DoctorLogic Security & Reliability Policy

LAST REVISION DATE:

11/3/2025

DOCUMENT OWNER:

William Hyde, VP Technology / Security & Privacy Officer

VERSION: 1.0

1. INTRODUCTION

1.1 Purpose

This policy defines the service commitments, performance standards, security requirements, and operational responsibilities that DoctorLogic, LLC (“DL” or “Service Provider”) shall provide. This agreement establishes measurable service levels, monitoring requirements, incident response protocols, and accountability mechanisms to ensure reliable, secure, and compliant service delivery.

1.2 Scope

This policy applies to all services provided by DL, including but not limited to:

- Web application hosting and infrastructure services
- API services and integrations
- Data storage and processing systems
- Security monitoring and incident response
- Technical support services
- Disaster recovery and business continuity services

1.3 Applicable Regulations

Services provided under this agreement shall comply with:

- Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health (HITECH) Act
- Applicable state and federal data protection regulations

1.4 Agreement Term

This policy shall remain in effect for the duration of the service contract between DL and Client, and shall be reviewed and updated annually or as needed to reflect changes in security, service delivery, technology, or regulatory requirements.DL reserves the right to amend or update any part of this agreement without prior consent of Client. However, if DL makes material changes to any part of this agreement which results in a significant modification to agreed upon SLA’s, DL shall notify Client of such changes and provide a reasonable period to review and provide feedback. The final decision of what changes are incorporated into the document shall lie solely with DL.

DL agrees to adhere to all policies stated in this agreement.

2. AVAILABILITY & PERFORMANCE

2.1 Uptime Commitments

DL commits to maintaining a minimum infrastructure uptime of **99.95%** for production services, measured monthly.

Calculation Method:

- Uptime % = ((Total Minutes in Month - Downtime Minutes) / Total Minutes in Month) × 100
- Downtime minutes excludes scheduled maintenance windows

Exclusions from Downtime:

- Scheduled maintenance windows
- Outages caused by third-party networks or internet service providers beyond DL's control
- Failures in client-controlled software, configurations, or integrations
- Performance degradation where the service remains accessible, even if slower than normal
- Force majeure events

2.2 Maintenance Windows

Regular Maintenance Schedule:

- **Frequency:** Weekly maintenance windows
- **Timing:** Business days between 9:00 PM and 12:00 AM Central Standard Time (CST)
- **Advance Notice:** Minimum 48 hours advance notice for all scheduled maintenance via in-app messaging
- **Communication:** Maintenance notices shall be provided via in app notices or email

Emergency Maintenance: May be performed outside scheduled windows for critical security patches or system failures. Best effort notification will be provided when circumstances permit.

2.3 Performance Standards

DL utilizes industry standard and recognized applications/tools to monitor the items listed in this section.

2.3.1 Core Web Vitals

DL shall maintain the following **Core Web Vitals** thresholds for core platform infrastructure, application code, and DL-managed integrations:

Metric	Target	Measurement
Largest Contentful Paint (LCP)	≤ 2.5 seconds	75th percentile
First Input Delay (FID)	≤ 100 milliseconds	75th percentile
Cumulative Layout Shift (CLS)	≤ 0.1	75th percentile
Interaction to Next Paint (INP)	≤ 200 milliseconds	75th percentile

In cases where CWV is unavailable via PageSpeed Insights, Cloudflare CWV will be used. CWV is calculated on a 28-day rolling average to ensure all data is coming from DL site and not prior vendor.

Performance degradation caused by Client required third-party components or integrations will not constitute a breach of service levels.

2.3.2 API Performance

Performance sla's to be added upon initial launch of public facing api's.

2.3.3 Content Delivery Network (CDN)

CDN Performance Standards: - **Cache hit ratio:** ≥ 90% - **CDN edge response time:** ≤ 100 milliseconds (p95)

Exclusions include dynamic content pages, such as finders, filter states, etc.

2.3.4 Performance Monitoring

- Continuous monitoring of all performance metrics using industry-standard tools
- Real-time alerting when thresholds are exceeded

3. SECURITY & COMPLIANCE

3.1 24/7 Security Monitoring

Security Operations Center (SOC):

- **24/7/365 monitoring** of all production systems and infrastructure
- Real-time threat detection and automated alerting

Monitoring Scope:

- Network traffic and firewall logs
- Application security events
- Authentication and access logs
- System integrity and file changes
- Database activity monitoring
- Cloud infrastructure events

3.2 Independent Security Assurance

3.2.1 HIPAA Compliance

- Annual third-party HIPAA compliance assessment
- Business Associate Agreements (BAA) maintained in accordance with HIPAA requirements
- Documentation of all HIPAA-required safeguards (administrative, physical, and technical)
- Annual HIPAA security and privacy attestation provided to Client on request

3.3 Data Loss Prevention (DLP)

DLP Controls:

- Data is encrypted In Transit and at Rest.
- NSG controls to allow privileged access

Data Classification:

- Encryption enforced for all PHI at rest and in transit. See section on Encryption Standards for details.

3.4 Endpoint & Infrastructure Hardening

Endpoint Detection and Response (EDR):

- EDR solutions deployed on all servers, containers, and endpoints
- Real-time threat detection and automated response capabilities

Security Baselines:

- Configuration drift reviewed and prioritized for remediation based on priority

Access Control:

- Multi-factor authentication (MFA) required for all administrative access to infrastructure
- Principle of least privilege enforced
- Role-based access control (RBAC) implemented
- Quarterly user access reviews

3.5 Encryption Standards

Data at Rest:

- Databases that handle PHI and file storage use TDE with AES-256 encryption
- Full disk encryption on all servers and workstations
- Hardware Security Module (HSM) or cloud-native key management for encryption keys

Data in Transit:

- TLS 1.3 encryption for all web applications and APIs
- Secure FTP (SFTP) or encrypted alternatives for file transfers
- VPN required for all remote administrative access

3.6 Network Architecture Security Controls

Perimeter Controls:

- Cloudflare WAF
- Azure Application Gateway
- Network Security Groups (NSGs)

Access Management:

- Subnets
- Private Endpoints

Monitoring & Detection:

- Cloudflare DDoS Protection

3.7 Sub-processors

DL uses the third-part entities below to process data on behalf of Clients in accordance between DL and the sub-processor.

Sub-processor	Nature and Purpose of Processing	Categories of Personal Data	Location of Processing

Microsoft Azure	Cloud hosting and infrastructure provider	Customer Personal Data created by customer and stored in applicable services	United States, South Central region
Microsoft SQL Server	Database management and storage	Customer Personal Data, transaction data, application data	United States, South Central region, Geo-retention for data storage
CData	Data connectivity and integration services	Customer GA4 data synchronized across system	United States, South Central region
CallTrackingMetrics	Call tracking and analytics services	Customer contact information, call recordings, call metadata	United States
Google Analytics 4 (GA4)	Analytics and usage tracking	Usage data, anonymized user behavior data	United States
Google Business Profile	Business listing and customer engagement	Business information, customer reviews, engagement data	United States
Google Maps	Mapping and location services	Location data, address information	United States
Cloudflare	Content delivery network and security services	Customer Personal Data in transit, security logs	Global Network
Datadog	APM monitoring and logging	Application logs, performance metrics, error data	United States
Hyperping	Uptime monitoring and alerting services	Service availability data, performance metrics, alert notifications	United States
GTranslate	Website translation and localization services	Website content, user language preferences	France, United States

4. INCIDENT MANAGEMENT

4.1 Major Incident Response Categories

- **Security Incidents:** Cyber attacks, data breaches, unauthorized access
- **Service Incidents:** Outages, performance degradation, functionality failures
- **Data Incidents:** Data loss, corruption, or integrity issues

4.2 Incident Response Severity Levels

Severity	Description	Remediation Timeline
P1 - Critical	Service outage, data breach, active cyber attack	8 hours
P2 - High	Significant degradation, security vulnerability	24 hours

4.3 Vulnerability Management

Vulnerability Scanning:

- Continuous automated vulnerability scanning of all production systems
- Annual vulnerability assessment reports provided to Client on request

Vulnerability Remediation SLAs:

Severity	Remediation Timeline
Critical	≤ 24 hours
High	≤ 72 hours
Medium	≤ 7 days
Low	≤ 30 days

Severity and timeline are determined at the discretion of DL, taking into account the nature of the vulnerability, potential exposure, likelihood of exploitation, and impact on functionality and operations.

4.4 Notification Requirements

Internal Escalation:

- Immediate notification to DL Security & Privacy Officer for P1/P2 incidents
- Escalation to CTO and executive team for P1 incidents
- Incident response team assembled within 30 minutes for P1 incidents

Client Notification:

- **P1 Incidents:** Initial notification in-app or via email within 1 hour of detection
- **P2 Incidents:** Initial notification in-app or via email within 4 business hours of detection
- **Data Breach:** Initial notification in accordance with HIPAA/HITECH requirements (see Section 4.6)

Progress/Resolution Updates:

- **P1 Incidents:** DL will communicate updates to clients every 60 minutes via in-app messaging or email

4.5 Root Cause Analysis (RCA)

All incidents shall receive formal Root Cause Analysis including:

RCA Components:

- **Incident Timeline:** Detailed chronology of events
- **Root Cause Identification:** Technical and procedural causes
- **Impact Assessment:** Affected systems, data, and users
- **Containment Actions:** Steps taken to resolve incident
- **Preventive Measures:** Recommendations to prevent recurrence
- **Action Items:** Specific tasks with owners and deadlines

RCA Delivery:

- P1 incidents: RCA available upon request within 3 business days of resolution
- P2 incidents: RCA available upon request within 5 business days of resolution
- Review meeting scheduled with Client stakeholders upon request

4.6 Data Breach & Exfiltration Response

Detection & Response:

- Immediate containment of suspected exfiltration
- Notification and target response upon determination an incident has occurred

Target Response Times for Data Exfiltration Events:

Action	Target Time
Initial Assessment	≤ 30 minutes
Containment	≤ 4 hours
Impact Analysis	≤ 8 hours
Client Notification	≤ 4 hours

Action	Target Time
Regulatory Notification Planning	≤ 24 hours

HIPAA Breach Notification:

- Assessment completed within 24 hours to determine if HIPAA breach has occurred
- Notification to affected individuals within 60 days as required by law
- HHS notification for breaches affecting 500+ individuals
- Documentation maintained per HIPAA requirements

5. DISASTER RECOVERY & BUSINESS CONTINUITY

Following any system failure or unplanned outage, DoctorLogic will restore all affected systems to their operational state immediately prior to the incident. This includes:

- Backend databases and application data
- Frontend presentation layer components (templates, media assets, custom design elements)
- Site-specific configurations and customizations

All restored systems must pass automated validation checks comparing post-recovery state against pre-outage baselines before returning to production. Sites will remain in maintenance mode until validation confirms complete restoration integrity.

5.1 Recovery Objectives

Recovery Time Objective (RTO):

- **Production Services:** ≤ 1 hour
  - Websites, including assets and data functions
- **Non-Critical Services:** ≤ 24 hours
  - Premium Call Tracking, GA4, etc
- **Support Systems:** ≤ 24 hours

Recovery Point Objective (RPO):

- **Critical Databases:** ≤ 1 hour
- **Application Data:** ≤ 1 hour
- **Configuration Data:** ≤ 24 hours

5.2 Backup & Data Resilience

Backup Schedule:

Data Type	Frequency	Retention Period
Production Databases	Hourly (logs)	30 days
Full Database Backups	Daily	90 days

Backup Infrastructure:

- **Immutable Backups:** Write-once-read-many (WORM) storage preventing deletion or modification
- **Geographic Redundancy:** Backups stored in multiple Azure regions
- **Encryption:** All backups encrypted with AES-256

Backup Storage Locations:

- Primary: Microsoft Azure (South Central region)
- Secondary: Microsoft Azure (geo-redundant region)

5.3 Hosting & Infrastructure

Cloud Infrastructure:

- **Primary Hosting:** Microsoft Azure
- **Geo-Retention:** Data replicated across Azure regions for disaster recovery
- **Availability Zones:** Services deployed across multiple availability zones

Database Infrastructure:

- VM SQL Database - Azure South Central Region
- HA failover groups configured
- Point-in-time restore capability

Assets Infrastructure:

- Assets Primary: Azure South Central Region
- Failover load balanced set
- Continuous back to failover; hourly backup to non-production server; nightly backup to geo-redundant storage

Design and Code:

- Code base utilizes Gitlab
- Local back ups on development machines

5.4 Business Continuity Planning

Disaster Recovery Plan:

- Comprehensive written DR plan maintained and updated quarterly
- Plan includes detailed recovery procedures for all critical systems
- Contact information for emergency response team maintained
- Copies stored securely both off-site

Annual Tabletop Exercise:

- Full disaster recovery tabletop exercise conducted annually
- Scenarios include natural disasters, cyber attacks, and infrastructure failures
- Results documented with action items and improvement plans

Disaster Recovery Service Level Agreements:

- **Minimal environment setup time:** ≤ 1 hours
- **Fully operational environment restoration:** ≤ 24 hours
- These SLAs apply to infrastructure components supporting production services

6. MONITORING & REPORTING

6.1 Continuous Monitoring

Infrastructure Monitoring:

- 24/7 monitoring of server health, performance, and availability
- Network traffic analysis and anomaly detection
- Application performance monitoring (APM)
- Database performance and query optimization
- Storage capacity and performance monitoring

Security Monitoring:

- File integrity monitoring (FIM)
- Log aggregation and analysis
- Threat intelligence integration

Log Retention:

- **Security logs:** 12 months minimum
- **Application logs:** 90 days
- **System logs:** 90 days
- **Audit logs:** 7 years (HIPAA requirement)

7. CHANGE MANAGEMENT

7.1 Change Control Process

Change Categories:

Category	Examples	Testing Required
Standard	Routine patches, minor updates	Staging validation
Normal	Feature releases, configuration changes	Full staging tests
Emergency	Critical security patches, outage remediation	Staging validation when possible, Production validation

7.2 Release Testing & Validation

Staging Environment:

- All changes tested in production-like staging environment
- Performance testing validates no degradation
- Automated testing validates no regressions

Deployment Process:

- Automated deployment pipelines with built-in checks
- Post-deployment validation and monitoring
- Immediate rollback capability maintained

7.3 Maintenance Notice Requirements

Scheduled Maintenance:

- **Minimum 48 hours advance notice** for standard maintenance via in-app messaging
- Notice includes: date/time, expected duration, affected services, expected impact

Emergency Maintenance:

- Best effort advance notice when possible
- Real-time communication during maintenance
- Post-maintenance update explaining necessity and actions taken

8. SUPPORT SERVICES

8.1 Support Availability

Support Channels:

- Email: support@doctorlogic.com
- Phone: 469-458-7101

Support Hours:

- **P1/P2 Support:** 24/7/365
- **P3/P4 Support:** Business hours (8:00 AM - 5:00 PM CST, Monday-Friday)

8.2 Support SLAs

Response & Resolution Targets:

Priority	Description	Response Time	Service Restoration	Resolution Target
P1 - Critical	Production outage, complete service unavailability, data breach	15 minutes	1 hour	1 hours
P2 - High	Significant functionality unavailable, major performance degradation	1 hour	8 hours	24 hours

Response and resolution targets are based upon notification/identification of an issue.
Service Restoration vs. Resolution:

- **Service Restoration:** Implementing a workaround to restore critical functionality when possible
- **Resolution:** Permanent fix addressing root cause

8.3 Support Escalation

DL Escalation Path:

- **Level 1:** Client Support Specialist
- **Level 2:** Product and Engineering (technical escalation)
- **Level 3:** VP Technology / Security & Privacy Officer
- **Level 4:** CTO / Executive Team

Automatic Escalation Triggers:

- P1 incidents not acknowledged within 15 minutes
- P1 incidents not contained within 4 hours
- P2 incidents not responded to within 1 hour

9. COMPLIANCE & ENFORCEMENT

9.1 Continuous Improvement

Quarterly Reviews:

- Review security incidents, policy effectiveness, and compliance
- Identify training needs and policy updates
- Maintain log of security concerns and actions taken

Annual Reviews:

- Comprehensive review of security in and reliability policy
- Update procedures based on lessons learned
- Technology and threat landscape assessment
- Staff training and awareness updates

9.2 Documentation & Records

Required Documentation for Quarterly and Annual Reviews:

- Security incident logs
- Change management logs
- Access control reviews
- Training completion records
- Audit logs (7-year retention for HIPAA)

APPENDIX A: DEFINITIONS

Availability: Data or information is accessible and usable upon demand by an authorized person.

Confidentiality: Data or information is not made available or disclosed to unauthorized persons or processes.

Downtime: Any period during which production services are unavailable or non-functional due to unplanned interruptions.

Integrity: Data or information that has not been altered or destroyed in an unauthorized manner.

PHI (Protected Health Information): Individually identifiable health information in any form or media.

ePHI (Electronic Protected Health Information): PHI in electronic format.

RTO (Recovery Time Objective): Target duration for service restoration after disruption.

RPO (Recovery Point Objective): Maximum acceptable data loss measured in time.

SIEM (Security Information and Event Management): Centralized system for real-time security monitoring.

SOC (Security Operations Center): 24/7 security monitoring and response facility.

APPENDIX B: CONTACT INFORMATION

Yapi/DL Security & Privacy Officer:

- William Hyde
- Email: whyde@doctorlogic.com

Yapi/DL CTO:

- Rachel Handschke
- Email: rachel.handschke@yapicentral.com

Emergency Hotline: 469-458-7101

Support Email: support@doctorlogic.com

Document Version Control:

Version	Date	Author	Changes
1.0	11/3/2025	William Hyde	Initial creation