# Security Policy

==========

| Security Feature | Benefit | Description |
|---|---|---|
| Environment Variables | Secure Configuration | Uses environment variables to manage sensitive configurations securely. |
| No Telemetry | Enhanced Privacy | Prioritizes user privacy by not collecting telemetry data. |
| Data Encryption | Data Protection | Encrypts sensitive data to protect it from unauthorized access. |
| Authentication | Access Control | Ensures that only authorized users can access the system. |
| Authorization | Fine-grained Access | Provides specific access rights to users based on roles and permissions. |
| Dependency Security | Reduced Vulnerabilities | Securely manages dependencies to prevent vulnerabilities. |
| Secure Installation | Integrity Assurance | Ensures the integrity of the software through verified sources and checksums. |
| Regular Updates | Ongoing Protection | Keeps the system secure by regularly updating to patch vulnerabilities. |
| Logging and Monitoring | Operational Oversight | Tracks system activity for security monitoring and anomaly detection. |
| Error Handling | Robust Security | Manages errors securely to prevent |

leakage of sensitive information. |

| Data Storage Security | Secure Data Handling | Stores data securely, ensuring confidentiality and integrity. |

| Data Transmission Security | Secure Data Transfer | Protects data during transit from eavesdropping and tampering. |

| Access Control Mechanisms | Restricted Access | Limits system access to authorized personnel only. |

| Vulnerability Management | Proactive Protection | Identifies and mitigates security vulnerabilities effectively. |

| Regulatory Compliance | Legal Conformity | Ensures that the system adheres to relevant legal and regulatory standards. |

| Security Audits |

# Reporting a Vulnerability

---

* * * * *

If you discover a security vulnerability in any of the above versions, please report it immediately to our security team by sending an email to kye@apac.ai. We take security vulnerabilities seriously and appreciate your efforts in disclosing them responsibly.

Please provide detailed information on the vulnerability, including steps to reproduce, potential impact, and any known mitigations. Our security team will acknowledge receipt of your report within 24 hours and will provide regular updates on the progress of the investigation.

Once the vulnerability has been thoroughly assessed, we will take the necessary steps to address it. This may include releasing a security patch, issuing a security advisory, or implementing other appropriate mitigations.

We aim to respond to all vulnerability reports in a timely manner and work towards resolving them as quickly as possible. We thank you for your contribution to the security of our software.

Please note that any vulnerability reports that are not related to the specified versions or do not provide sufficient information may be declined.