NEMR AI Policy for Employees
Effective Date: 5/1/2025
Version 1.0

---

1. Purpose

This policy provides guidelines for all employees of NEMR regarding the appropriate and responsible use of Artificial Intelligence (AI) tools and technologies in their daily work. It ensures ethical practices, data protection, and alignment with company goals and values.

---

2. Scope

This policy applies to all full-time, part-time, contract, and temporary employees using AI-powered tools or engaging in AI-related activities within the company environment.

---

3. Key Responsibilities

Employees are expected to:

- Use AI tools ethically and in accordance with legal and company standards.
- Protect customer, employee, and company data when interacting with AI systems.
- Report any unintended outcomes, biases, or security concerns in AI systems.
- Follow all applicable training and compliance requirements related to AI.

---

4. Acceptable Use of AI Tools

Employees may use AI tools to:

- Automate routine tasks (e.g., email summarization, meeting transcriptions).
- Analyze and interpret large data sets for business insights.
- Improve customer support via AI-powered assistants and chatbots.
- Enhance productivity through internal AI solutions (e.g., document drafting, translation).

All AI usage must be aligned with an employee’s role and receive approval from their supervisor or the IT team when integrating third-party tools.

---

5. Prohibited Uses

Employees may **not** use AI to:

- Process or expose sensitive customer data and company information.
- Make decisions on hiring, promotions, or terminations without required human oversight.
- Generate or disseminate false, misleading, or manipulated content (e.g., deepfakes).
- Bypass security controls or violate licensing terms of AI tools.
- Use AI in a way that could result in discrimination or harassment.

---

6. Data Privacy & Confidentiality

Employees must ensure:

- AI systems are not trained using internal, customer, or proprietary data.
- No confidential or personal information is entered into public or unsecured AI platforms (e.g., public generative AI tools).
- AI-generated content does not unintentionally disclose sensitive information.

---

7. Reporting Concerns

If you observe inappropriate use of AI, discover a potential bias, or experience a system error or data exposure involving AI, report it immediately to:

- Your direct manager
- The IT Security Team

Confidentiality will be maintained, and retaliation for good-faith reporting is strictly prohibited.

8. Violations

Violations of this policy may result in disciplinary action up to and including termination, depending on the severity of the offense and applicable laws or labor agreements.

9. Policy Review

This policy will be reviewed and updated annually or as required due to technological, legal, or business changes.

Questions or Clarifications?
Please contact: **Network/IT Manager Jason Hill** at netmgr@nemr.net or your direct manager.