Category	Risk_ID	Risk_Description	Likelihood	Impact	Context	Mitigation	Risk_Score	Risk_Level			Owner	KPI
Bias	B1	Speed control algorithms discriminate against certain neighborhoods, creating unequal safety standards	4	4	AI speed zones may reflect historical biases in urban planning	Implement fairness audits and equitable zone mapping across all neighborhoods	16	High	AI Ethics Team	≥95% bias test cases passed		
Bias	B2	Hazard detection AI performs poorly in low-income areas due to training data gaps	3	5	Limited sensor data from underserved communities affects model accuracy	Diversify training datasets and deploy additional sensors in underrepresented area	15	Medium	AI Ethics Team	≤5% demographic parity gap		
Bias	B3	Parking verification AI flags legitimate parking spots in certain cultural/linguistic communities	3	3	Image recognition may struggle with diverse urban environments and signage	Multi-cultural training data and community feedback integration	9	Medium	AI Ethics Team	≥90% fairness audit score		
Bias	B4	AI-optimized vehicle placement favors affluent areas, reducing access equity	4	4	Revenue optimization may conflict with equitable access goals	Mandate minimum service levels across all demographic areas	16	High	AI Ethics Team	≥95% bias test cases passed		
Transparency	T1	Riders cannot understand why speed restrictions activate, reducing trust and compliance	3	3	Black-box AI decisions without clear explanations to users	Implement explainable AI with real-time rider notifications and reasoning	9	Medium	Product Owner	≤2 sec explanation response time		
Transparency	T2	City regulators lack visibility into AI decision-making processes for audit compliance	4	4	Regulatory oversight requires transparent algorithmic accountability	Provide audit trails and algorithmic impact assessments to regulators	16	High	Product Owner	≥90% audit trail completeness		
Transparency	T3	Hazard detection false positives/negatives cannot be explained or corrected	3	4	Safety-critical decisions need clear reasoning for improvement	Deploy interpretable models with feedback loops for continuous improvement	12	Medium	Product Owner	≥85% user comprehension score		
Transparency	T4	Data usage and sharing practices unclear to riders and city partners	2	3	Privacy expectations require clear data governance communication	Publish transparent data governance policies and usage dashboards	6	Medium	Product Owner	≤2 sec explanation response time		
Privacy	P1	Location tracking for safety features enables surveillance and profiling of rider behavior	4	4	Continuous GPS tracking for hazard detection creates privacy concerns	Implement data minimization and anonymization techniques	16	High	Security Team	100% encryption compliance		
Privacy	P2	Parking verification photos inadvertently capture bystanders and private property	5	3	Photo requirements for compliance may violate privacy expectations	Use privacy-preserving computer vision and automatic face/license plate blurring	15	Medium	Security Team	≥99% security audit pass		
Privacy	P3	Cross-platform data sharing with cities exposes individual mobility patterns	3	4	Regulatory data sharing requirements may compromise rider privacy	Implement differential privacy and aggregate-only data sharing	12	Medium	Security Team	≤1% data breach incidents		
Privacy	P4	AI model training inadvertently memorizes sensitive rider information	2	4	Machine learning models may retain individual data points	Use federated learning and privacy-preserving ML techniques	8	Medium	Security Team	100% encryption compliance		
Security	S1	Malicious actors hack speed control systems to cause accidents or disable safety features	2	5	Safety-critical AI systems are high-value targets for cyberattacks	Implement robust cybersecurity frameworks and real-time threat monitoring	10	Medium	Product Owner	≥90% performance target		
Security	S2	Data breaches expose rider location patterns and personal information	3	4	Centralized data storage creates attractive targets for cybercriminals	Deploy end-to-end encryption and distributed data architecture	12	Medium	Product Owner	≥90% performance target		
Security	S3	AI model poisoning attacks compromise hazard detection accuracy	2	5	Adversarial inputs could degrade safety-critical AI performance	Implement adversarial training and model validation protocols	10	Medium	Product Owner	≥90% performance target		
Security	S4	Insecure API endpoints allow unauthorized access to vehicle control systems	3	4	IoT connectivity creates multiple attack vectors	Secure API design with authentication, authorization, and rate limiting	12	Medium	Product Owner	≥90% performance target		
Adoption	A1	Rider resistance to AI safety features leads to reduced usage and revenue loss	3	3	User acceptance critical for safety feature effectiveness	User education campaigns and gradual feature rollout with feedback	9	Medium	Product Owner	≤10% user complaint rate		
Adoption	A2	Cities reject AI-powered micromobility due to algorithmic accountability concerns	2	5	Regulatory approval essential for market access	Proactive engagement with regulators and transparent governance frameworks	10	Medium	Product Owner	≥4.0/5 user satisfaction		
Adoption	A3	Technical complexity overwhelms operational teams, leading to poor implementation	4	3	AI systems require specialized expertise for effective deployment	Comprehensive training programs and user-friendly management interfaces	12	Medium	Product Owner	≥80% user adoption rate		
Adoption	A4	High implementation costs prevent smaller operators from competing, reducing market diversity	4	3	AI safety becoming competitive requirement may consolidate market	Develop scalable, cost-effective AI solutions and industry partnerships	12	Medium	Product Owner	≤10% user complaint rate		
Privacy	P5	Location data aggregation reveals sensitive user movement patterns and personal habits	4	4	Micromobility AI systems track precise location data for safety recommendations	Implement differential privacy, data minimization, and user consent controls	16	High	Security Team	≥99% data anonymization compliance		
Privacy	P6	Third-party data sharing agreements expose user location data without explicit consent	3	5	Integration with city infrastructure and partner services requires data sharing	Establish strict data sharing agreements and consent management systems	15	High	Privacy Officer	100% consent tracking accuracy		
Adoption	A7	Users lose trust in AI safety recommendations due to perceived algorithmic bias	4	4	User trust is critical for safety compliance and platform adoption	Implement transparent bias testing and user feedback mechanisms	16	High	Product Owner	≥75% user trust score		
Adoption	A8	Complex AI explanations reduce user engagement and safety compliance	3	3	Users need to understand AI recommendations to follow safety guidance	Design simple, intuitive explanation interfaces with user testing	9	Medium	UX Team	≤15 sec explanation comprehension time		