where applicable) has been obtained and stored.

☐ Data is used only for approved purposes.
☐ Personal data is encrypted in transit and at rest.
☐ Data transfers to third parties are justified and approved.
☐ Anonymization/masking techniques are applied where possible.
☐ AI-related data breach protocol is documented.
☐ Employees know how to report accidental data exposure.

4. SECURITY

☐ All AI tools require secure corporate accounts.
☐ MFA is enabled for all AI system access.
☐ API keys are securely stored and rotated.
☐ Access controls follow least-privilege principles.
☐ AI system logs are securely stored and monitored.
☐ Unauthorized AI tools are blocked by DLP/firewall.
☐ Prompts and outputs are logged for compliance review.
☐ Anomalies are automatically flagged.

5. ACCEPTABLE USE

☐ Only approved AI systems are used for company work.
☐ AI-generated content is reviewed line-by-line by a human.
☐ Facts and figures generated by AI are independently verified.
☐ AI output is edited for quality, tone, and professionalism.
☐ AI is treated as assistive—not authoritative.

6. PROHIBITED USE

☐No personal data is entered into unapproved AI tools.
☐ No sensitive data is entered into any generative AI.
☐ Confidential business information is not shared with unauthorized tools.
☐ No harmful, abusive, explicit, or discriminatory content is generated.

☐ No attempts are made to bypass AI safety or security controls.
☐ No AI work is performed using personal accounts or consumer tools.

7. ETHICAL & RESPONSIBLE AI

☐ AI outputs are monitored for fairness and bias.
☐ Bias testing is documented and reviewed.
☐ AI does not produce harmful or discriminatory content.
☐ Adversarial prompts are used to test safety.
☐ Issues of bias or harm are reported immediately.

8. HUMAN OVERSIGHT

☐ All high-impact AI-assisted decisions undergo human review.
☐ Human reviewers validate reasoning and correctness.
☐ Decision-maker identity is documented.
☐ Manual overrides or corrections are logged.
☐ AI never independently makes decisions affecting rights or well-being.

9. TRANSPARENCY

☐ AI involvement is disclosed when required.
☐ Customer-facing content includes AI-disclosure where applicable.
☐ Model limitations and risks are documented and visible.

10. MODEL LIFECYCLE MANAGEMENT

☐ Model purpose and scope are clearly defined.
☐ Training data sources are documented.
☐ Accuracy and limitations are documented.
☐ Model version control is maintained.
☐ Retired models are archived securely.
☐ Documentation is up-to-date and reviewed regularly.

11. VENDOR & THIRD-PARTY REVIEW

☐ Vendors pass security and privacy assessments.
☐ Vendor policies align with DPDP and internal requirements.
☐ Data Processing Agreements (DPAs) are signed.
☐ Sub-processors are disclosed and approved.
☐ Vendor re-evaluations occur annually.

12. PERFORMANCE MONITORING & DRIFT

☐ Performance metrics are monitored continuously.
☐ Drift warnings are triggered and logged.
☐ Accuracy tests are conducted periodically.
☐ Safety violations are tracked.
☐ Model recalibration or retraining is performed when needed.

13. INCIDENT REPORTING

☐ Employees know how to report AI issues.
☐ Incident reporting workflow is documented.
☐ All AI incidents are logged and reviewed.
☐ Corrective actions are documented.
☐ Lessons learned are implemented.

14. TRAINING

☐ All employees completed AI safety training.
☐ High-risk system users completed advanced training.
☐ Annual refresher courses are assigned and tracked.
☐ Training records are maintained.

15. MODEL & PROMPT CHANGE MANAGEMENT

☐ Any model/prompt change is documented and justified.
☐ Governance approval is obtained before the change.
☐ A rollback plan is prepared.
☐ Validation tests are rerun after each change.
☐ Accuracy, safety, privacy, bias, and stability tests pass.
☐ Re-approval is granted before deployment.
☐ Unauthorized changes are rolled back immediately.

16. AI VALIDATION TEST SUITE

☐ Accuracy tests pass consistently.
☐ Safety refusal tests pass.
☐ Bias prevention tests show no anomalies.
☐ Privacy refusal tests work correctly.
☐ Security-related prompts are correctly declined.
☐ Tone and professionalism remain stable.
☐ Output consistency is maintained across repeated runs.

17. DEPLOYMENT & MONITORING

☐ All deployment approvals are attached and verified.
☐ Logs are fully active before deployment.
☐ Monitoring alerts are configured.
☐ System is continuously monitored post-deployment.
☐ Anomalies are escalated immediately.

18. DOCUMENT CONTROL

☐ Handbook versioning is maintained.
☐ Employees are notified of updates.
☐ Old versions are archived.
☐ Change logs are maintained.