Security Policy

Overview

This document outlines the security policies and procedures for the agent-orchestration-ops repository. We take security seriously and are committed to ensuring the safety and integrity of our systems and data.

Supported Versions

We provide security updates for the following versions:

Version	Supported
0.2.x	:white_check_mark:
0.1.x	:white_check_mark:
< 0.1	:x:

Reporting a Vulnerability

Responsible Disclosure

We encourage responsible disclosure of security vulnerabilities. If you discover a security issue, please follow these steps:

1. **Do not** create a public GitHub issue for security vulnerabilities
2. Send an email to our security team at: `security@empire325marketing.com`
3. Include detailed information about the vulnerability
4. Allow us reasonable time to respond and address the issue

What to Include

When reporting a vulnerability, please include:

- **Description**: Clear description of the vulnerability
- **Impact**: Potential impact and severity assessment
- **Reproduction**: Step-by-step instructions to reproduce the issue
- **Environment**: System information, versions, and configuration details
- **Evidence**: Screenshots, logs, or proof-of-concept code (if applicable)

Response Timeline

- **Initial Response**: Within 24 hours of report
- **Assessment**: Within 72 hours of report
- **Resolution**: Based on severity (see timeline below)

Severity	Response Time	Resolution Time
Critical	2 hours	24 hours
High	4 hours	72 hours
Medium	24 hours	1 week
Low	72 hours	2 weeks

Security Measures

Access Control

- **Multi-Factor Authentication (MFA)**: Required for all team members
- **Role-Based Access Control (RBAC)**: Principle of least privilege
- **Regular Access Reviews**: Quarterly access audits
- **Automated Deprovisioning**: Immediate access removal upon role changes

Code Security

- **Static Code Analysis**: Automated security scanning in CI/CD
- **Dependency Scanning**: Regular vulnerability assessments of dependencies
- **Code Reviews**: Mandatory peer review for all changes
- **Branch Protection**: Protected branches with required status checks

Infrastructure Security

- **Encryption**: All data encrypted in transit and at rest
- **Network Security**: Secure network configurations and monitoring
- **Logging and Monitoring**: Comprehensive audit logging
- **Incident Response**: 24/7 security monitoring and response

Data Protection

- **Data Classification**: Sensitive data properly classified and protected
- **Data Retention**: Automated data lifecycle management
- **Backup Security**: Encrypted backups with tested recovery procedures
- **Privacy Compliance**: GDPR and other privacy regulation compliance

Security Controls

Authentication

- **Strong Passwords**: Minimum 12 characters with complexity requirements
- **Multi-Factor Authentication**: TOTP or hardware tokens required
- **Session Management**: Secure session handling with timeout policies
- **API Authentication**: Token-based authentication with rotation

Authorization

- **Principle of Least Privilege**: Minimal required permissions
- **Role-Based Access**: Defined roles with specific permissions

- **Resource-Level Controls**: Granular access controls
- **Regular Permission Audits**: Quarterly access reviews

Monitoring and Logging

- **Security Event Logging**: Comprehensive audit trails
- **Real-Time Monitoring**: 24/7 security monitoring
- **Anomaly Detection**: Automated threat detection
- **Incident Response**: Defined response procedures

Compliance and Standards

Frameworks

- **SOC 2 Type II**: Security and availability controls
- **ISO 27001**: Information security management
- **NIST Cybersecurity Framework**: Risk-based security approach
- **GDPR**: Data protection and privacy compliance

Regular Assessments

- **Vulnerability Assessments**: Monthly automated scans
- **Penetration Testing**: Annual third-party testing
- **Security Audits**: Quarterly internal audits
- **Compliance Reviews**: Annual compliance assessments

Incident Response

Response Team

- **Security Lead**: Primary incident coordinator
- **Technical Lead**: System and application expertise
- **Communications Lead**: Internal and external communications
- **Legal Counsel**: Regulatory and legal guidance

Response Process

1. **Detection and Analysis**
   - Incident identification and classification
   - Impact assessment and severity rating
   - Evidence collection and preservation

2. **Containment and Eradication**
   - Immediate threat containment
   - Root cause analysis
   - Threat elimination and system hardening

3. **Recovery and Post-Incident**
   - System restoration and validation
   - Monitoring for recurring issues
   - Lessons learned and process improvement

Communication

- **Internal Notifications**: Immediate team notification
- **Management Reporting**: Executive briefings
- **Customer Communications**: Transparent customer updates
- **Regulatory Reporting**: Compliance with notification requirements

Security Training

Required Training

- **Security Awareness**: Annual training for all personnel
- **Secure Coding**: Developer-specific security training
- **Incident Response**: Response team training and exercises
- **Compliance Training**: Role-specific compliance requirements

Ongoing Education

- **Security Updates**: Regular security bulletins and updates
- **Threat Intelligence**: Current threat landscape briefings
- **Best Practices**: Industry security best practices
- **Certification Support**: Professional security certifications

Third-Party Security

Vendor Management

- **Security Assessments**: Vendor security evaluations
- **Contractual Requirements**: Security clauses in contracts
- **Ongoing Monitoring**: Regular vendor security reviews
- **Incident Coordination**: Joint incident response procedures

Supply Chain Security

- **Dependency Management**: Regular dependency updates
- **Source Code Verification**: Integrity checks for third-party code
- **License Compliance**: Open source license management
- **Vulnerability Monitoring**: Continuous dependency scanning

Contact Information

Security Team

- **Primary Contact**: security@empire325marketing.com
- **Emergency Contact**: +1-XXX-XXX-XXXX (24/7 hotline)
- **PGP Key**: [Security Team Public Key]

Escalation Contacts

- **Security Manager**: security-manager@empire325marketing.com
- **Chief Information Security Officer**: ciso@empire325marketing.com
- **Legal Counsel**: legal@empire325marketing.com

Security Resources

Documentation

- Security Architecture Guide (./security/architecture.md)
- Incident Response Playbook (./security/incident-response.md)
- Security Configuration Standards (./security/configuration-standards.md)
- Data Classification Guide (./security/data-classification.md)

Tools and Services

- **Vulnerability Scanner**: [Internal vulnerability management system]
- **SIEM Platform**: [Security information and event management]
- **Threat Intelligence**: [Threat intelligence feeds and analysis]
- **Security Training**: [Security awareness training platform]

Updates and Changes

This security policy is reviewed and updated regularly to ensure it remains current and effective.

- **Last Updated**: 2025-09-29
- **Next Review**: 2025-12-29
- **Version**: 1.0
- **Approved By**: Security Team

For questions about this security policy, please contact our security team at security@empire325marketing.com.

This document is part of our comprehensive security program and is regularly updated to reflect current best practices and regulatory requirements.