AI Control Matrix	Control Objective		
Control Type	Prevent	Detect	Correct
Administrative Controls *(Policies, Governance, Awareness)*	**AI Governance Framework** (Establish risk policies, ethics guidelines)	**AI Model Logging & Audit Trails** (Track model decisions and actions)	**AI Playbook extension** to the **Incident Response Plan** (Define response for AI-related security breaches)
	AI Risk Assessment Process (Conduct periodic evaluations)	**AI Incident Reporting Procedures** (Establish AI-specific security incident workflows)	**AI Bias & Model Correction Process** (Monitor and retrain models as needed)
	Third-Party AI Vendor Due Diligence (Security reviews of AI providers)	Regular **AI Risk Audits** (Identify non-compliance with governance standards)	**Regulatory Compliance Review** (Ensure ongoing adherence to AI regulations)
	AI Responsible Use Policy & Acceptable Use guidelines (Define authorized Use cases)		
Physical Controls *(Access, Environment, Physical Infrastructure)*	**Secure Data Centers** (Restrict access to AI training and inference systems)	**Environmental Monitoring** (Detect unauthorized access to AI compute resources)	**Backup and Disaster Recovery of AI Models** (Ensure rollback options for corrupted models)
	Restricted AI Model Deployment Zones (Limit where models can operate)	**Surveillance & Access Logging** (Monitor physical access to AI training infrastructure)	**Physical AI Infrastructure Remediation** (Replace compromised AI hardware)
	Tamper-Proof AI Hardware (Deploy AI-specific protections in edge devices)		
Technical Controls *(AI Model Security, Data Protection, Access Controls)*	**Secure AI Model Development Lifecycle (SDLC)** (Integrate security in AI pipeline)	**AI Behavior Monitoring** (Detect anomalies in AI decision-making)	Automated **AI Model Patching** (Deploy security updates to AI models)
	AI Anonymization & Data Encryption (Protect sensitive training data)	**Adversarial Attack Detection** (Identify AI poisoning or evasion attacks)	AI **Output Validation & Correction** (Flag and fix biased or harmful AI responses)
	Role-Based Access Control (RBAC) for AI Systems (Limit model access)	**Real-Time Model Explainability Tools** (Monitor AI outputs for security risks)	**Incident Containment Measures for AI Compromise** (Quarantine affected models)