**Risk Management Table**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Risk ID** | **Risk Description** | **Probability** | **Impact** | **Risk Score (P × I)** | **Category** | **Mitigation Strategy** |
| R001 | Database connection failure. | Medium (2) | High (3) | 6 | Technical | Implement connection retries and fallback; monitor DB uptime with alerts. |
| R002 | Server downtime during deployment. | Medium (2) | High (3) | 6 | Deployment | Schedule deployments during off-peak hours; use Docker rollback if failure occurs. |
| R003 | User data privacy breach. | Low (1) | High (3) | 3 | Security | Use HTTPS, sanitize inputs, and enforce secure password policies and encryption. |
| R004 | Payment gateway failure. | Low (1) | High (3) | 3 | External Dependency | Set up alerts, integrate backup gateway if primary fails. |
| R005 | High traffic overload during peak hours. | Medium (2) | Medium (2) | 4 | Performance | Enable auto-scaling; use caching mechanisms to balance load. |
| R006 | Bugs in new feature releases. | Medium (2) | Medium (2) | 4 | Development | Perform unit & integration tests; deploy to staging before production. |
| R007 | Team member unavailability near deadlines. | Medium (2) | Medium (2) | 4 | Organizational | Cross-train team members; maintain buffer time in project timeline. |
| R008 | Outdated third-party libraries. | High (3) | Medium (2) | 6 | Maintenance | Regularly audit dependencies; schedule periodic updates and security checks. |