OpsMind AI – Information Security Policy

This Information Security Policy defines the standards and controls implemented in the OpsMind AI system to ensure confidentiality, integrity, and availability of enterprise Standard Operating Procedure (SOP) documents and user data.

1. Purpose The purpose of this policy is to protect organizational SOP documents and user information processed within OpsMind AI. The system ensures that sensitive operational knowledge is accessed only by authorized users and used strictly within approved contexts.

2. Scope This policy applies to all users, administrators, developers, and systems interacting with OpsMind AI, including frontend applications, backend services, databases, and AI inference components.

3. Access Control Access to OpsMind AI is restricted through secure user authentication mechanisms. Each user must register and log in using valid credentials. JSON Web Tokens (JWT) are used to manage authenticated sessions, ensuring that only authorized users can access protected endpoints such as document upload, chat, and dashboard services.

4. Data Protection All uploaded SOP documents are processed securely. Sensitive data extracted from documents is stored in a structured format within the database. No document content is exposed without authentication. Encryption practices are applied where applicable, and data transmission between frontend and backend occurs over secure channels.

5. AI Usage and Data Isolation OpsMind AI uses a Retrieval-Augmented Generation (RAG) approach. The AI model is strictly constrained to answer questions using only the retrieved document context. The system prevents hallucination by disallowing external knowledge beyond the uploaded SOPs.

6. Logging and Monitoring System activities such as user logins, document uploads, and query execution are logged for monitoring and audit purposes. Logs help detect unauthorized access attempts and system misuse.

7. Incident Management Any security incident, including unauthorized access, data leakage, or system failure, must be reported immediately to system administrators. Corrective actions are taken promptly to restore system integrity.

8. Availability and Reliability The system is designed to ensure high availability. Backend services are monitored, and failures in AI inference or database access are handled gracefully with appropriate error responses.

9. User Responsibilities Users are responsible for maintaining the confidentiality of their login credentials. Sharing of accounts or misuse of the system for unauthorized purposes is strictly prohibited.

10. Compliance This policy aligns with standard enterprise security practices and is designed to support compliance with organizational and academic data protection requirements.

11. Policy Review This policy is reviewed periodically and updated as the OpsMind AI system evolves or new security requirements emerge.