

	AI Usage Policy	Ref: NLL_AI_V1.3
		Date: 30-09-2026



NEULAND LABORATORIES LIMITED

Phoenix IVY III, Rd Number 82, Jubilee Hills, Hyderabad – 500 033

AI Usage Policy

Reference	NLL_AI_V1.3		Issue No.	1.3
Release Date	30-09-2026		Total No. of pages	09
	Name	Designation	Date	Authorization
Prepared by	Syed Kareem	Manager – ITS	30-09-2026	Email dated: 30-09-2026
Reviewed by	Nageswara Rao YSVR	AGM – ITS	30-09-2026	Email dated: 30-09-2026
Approved by	Ajitabh Singh	VP – ITS	30-09-2026	Email dated: 30-09-2026

Record of Revision

S. No	Version		Date of Change	Changes made
	From	To		
1	1.0	-	06-11-2025	Draft for Approval
2	1.0	1.1	07-11-2025	Approved
3	1.1	1.2	24-03-2026	Reviewed and no changes required
4	1.2	1.3	30-09-2026	Policy reviewed and updated to include responsible AI principles, cybersecurity controls, human oversight, training, compliance, reporting, third-party AI governance, and employee do's and don'ts.

Table of Content

Sl. No	Content	Page No
1	Overview	4
2	Purpose and Scope	4
3	Responsible Artificial Intelligence Principles	5
4	Key Principles	5
5	Roles & Responsibilities	7
6	Cybersecurity of Artificial Intelligence Systems	7
7	Human Oversight and Human Intervention	8
8	Awareness, Training and Responsible Use	8
9	Compliance and Continuous Improvement	8
10	Third-Party Artificial Intelligence Systems	9
11	Reporting	9

	AI Usage Policy	Ref: NLL_AI_V1.3
		Date: 30-09-2026

1. Overview

At Neuland, we are committed to conducting our business with integrity, transparency, accountability, and responsibility. As technology and artificial intelligence (AI) continue to evolve, we recognize the opportunities AI can provide to enhance operational efficiency, innovation, decision-making, customer experience, risk management, and business resilience.

At the same time, we recognize that the use and development of AI systems may give rise to risks relating to data privacy, cybersecurity, bias and discrimination, transparency, accountability, human rights, safety, environmental impacts, and unintended societal consequences.

This Responsible Artificial Intelligence Policy establishes the principles and requirements that govern responsible use, development, procurement, and monitoring of AI systems across Neuland. The Policy applies to AI systems developed internally as well as AI systems, models, platforms, applications, and services provided by third parties.

Neuland is committed to using AI in a manner that respects human rights, protects individuals and information, supports fair and responsible decision-making, safeguards the environment, and complies with applicable laws and regulations

2. Purpose and Scope

This policy ensures the ethical, secure, and compliant use of Artificial Intelligence (AI) tools within Neuland. It aims to protect company data, maintain regulatory compliance, and foster responsible innovation.

The purpose of this Policy is to establish a responsible and risk-based framework for the use and development of AI across Neuland.

This Policy applies to:

- All employees, workers, and other personnel are involved in the use, procurement, development, implementation, or oversight of AI systems.
- AI systems and models that are developed, owned, licensed, procured, or deployed by Neuland
- Third-party AI systems, platforms, applications, models, and services used in connection with Neuland operations.
- AI systems used for operational, commercial, analytical, administrative, customer-facing, human resources, supply chain, cybersecurity, research and development, or other business purposes.

AI systems shall only be used for legitimate and authorized business purposes and within their defined scope, capabilities, and limitations.

	AI Usage Policy	Ref: NLL_AI_V1.3
		Date: 30-09-2026

3. Responsible Artificial Intelligence Principles

Neuland approach to AI is founded on the following principles:

1. Respect for data privacy and confidentiality
2. Cybersecurity and resilience
3. Human oversight and intervention
4. Transparency and explainability
5. Clear accountability
6. Defined boundaries and responsible use
7. Prevention of prohibited and harmful AI applications

These principles shall apply throughout the AI lifecycle, including the identification, design, development, procurement, testing, deployment, use, monitoring, modification, and retirement of AI systems.

4. Key Principles

i) Data Privacy & Security

- Do NOT upload, paste, or share confidential, proprietary, or personally identifiable information (PII) into external AI tools (e.g., free public AI platforms).
- Use only IT-approved AI tools (e.g., Microsoft Copilot, Grammarly Enterprise, Canva, Automation Edge, 3RD Party AI Integrated tools like CLM) i within Neuland's security framework.
- Confidential, proprietary, and PII data must never be uploaded into AI tools.

Data Classification:

- Public: Allowed
- Internal: Allowed with caution
- Confidential: Not allowed
- GxP/Regulatory: Strictly prohibited
- Respect applicable data protection and privacy laws and regulations in the jurisdictions in which it operates.
- Ensure that personal data is processed lawfully, fairly, transparently, and for legitimate and defined purposes.

ii) Shadow AI Prohibition

- Employees must not use unauthorized AI tools for work purposes.
- Report any AI tool requirement to IT for evaluation and approval.

iii) Compliance with Regulations

- Ensure AI usage aligns with GDPR, Indian IT Act, and industry-specific compliance (e.g., GxP for pharma).
- Accuracy & Accountability
- AI output must be verified by employees before use in decision-making, reporting, or external communication.

	AI Usage Policy	Ref: NLL_AI_V1.3
		Date: 30-09-2026

- Employees remain accountable for all work produced using AI.
- No autonomous agent should be created which is allowed to take any action without human foresight.
- Each agent should have human owner assigned.

iv) **Ethical Use**

- Avoid generating misleading, discriminatory, or harmful content.
- Do not use AI for surveillance or profiling without explicit legal and organizational approval.
- Allowed: Email drafting, summaries, document structuring.
- Prohibited: customer confidential data and any IP content data.

v) **Intellectual Property**

- Respect copyright laws; do not use AI to reproduce copyrighted material.
- Ensure AI-generated content is properly attributed when required.

vi) **Transparency**

- Disclose AI involvement in content creation when sharing externally (e.g., reports, presentations).

vii) **Training & Awareness**

- Employees must complete Responsible AI training in LMS provided by IT before using AI tools.

viii) **Monitoring & Enforcement**

- IT will monitor AI usage for compliance.
- Violations may lead to disciplinary action per company policy.

ix) **Access request for AI tools**

- Take internal approval for Gen AI tools like Grammarly and Copilot from HOD.
- Request to IT for Gen AI Software with HOD budget approval. Allocation of Gen AI tools will be as per sole discretion of Head of IT only.

Examples of Approved AI Use

- Grammar and clarity improvements using Grammarly Enterprise.
- Productivity enhancements using Microsoft Copilot integrated with Neuland systems.
- AI-driven analytics within validated platforms approved by IT.
- Low Risk: Email drafting, meeting summaries

Prohibited Practices

- Uploading confidential project data to free AI tools.
- Using AI to generate regulatory and quality documents without validation.
- Sharing AI-generated content externally without review.

	AI Usage Policy	Ref: NLL_AI_V1.3
		Date: 30-09-2026

5. Roles & Responsibilities

Role	Responsibility
Employees	Ensure safe and compliant use of AI tools
Managers	Ensure team adherence and awareness
IT Team	Tool governance, approval, monitoring
InfoSec Team	Risk management, data protection, audits

6. Cybersecurity of Artificial Intelligence Systems

Neuland is committed to protecting AI systems, associated infrastructure, models, applications, data, and interfaces against cybersecurity threats and unauthorized use.

AI systems shall be subject to appropriate cybersecurity measures proportionate to their risk and intended use. Such measures may include:

- Access controls and authentication mechanisms.
- Encryption and protection of data in transit and at rest, where appropriate.
- Secure configuration and secure development practices.
- Vulnerability assessment and security testing.
- Monitoring for unauthorized access, misuse, manipulation, or abnormal system behavior.
- Appropriate incident detection, response, containment, recovery, and reporting mechanisms.
- Protection against malicious inputs, unauthorized prompts, data leakage, model manipulation, and other AI-specific threats, where relevant.
- Periodic review of cybersecurity controls throughout the AI system lifecycle.

AI systems shall not be deployed or used where identified cybersecurity risks cannot be appropriately managed within Neuland risk tolerance.

7. Human Oversight and Human Intervention

Neuland recognizes that AI systems should support human decision-making and shall not replace appropriate human accountability for critical or high-risk decisions.

Neuland shall ensure that:

- Appropriate human oversight is maintained over AI systems based on their risk, purpose, and potential impact.
- Critical or high-risk decisions influenced by AI are subject to meaningful human review.
- Authorized personnel have the ability to question, review, reject, modify, override, suspend, or discontinue AI-generated recommendations or outputs where appropriate.
- AI systems are not permitted to make irreversible or high-impact decisions without appropriate human oversight and intervention mechanisms.
- Employees responsible for reviewing AI-generated outputs have sufficient authority, competence, and information to exercise meaningful judgment.
- AI-generated recommendations shall not be treated as automatically correct or authoritative.

	AI Usage Policy	Ref: NLL_AI_V1.3
		Date: 30-09-2026

Where necessary, AI systems shall be designed or configured to escalate decisions or situations to an appropriately authorized human decisionmaker.

8. Awareness, Training and Responsible Use

Neuland recognizes that responsible AI depends on informed and accountable users.

Relevant employees and personnel shall receive appropriate awareness, guidance, or training regarding:

- Responsible and authorized use of AI.
- Data privacy and confidentiality.
- Cybersecurity risks associated with AI.
- Potential bias and discrimination.
- Human oversight and professional judgment.
- AI limitations, inaccuracies, and hallucinations.
- Appropriate use of AI-generated information and outputs.
- Applicable organizational requirements and legal obligations.

Personnel shall remain responsible for exercising appropriate judgment when using or relying upon AI-generated information.

9. Compliance and Continuous Improvement

All personnel and relevant third parties shall comply with this Policy and applicable procedures established under it.

Neuland shall promote continuous improvement in its responsible AI practices by periodically reviewing AI-related risks, controls, governance arrangements, and emerging good practices.

Where non-compliance or material weaknesses are identified, appropriate corrective and preventive actions shall be taken within defined timelines.

Neuland may restrict, suspend, modify, or discontinue an AI system where its use presents unacceptable legal, ethical, privacy, cybersecurity, human rights, environmental, or other material risks.

10. Third-Party Artificial Intelligence Systems

Neuland recognizes that significant AI-related risks may arise from third-party systems, models, platforms, cloud services, and AI providers.

Before adopting material or higher-risk third-party AI systems, Neuland shall, as appropriate to the risk:

- Assess the intended use and potential risks of the AI system.
- Consider data privacy and information-security requirements.

	AI Usage Policy	Ref: NLL_AI_V1.3
		Date: 30-09-2026

- Consider the provider's approach to responsible AI, cybersecurity, data protection, transparency, and accountability.
- Establish appropriate contractual or other safeguards for the protection of Neuland data and information.
- Consider the environmental performance of relevant AI infrastructure and data centers.
- Define appropriate restrictions, access controls, and permitted uses.
- Monitor material risks associated with continued use of the third-party AI system.

Third-party AI systems shall remain subject to Neuland applicable policies, controls, and approval requirements.

11. Reporting

If you suspect misuse or need AI tool approval, contact IT Security at cybersecurity@neulandlabs.com

Employee Do's & Don'ts for Responsible AI Usage

✓ Do's

- **Use only IT-approved AI tools** (e.g., Microsoft Copilot, Grammarly Enterprise).
- **Verify AI-generated content** before using it in official documents or communications.
- **Complete mandatory Responsible AI training** before using any AI tool.
- **Report new AI tool requirements** to the IT Security Team for evaluation.
- **Disclose AI involvement** in external-facing content when required.
- **Follow data classification guidelines**—only share public or approved data with AI tools.

✗ Don'ts

- **Do NOT upload or paste confidential, proprietary, or personal data** into external AI tools.
- **Do NOT use free or unapproved AI platforms** for any work-related tasks.
- **Do NOT rely solely on AI outputs** for decision-making without human review.
- **Do NOT use AI to create misleading, discriminatory, or harmful content.**
- **Do NOT share AI-generated content externally without proper validation and approval.**
- **Do NOT bypass IT security controls** to access AI tools.