Algorithmic Trading Risk Register

| **Risk Description** | **Impact Description** | **Probability Level** | **Priority Level** | **Mitigation Notes** | **Owner** |
| --- | --- | --- | --- | --- | --- |
| *Brief summary of the risk* | *What will happen if the risk is not mitigated or eliminated* | *Rate 1(LOW) to 5 (HIGH)* | *(Impact X Probability) Address highest first* | *What can be done to lower or eliminate the impact or probability* | *Who’s responsible?* |
| The API service is no longer available | Data will not be updated. | 1 | 5 | Implement support for multiple data sources | Data analyst, Developer |
| IONOS hosting is no longer available | The system will be inaccessible | 1 | 20 | Keep a working version of the System and User Interface to host elsewhere if required |  |
| Data corruption | Valuable data is potentially lost | 2 | 10 | Create backups of the database. Log insertion processes. Establish database replication procedures | Database administrator |
| Exceed API rate limit | Data may not be recorded | 1 | 5 | Audit the real time data stored periodically, and system logging procedures | Developer |
| API Key breached | Compromise of sensitive information | 1 | 10 | Secure Key Management Practices | Developer |
| Unauthorized PhpMyAdmin access | Manipulation of data, or disruption of database operations from unauthorized users | 1 | 10 | Implement strong password policies. Implement multi-factor authentication (if supported by the host environment). | Database administrator |
| Scheduled tasks in system components fail to run | Can result in failure to collect data or failure of all system components | 2 | 10 | Implement system logging and alerts for failed tasks. Adopt redundancy procedures to automatically reschedule or investigate failed tasks. | Developer, Database Administrator, Data Administrator |
| Unauthorized access by regular users to sensitive pages (Configuration & Job Scheduling) | Potential execution of unauthorized operations | 1 | 10 | Implement strong password policies, user authentication, and access level security | Developer, Data Administrator |
| Possible corruption of configuration files suring change processes | Valuable data is potentially lost | 2 | 10 | Establish a robust backup system for the database to prevent data loss | Developer, Database Administrator |
| Connection to the database is lost/interrupted | Risk of compromised data integrity through dirty reads or writes | 2 | 10 | Implement a backup server to ensure continuous availability | Developer, Database Administrator |