




## Security Policy

---

### Supported Versions

---

We actively support the following versions with security updates:

Version	Supported
2.x.x	 Yes
1.x.x	 Yes
< 1.0	 No

### Reporting a Vulnerability

---

We take security vulnerabilities seriously. If you discover a security vulnerability, please follow these steps:

#### Contact Information

- **Email:** [security@agent-orchestration-ops.com](mailto:security@agent-orchestration-ops.com)
- **PGP Key:** [Download our PGP key](#) (./security/pgp-key.asc)
- **Response Time:** We aim to respond within 24 hours

#### What to Include

When reporting a vulnerability, please include:

1. **Description:** Clear description of the vulnerability
2. **Impact:** Potential impact and severity assessment
3. **Reproduction:** Step-by-step instructions to reproduce
4. **Environment:** Affected versions and configurations
5. **Evidence:** Screenshots, logs, or proof-of-concept code
6. **Suggested Fix:** If you have ideas for remediation

#### Process

1. **Initial Response** (24 hours): We'll acknowledge receipt
2. **Investigation** (1-7 days): We'll investigate and validate
3. **Resolution** (varies): We'll develop and test a fix
4. **Disclosure** (coordinated): We'll coordinate public disclosure
5. **Recognition:** We'll credit you in our security advisories

### Security Measures

---

#### Authentication & Authorization

- Multi-factor authentication required for all admin accounts

- Role-based access control (RBAC) implemented
- Regular access reviews and privilege audits
- API key rotation and management

## **Data Protection**

- Encryption at rest and in transit (TLS 1.3+)
- Regular security assessments and penetration testing
- Data classification and handling procedures
- Privacy by design principles

## **Secure Development**

- Security code reviews for all changes
- Automated security scanning in CI/CD pipeline
- Dependency vulnerability monitoring
- Container security scanning

## **Monitoring & Incident Response**

- 24/7 security monitoring and alerting
- Incident response plan and procedures
- Regular security training for team members
- Compliance with industry standards

## **Security Testing**

---

We encourage responsible security research and testing:

### **Allowed Activities**

- Testing on your own instances
- Automated scanning with reasonable rate limits
- Social engineering of our team members (with prior consent)
- Physical security testing of our facilities (with prior arrangement)

### **Prohibited Activities**

- Testing on production systems without permission
- Accessing or modifying user data
- Denial of service attacks
- Spam or phishing attacks
- Violating privacy of users or employees

## **Recognition**

---

We maintain a security hall of fame to recognize researchers who help improve our security:

### **Hall of Fame**

- [Researcher Name] - [Vulnerability Type] - [Date]
- [Researcher Name] - [Vulnerability Type] - [Date]

## Rewards

While we don't currently offer monetary rewards, we provide:

- Public recognition in our security advisories
- Listing in our security hall of fame
- Direct communication with our security team
- Swag and merchandise (when available)

## Security Resources

---

### Useful Links

- [OWASP Top 10](https://owasp.org/www-project-top-ten/) (<https://owasp.org/www-project-top-ten/>)
- [CWE/SANS Top 25](https://cwe.mitre.org/top25/) (<https://cwe.mitre.org/top25/>)
- [NIST Cybersecurity Framework](https://www.nist.gov/cyberframework) (<https://www.nist.gov/cyberframework>)

### Documentation

- [Security Architecture](#) ([./docs/security-architecture.md](#))
- [Threat Model](#) ([./docs/threat-model.md](#))
- [Incident Response Plan](#) ([./docs/incident-response.md](#))
- [Security Training](#) ([./docs/security-training.md](#))

## Emergency Contact

---

For critical security incidents requiring immediate attention:

- **Emergency Email:** [security-emergency@agent-orchestration-ops.com](mailto:security-emergency@agent-orchestration-ops.com)
- **Phone:** +1-XXX-XXX-XXXX (24/7 security hotline)
- **Escalation:** Contact our CEO directly for critical issues

## Policy Updates

---

This security policy is reviewed and updated quarterly. Last updated: [Current Date]

For questions about this policy, contact: [security-policy@agent-orchestration-ops.com](mailto:security-policy@agent-orchestration-ops.com)

---

**Remember:** Security is everyone's responsibility. If you see something, say something.