Security Policy

🛡️ Security Overview

This document outlines the security policies and procedures for the agent-orchestration-ops repository. We take security seriously and appreciate your help in keeping our project secure.

📋 Supported Versions

We provide security updates for the following versions:

Version	Supported
1.x.x	✅ Yes
0.9.x	✅ Yes
< 0.9	❌ No

🚨 Reporting a Vulnerability

Immediate Response Required

If you discover a security vulnerability, please report it immediately through one of these channels:

1. **GitHub Security Advisories** (Preferred)
   - Go to the repository's Security tab
   - Click "Report a vulnerability"
   - Fill out the security advisory form

2. **Email** (For sensitive issues)
   - Send details to: security@empire325marketing.com
   - Use PGP encryption if possible
   - Include "SECURITY VULNERABILITY" in the subject line

3. **Private Issue** (For less sensitive issues)
   - Create a private issue in the repository
   - Tag it with the "security" label

What to Include

When reporting a vulnerability, please include:

- **Description**: Clear description of the vulnerability
- **Impact**: Potential impact and attack scenarios
- **Reproduction**: Step-by-step instructions to reproduce
- **Environment**: Affected versions, configurations, or environments
- **Mitigation**: Any temporary workarounds you've identified
- **Evidence**: Screenshots, logs, or proof-of-concept code (if safe to share)

Response Timeline

We are committed to responding to security reports promptly:

- **Initial Response**: Within 24 hours
- **Assessment**: Within 72 hours
- **Status Update**: Weekly until resolved
- **Resolution**: Target 30 days for critical issues, 90 days for others

🔒 Security Measures

Code Security

- **Static Analysis**: Automated security scanning on all commits
- **Dependency Scanning**: Regular vulnerability checks for dependencies
- **Secret Scanning**: Automated detection of exposed secrets
- **Code Review**: All changes require security-focused code review

Infrastructure Security

- **Access Control**: Principle of least privilege for all access
- **Encryption**: Data encrypted in transit and at rest
- **Monitoring**: Continuous security monitoring and alerting
- **Backup**: Secure, encrypted backups with tested recovery procedures

CI/CD Security

- **Secure Pipelines**: Security checks integrated into CI/CD workflows
- **Environment Isolation**: Separate environments for development, staging, and production
- **Secret Management**: Secure handling of secrets and credentials
- **Deployment Gates**: Security approvals required for production deployments

🎯 Security Best Practices

For Contributors

1. **Never commit secrets** (API keys, passwords, tokens)
2. **Use secure coding practices** (input validation, output encoding)
3. **Keep dependencies updated** (regularly update to latest secure versions)
4. **Follow authentication best practices** (strong passwords, 2FA)
5. **Validate all inputs** (sanitize and validate user inputs)
6. **Use HTTPS everywhere** (secure communication channels)

For Users

1. **Keep software updated** (use latest versions with security patches)
2. **Use strong authentication** (complex passwords, multi-factor authentication)
3. **Monitor for suspicious activity** (review logs and access patterns)
4. **Follow principle of least privilege** (minimal necessary permissions)
5. **Regular security audits** (periodic security assessments)

🔍 Security Monitoring

Automated Monitoring

- **Vulnerability Scanning**: Daily scans for known vulnerabilities
- **Dependency Monitoring**: Automated alerts for vulnerable dependencies
- **Secret Detection**: Continuous monitoring for exposed secrets
- **Compliance Checking**: Regular compliance validation

Manual Reviews

- **Security Audits**: Quarterly comprehensive security reviews
- **Penetration Testing**: Annual third-party security assessments
- **Code Reviews**: Security-focused review of all code changes
- **Access Reviews**: Regular review of user access and permissions

📚 Security Resources

Documentation

- OWASP Top 10 (https://owasp.org/www-project-top-ten/)
- NIST Cybersecurity Framework (https://www.nist.gov/cyberframework)
- GitHub Security Best Practices (https://docs.github.com/en/code-security)

Tools and Services

- **Static Analysis**: CodeQL, Semgrep, Bandit
- **Dependency Scanning**: Dependabot, Snyk, Safety
- **Secret Scanning**: TruffleHog, GitLeaks
- **Infrastructure Security**: Checkov, TFSec, Terrascan

🏛️ Compliance

Standards and Frameworks

We align with the following security standards:

- **SOC 2 Type II**: Security, availability, and confidentiality controls
- **ISO 27001**: Information security management system
- **NIST Framework**: Cybersecurity risk management
- **GDPR**: Data protection and privacy requirements

Certifications

- Regular third-party security assessments
- Compliance audits and certifications
- Continuous monitoring and improvement

🚀 Incident Response

Response Team

- **Security Lead**: Primary security contact

- **DevOps Team**: Infrastructure and deployment security
- **Development Team**: Application security and code fixes
- **Management**: Executive oversight and communication

Response Process

1. **Detection**: Identify and validate security incident
2. **Containment**: Isolate and contain the threat
3. **Investigation**: Analyze the incident and determine impact
4. **Eradication**: Remove the threat and fix vulnerabilities
5. **Recovery**: Restore systems and monitor for recurrence
6. **Lessons Learned**: Document and improve security measures

Communication

- **Internal**: Immediate notification to security team and management
- **External**: Timely notification to affected users and stakeholders
- **Public**: Transparent communication about resolved issues
- **Regulatory**: Compliance with legal notification requirements

📞 Contact Information

Security Team

- **Primary Contact**: security@empire325marketing.com
- **Emergency Contact**: +1-XXX-XXX-XXXX (24/7 security hotline)
- **PGP Key**: Available at keybase.io/empire325security

Business Hours

- **Standard Response**: Monday-Friday, 9 AM - 5 PM EST
- **Emergency Response**: 24/7 for critical security issues
- **Escalation**: Automatic escalation for high-severity issues

📝 Security Policy Updates

This security policy is reviewed and updated regularly:

- **Quarterly Reviews**: Regular policy review and updates
- **Incident-Driven Updates**: Updates based on security incidents
- **Compliance Updates**: Updates to maintain compliance requirements
- **Community Feedback**: Incorporation of community suggestions

Version History

- **v1.0** (2025-09-29): Initial comprehensive security policy
- **v0.9** (2025-09-15): Basic security guidelines
- **v0.8** (2025-09-01): Initial security documentation

Last Updated: September 29, 2025

Next Review: December 29, 2025

Policy Owner: Empire325Marketing Security Team