S Nimbus LLC - ComplianceSeal Service Level Agreement

Company Name: S Nimbus LLC
Principal Place of Business: 1751 Pinnacle DR, Suite 600, McLean, Virginia 22102, USA

RECITALS

WHEREAS, S Nimbus LLC ("Provider", "Company", "We", "Us", or "Our") is a limited liability company duly organized and existing under the laws of the Commonwealth of Virginia, engaged in the business of providing software-as-a-service solutions for compliance, data protection, and regulatory management;

WHEREAS, Customer ("Customer", "Client", "You", or "Your") desires to obtain compliance management services from Provider through the ComplianceSeal platform;

WHEREAS, Provider has developed and maintains a proprietary software platform known as "ComplianceSeal" designed to assist organizations in achieving and maintaining compliance with various regulatory frameworks including but not limited to the General Data Protection Regulation ("GDPR"), California Consumer Privacy Act ("CCPA"), Sarbanes-Oxley Act ("SOX"), and Salesforce Shield compliance requirements;

WHEREAS, the parties desire to establish clear, measurable, and legally binding service level commitments, performance standards, availability guarantees, and remediation procedures governing the provision of ComplianceSeal services;

NOW, THEREFORE, in consideration of the mutual covenants, terms, and conditions contained herein, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties agree as follows:

---

1. DEFINITIONS AND INTERPRETATION

1.1 Definitions

For purposes of this Service Level Agreement, the following terms shall have the meanings ascribed to them below:

"Affiliate" means, with respect to any entity, any other entity that directly or indirectly controls, is controlled by, or is under common control with, such entity.

"Availability" means the percentage of time during any given measurement period that the ComplianceSeal Services are operational and accessible to Customer in accordance with the specifications set forth herein.

"Business Day" means any day that is not a Saturday, Sunday, or a federal holiday recognized by the United States government.

"Business Hours" means 8:00 AM to 6:00 PM Eastern Time on Business Days.

"Confidential Information" means all non-public, proprietary, or confidential information disclosed by one party to another, whether orally, in writing, or in any other form.

"Critical System Failure" means a complete unavailability of the ComplianceSeal Services that prevents Customer from accessing any functionality of the platform.

"Customer Data" means all data, content, and information submitted, uploaded, or otherwise provided by Customer to the ComplianceSeal platform.

"Downtime" means any period during which the ComplianceSeal Services are not available or accessible to Customer, excluding Planned Maintenance and Excused Downtime.

"Excused Downtime" means any downtime caused by factors beyond Provider's reasonable control, including but not limited to Force Majeure Events, third-party service failures, Customer actions or omissions, or internet connectivity issues not within Provider's direct control.

"Force Majeure Event" means any act of God, war, terrorism, epidemic, pandemic, government action, natural disaster, fire, flood, earthquake, labor dispute, or other event beyond a party's reasonable control.

"Incident" means any event that causes or may cause an interruption to or reduction in the quality of the ComplianceSeal Services.

"Planned Maintenance" means scheduled maintenance activities performed by Provider with advance notice to Customer.

"Recovery Point Objective" or "RPO" means the maximum acceptable amount of data loss measured in time from the point of failure.

"Recovery Time Objective" or "RTO" means the maximum acceptable length of time that the ComplianceSeal Services can be unavailable following an unplanned service interruption.

"Service Credits" means monetary credits applied to Customer's account as compensation for Provider's failure to meet the service level commitments specified herein.

"Services" or "ComplianceSeal Services"** means the software-as-a-service platform and related services provided by Provider under the terms of this SLA and the underlying Service Agreement.

1.2 Interpretation

In this SLA, unless the context otherwise requires: (a) references to sections, subsections, and exhibits are references to sections, subsections, and exhibits of this SLA; (b) words importing the singular include the plural and vice versa; (c) words importing gender include all genders; (d) "including" means "including without limitation"; (e) headings are for convenience only and do not affect interpretation; and (f) this SLA shall be construed without regard to any presumption or rule requiring construction against the party drafting the instrument.

---

2. SCOPE AND APPLICABILITY

2.1 Service Overview and Scope

This Service Level Agreement ("SLA") governs the provision of ComplianceSeal services by S Nimbus LLC to Customer and establishes legally binding commitments regarding service availability, performance standards, data protection measures, recovery objectives, and remediation procedures. The ComplianceSeal platform is a comprehensive compliance management system designed to assist organizations in achieving, maintaining, and demonstrating compliance with various regulatory frameworks including but not limited to GDPR, CCPA, SOX, HIPAA, ISO 27001, and Salesforce Shield requirements.

2.2 Incorporation by Reference

This SLA is incorporated by reference into and forms an integral part of the ComplianceSeal End User License Agreement and Master Service Agreement or similar agreement between the parties ("Primary Agreement"). In the event of any conflict between the terms of this SLA and the Primary Agreement, the terms of this SLA shall control solely with respect to service level commitments, availability guarantees, and related remedies.

2.3 Binding Effect

The commitments, obligations, and remedies set forth in this SLA constitute legally binding obligations of Provider and are enforceable in accordance with the dispute resolution procedures specified herein and in the Primary Agreement.

---

3. SERVICE AVAILABILITY COMMITMENTS AND UPTIME GUARANTEES

3.1 Monthly Uptime Commitment

Subject to the terms and conditions of this SLA, Provider hereby commits to maintain the availability of the ComplianceSeal Services in accordance with the following uptime guarantees, measured on a calendar month basis:

Minimum Uptime Guarantee: 99.5% monthly uptime for all production services, calculated as follows:

```
None
Monthly Uptime Percentage = ((Total Minutes in Month - Downtime Minutes) / Total Minutes in Month) × 100
```

Where "Downtime Minutes" excludes Planned Maintenance and Excused Downtime as defined herein.

3.2 Service Availability Tiers and Corresponding Commitments

Provider offers multiple service tiers with differentiated availability commitments and support levels:

Service Tier	Monthly Uptime Commitment	Maximum Allowable Downtime	Incident Response Time	Resolution Target
Standard Tier	99.5%	3 hours 36 minutes	4 Business Hours	8 Business Hours
Professional Tier	99.7%	2 hours 10 minutes	2 Business Hours	4 Business Hours
Enterprise Tier	99.9%	43 minutes 49 seconds	1 Hour (24/7)	2 Hours (24/7)

3.3 Measurement and Calculation Methodology

- **Measurement Period:** Each calendar month from 12:00:01 AM Eastern Time on the first day through 11:59:59 PM Eastern Time on the last day
- **Monitoring Systems:** Automated monitoring systems with measurement intervals of no more than one (1) minute
- **Geographic Scope:** Measurements taken from multiple geographic locations within the United States
- **Documentation:** All availability measurements shall be documented and made available to Customer upon reasonable request

3.4 Planned Maintenance Windows

Provider reserves the right to perform Planned Maintenance in accordance with the following parameters:

- **Standard Maintenance Window:** Sundays between 2:00 AM and 6:00 AM Eastern Time
- **Maximum Monthly Planned Maintenance:** Four (4) hours per calendar month
- **Advance Notice Requirement:** Minimum forty-eight (48) hours written notice via email and platform notifications
- **Emergency Security Maintenance:** May be performed with reasonable notice when necessary to address critical security vulnerabilities

3.5 Exclusions from Availability Calculations

The following events shall be excluded from Downtime calculations and shall not constitute breaches of the availability commitments:

(a) **Force Majeure Events** as defined in Section 1.1; (b) **Planned Maintenance** performed in accordance with Section 3.4; (c) **Customer-Caused Downtime** resulting from Customer's actions, omissions, or misconfigurations; (d) **Third-Party Service Failures** beyond Provider's reasonable control, including but not limited to internet service provider outages, domain name system failures, or cloud infrastructure provider outages; (e) **Security Incidents** including but not limited to distributed denial-of-service attacks, data breaches, or other malicious activities directed at the Services; (f) **Suspension of Services** in accordance with the terms of the Primary Agreement due to Customer's breach or non-payment; (g) **Beta Features** or services explicitly designated as experimental or pre-release; and (h) **Customer's Failure to Implement** recommended updates, patches, or configuration changes that would have prevented or mitigated the downtime.

---

4. RECOVERY TIME OBJECTIVES AND INCIDENT RESPONSE PROCEDURES

4.1 Incident Classification and Response Commitments

Provider hereby commits to respond to and resolve service incidents in accordance with the following Recovery Time Objectives, which constitute binding contractual commitments:

Severity Level	Definition and Criteria	Initial Response RTO	Resolution Target RTO	Maximum Allowable RTO
Critical (P1)	Complete service unavailability affecting all users; critical security breach; data loss incident	30 minutes	2 hours	4 hours
High (P2)	Major functionality impaired for majority of users; significant performance degradation; partial service unavailability	1 hour	4 hours	8 hours

Medium (P3)	Minor functionality affected; isolated user issues; non-critical performance issues	4 hours	8 hours	24 hours
Low (P4)	Cosmetic issues; documentation errors; feature requests; minor inconveniences	1 Business Day	48 hours	5 Business Days

4.2 Incident Response Procedures and Escalation Matrix

4.2.1 Detection and Notification Process:

1. **Automated Detection:** Provider maintains automated monitoring systems capable of detecting service anomalies within five (5) minutes of occurrence
2. **Initial Assessment:** Provider's technical team shall conduct an initial impact assessment within fifteen (15) minutes of detection
3. **Customer Notification:** Provider shall notify Customer of Critical and High severity incidents within thirty (30) minutes of confirmed detection via multiple channels including email, SMS (where provided), and in-platform notifications
4. **Status Page Updates:** Provider shall update the public status page within fifteen (15) minutes of incident confirmation

4.2.2 Response and Resolution Process:

1. **Team Mobilization:** Appropriate technical resources shall be mobilized within the Initial Response RTO specified above
2. **Communication Protocol:** Provider shall provide regular status updates to Customer at intervals not exceeding sixty (60) minutes for Critical incidents and four (4) hours for High severity incidents
3. **Escalation Procedures:** Incidents not resolved within fifty percent (50%) of the Maximum Allowable RTO shall be automatically escalated to senior management
4. **Resolution Verification:** Provider shall confirm resolution through automated testing and Customer validation where appropriate

4.2.3 Post-Incident Procedures:

1. **Root Cause Analysis:** Provider shall conduct a thorough root cause analysis for all Critical and High severity incidents
2. **Post-Incident Report:** A detailed post-incident report shall be provided to Customer within five (5) Business Days of resolution for Critical incidents and ten (10) Business Days for High severity incidents
3. **Corrective Action Plan:** Provider shall implement appropriate corrective measures to prevent recurrence of similar incidents

4.3 Service Restoration Priorities

In the event of partial service degradation, Provider shall prioritize restoration efforts in the following order:

1. Core compliance monitoring and alerting functions
2. Data access and retrieval capabilities
3. Reporting and dashboard functionality
4. Administrative and configuration features
5. Ancillary features and integrations

---

5. DATA PROTECTION AND RECOVERY POINT OBJECTIVES

5.1 Data Loss Tolerance Levels and RPO Commitments

Provider hereby commits to maintain the following Recovery Point Objectives for different categories of Customer Data, representing the maximum acceptable data loss in the event of a system failure:

Data Category	Description	Backup Frequency	RPO Target	Maximum RPO	Geographic Redundancy
Critical Configuration Data	User accounts, system settings, compliance rules	Real-time replication	5 minutes	15 minutes	Multi-region
Compliance Reports and Assessments	Generated reports, audit results, risk assessments	Every 2 hours	2 hours	4 hours	Cross-region
Audit Logs and Activity Records	User activity, system events, compliance tracking	Real-time streaming	1 minute	5 minutes	Multi-region
Customer Uploaded Documents	Policies, procedures, evidence files	Hourly snapshots	30 minutes	1 hour	Cross-region
Historical Compliance Data	Archived reports, historical trends	Daily backups	12 hours	24 hours	Regional
System Metadata and Configurations	Platform settings, integrations, customizations	Every 4 hours	4 hours	8 hours	Regional

5.2 Data Backup and Recovery Infrastructure

5.2.1 Backup Architecture:

- **Primary Storage:** High-availability storage systems with real-time replication
- **Secondary Backup:** Automated backup systems with configurable retention policies
- **Tertiary Archive:** Long-term archival storage for compliance and legal requirements
- **Geographic Distribution:** Data replicated across multiple geographically separated data centers

5.2.2 Backup Testing and Validation:

- **Regular Testing Schedule:** Backup and recovery procedures tested monthly with documented results
- **Validation Processes:** Automated integrity checks performed on all backup data
- **Recovery Drills:** Quarterly disaster recovery exercises conducted to validate RTO and RPO commitments
- **Documentation Requirements:** All backup and recovery activities documented with audit trails

5.3 Data Recovery Procedures and Service Level Commitments

5.3.1 Data Recovery Request Process:

1. Customer submits data recovery request through designated support channels
2. Provider validates request and determines scope within two (2) hours
3. Recovery initiation within four (4) hours of validated request
4. Data restoration completed within the applicable RPO timeframes specified above
5. Customer notification and validation of recovered data

5.3.2 Data Recovery SLA Commitments:

- **Point-in-Time Recovery:** Available for all data categories with granularity matching backup frequencies
- **Partial Recovery:** Capability to recover specific data subsets without full system restoration
- **Cross-Platform Recovery:** Data recovery available across different deployment environments
- **Verification Procedures:** Automated and manual verification of data integrity post-recovery

5.4 Data Security and Encryption Standards

5.4.1 Encryption Requirements:

- **Data at Rest:** AES-256 encryption for all stored data
- **Data in Transit:** TLS 1.3 encryption for all data transmissions
- **Backup Encryption:** All backup data encrypted using industry-standard algorithms
- **Key Management:** Secure key management practices with regular rotation

5.4.2 Access Controls and Monitoring:

- **Multi-Factor Authentication:** Required for all administrative access
- **Role-Based Access Control:** Granular permissions based on principle of least privilege

- **Audit Logging:** Comprehensive logging of all data access and modification activities
- **Anomaly Detection:** Automated monitoring for unusual data access patterns

---

6. PERFORMANCE STANDARDS AND BENCHMARKS

6.1 Response Time and Performance Commitments

Provider hereby commits to maintain the following performance standards for the ComplianceSeal Services:

6.1.1 Web Application Performance:

- **Page Load Time:** Less than three (3) seconds for ninety-five percent (95%) of page requests during normal operating conditions
- **Interactive Response Time:** Less than one (1) second for ninety percent (90%) of user interface interactions
- **Dashboard Refresh Rate:** Real-time data updates within thirty (30) seconds of data changes
- **Search Functionality:** Query results delivered within two (2) seconds for ninety-five percent (95%) of searches

6.1.2 API Performance Standards:

- **REST API Response Time:** Less than 500 milliseconds for ninety percent (90%) of API calls
- **Batch Processing APIs:** Processing initiation within sixty (60) seconds of request submission
- **Data Export APIs:** Initiation of export processes within two (2) minutes of request
- **Webhook Delivery:** Event notifications delivered within five (5) minutes of trigger occurrence

6.1.3 Report Generation Performance:

- **Standard Reports:** Generation completed within thirty (30) seconds for reports containing up to 10,000 records
- **Complex Reports:** Generation completed within five (5) minutes for reports containing up to 100,000 records
- **Custom Reports:** Generation time proportional to data complexity with maximum of fifteen (15) minutes
- **Scheduled Reports:** Delivered within thirty (30) minutes of scheduled time

6.2 System Capacity and Scalability Commitments

6.2.1 User Concurrency:

- **Concurrent User Support:** Platform shall support the contracted number of concurrent users plus twenty percent (20%) buffer capacity
- **Peak Load Handling:** System shall maintain performance standards during peak usage periods

- **Automatic Scaling:** Infrastructure shall automatically scale to accommodate usage spikes
- **Capacity Monitoring:** Real-time monitoring of system capacity with proactive scaling

6.2.2 Data Storage and Processing:

- **Storage Capacity:** Unlimited storage for compliance-related data within reasonable usage parameters
- **Processing Capacity:** Sufficient computational resources to maintain performance standards
- **Database Performance:** Query response times optimized for typical compliance workflows
- **File Upload Limits:** Support for individual file uploads up to 100 MB with batch processing capabilities

6.3 Performance Monitoring and Reporting

6.3.1 Monitoring Infrastructure:

- **Real-Time Monitoring:** Continuous monitoring of all performance metrics
- **Geographic Monitoring:** Performance measurements from multiple geographic locations
- **User Experience Monitoring:** Synthetic transaction monitoring to simulate user workflows
- **Alerting Systems:** Automated alerts when performance thresholds are exceeded

6.3.2 Performance Reporting:

- **Monthly Performance Reports:** Detailed reports provided to Customer showing compliance with performance standards
- **Trend Analysis:** Historical performance data and trend analysis
- **Benchmarking:** Performance comparisons against industry standards
- **Improvement Recommendations:** Proactive recommendations for performance optimization

---

7. COMPREHENSIVE SUPPORT SERVICES AND RESPONSE COMMITMENTS

7.1 Support Tier Structure and Availability

Provider offers multiple support tiers with differentiated response times, availability, and service levels:

Support Tier	Availability Schedule	Response Time Commitment	Escalation Timeline	Dedicated Resources
Basic Support	Business Hours (M-F, 8 AM-6 PM ET)	8 hours	24 hours	Shared support queue

Professional Support	Extended Hours (M-F, 6 AM-10 PM ET)	4 hours	12 hours	Priority queue access
Enterprise Support	24/7/365 availability	1 hour	4 hours	Dedicated support manager

7.2 Support Channel Availability and Service Level Commitments

7.2.1 Primary Support Channels:

- **Web-Based Support Portal:** Available 24/7 with ticket tracking and status updates
- **Email Support:** cssupport@snimbus.ai with guaranteed response within published timeframes
- **Knowledge Base:** Comprehensive self-service resources available 24/7
- **Community Forum:** Peer-to-peer support with Provider moderation during Business Hours

7.2.2 Premium Support Channels (Professional and Enterprise Tiers):

- **Priority Email Queue:** Dedicated email routing for faster response times
- **Phone Support:** Direct phone access during specified availability hours
- **Screen Sharing:** Remote assistance capabilities for complex technical issues
- **Video Conferencing:** Scheduled consultation sessions for implementation and optimization

7.2.3 Emergency Support (Enterprise Tier Only):

- **Emergency Hotline:** 24/7 phone access for Critical (P1) incidents
- **Emergency Escalation:** Direct escalation to senior technical staff and management
- **On-Site Support:** Available upon request for major implementations or critical issues
- **Dedicated Support Manager:** Named support contact with deep knowledge of Customer's environment

7.3 Support Response and Resolution Commitments

7.3.1 Response Time Definitions:

- **First Response:** Acknowledgment of support request with initial assessment
- **Progress Updates:** Regular communication regarding status and expected resolution
- **Resolution:** Complete resolution of the support request or acceptable workaround
- **Escalation:** Transfer to higher-level support resources when initial efforts are insufficient

7.3.2 Support Quality Standards:

- **Technical Expertise:** Support staff certified in ComplianceSeal platform and relevant compliance frameworks
- **Communication Standards:** Professional, clear, and timely communication in Customer's preferred language
- **Documentation:** Comprehensive documentation of all support interactions and resolutions

- **Follow-Up Procedures:** Post-resolution follow-up to ensure Customer satisfaction

---

8. SERVICE LEVEL REMEDIES AND COMPENSATION FRAMEWORK

8.1 Service Credit Calculation and Eligibility

In the event Provider fails to meet the service level commitments specified in this SLA, Customer shall be eligible for Service Credits calculated as follows:

8.1.1 Availability-Based Service Credits:

Monthly Uptime Achievement	Service Credit Percentage	Calculation Method
99.0% to 99.49%	10% of monthly service fees	Pro-rated based on actual downtime
98.0% to 98.99%	25% of monthly service fees	Applied to affected service modules
97.0% to 97.99%	50% of monthly service fees	Full month credit consideration
Below 97.0%	100% of monthly service fees	Complete service fee waiver

8.1.2 Performance-Based Service Credits:

- **Response Time Failures:** 5% credit for each performance standard not met during the measurement period
- **RTO Violations:** 15% credit for each incident exceeding maximum RTO commitments
- **RPO Violations:** 25% credit for any data loss exceeding maximum RPO commitments
- **Support Response Failures:** 10% credit for each support response time violation

8.2 Service Credit Request and Processing Procedures

8.2.1 Claim Submission Requirements:

- Service Credit claims must be submitted within thirty (30) days of the incident or measurement period
- Claims must include specific details of the service level breach and impact on Customer's operations
- Provider reserves the right to request additional documentation to validate claims

- Claims must be submitted through the designated support portal or via email to cssupport@snimbus.ai

8.2.2 Claim Processing Timeline:

- Provider shall acknowledge receipt of Service Credit claims within two (2) Business Days
- Initial review and validation completed within ten (10) Business Days
- Final determination and credit application within fifteen (15) Business Days
- Customer notification of credit approval or denial with detailed explanation

8.2.3 Credit Application and Limitations:

- Service Credits applied to future monthly service fees
- Credits cannot be exchanged for cash payments
- Unused credits expire twelve (12) months from issuance date
- Maximum aggregate Service Credits limited to one hundred percent (100%) of annual service fees

8.3 Exclusions and Limitations of Remedies

8.3.1 Service Credit Exclusions: Service Credits shall not apply to service level breaches caused by or resulting from:

- Force Majeure Events as defined in Section 1.1
- Customer's breach of the Primary Agreement or this SLA
- Customer's failure to implement recommended updates or configurations
- Third-party service failures beyond Provider's reasonable control
- Misuse or abuse of the Services by Customer or its users
- Customizations or modifications not approved by Provider

8.3.2 Limitation of Liability: CUSTOMER ACKNOWLEDGES AND AGREES THAT THE SERVICE CREDITS SPECIFIED IN THIS SECTION CONSTITUTE CUSTOMER'S SOLE AND EXCLUSIVE REMEDY FOR PROVIDER'S FAILURE TO MEET THE SERVICE LEVEL COMMITMENTS SET FORTH IN THIS SLA. PROVIDER'S TOTAL LIABILITY FOR ALL SERVICE LEVEL BREACHES IN ANY TWELVE (12) MONTH PERIOD SHALL NOT EXCEED THE TOTAL AMOUNT OF SERVICE FEES PAID BY CUSTOMER DURING SUCH PERIOD.

---

9. MONITORING, MEASUREMENT, AND REPORTING OBLIGATIONS

9.1 Service Level Monitoring Infrastructure

9.1.1 Monitoring System Requirements: Provider shall maintain comprehensive monitoring systems including:

- **Real-Time Monitoring:** Continuous monitoring of all service components with measurement intervals not exceeding sixty (60) seconds
- **Multi-Point Monitoring:** Monitoring from multiple geographic locations to ensure representative measurements
- **Synthetic Transaction Monitoring:** Automated simulation of typical user workflows and transactions
- **Infrastructure Monitoring:** Monitoring of underlying infrastructure components including servers, networks, and databases

9.1.2 Data Collection and Retention:

- **Monitoring Data Retention:** All monitoring data retained for minimum of twenty-four (24) months
- **Audit Trail Requirements:** Complete audit trails maintained for all service level measurements
- **Data Accuracy Standards:** Monitoring systems calibrated and validated monthly for accuracy
- **Third-Party Validation:** Independent monitoring services may be utilized to validate internal measurements

9.2 Reporting Requirements and Delivery Schedule

9.2.1 Monthly Service Level Reports: Provider shall deliver comprehensive monthly reports to Customer within five (5) Business Days following the end of each calendar month, including:

- Detailed availability statistics and uptime calculations
- Performance metrics and benchmark comparisons
- Incident summaries with root cause analysis
- Service Credit calculations and applications
- Trend analysis and recommendations for improvement

9.2.2 Quarterly Business Reviews (Professional and Enterprise Tiers):

- **Service Performance Assessment:** Comprehensive review of service delivery against SLA commitments
- **Strategic Planning:** Discussion of Customer's evolving requirements and service optimization opportunities
- **Roadmap Alignment:** Review of Provider's product roadmap and alignment with Customer needs
- **Process Improvement:** Identification and implementation of process improvements

9.2.3 Annual Service Assessment:

- **Comprehensive SLA Review:** Annual assessment of SLA performance and effectiveness
- **Benchmarking Analysis:** Comparison of service delivery against industry standards
- **Contract Optimization:** Recommendations for SLA modifications based on performance history
- **Strategic Alignment:** Review of service alignment with Customer's long-term objectives

9.3 Customer Access to Monitoring Data

9.3.1 Real-Time Status Information:

- **Public Status Page:** Real-time service status information available at [status.snimbus.ai]
- **API Access:** Programmatic access to service status information via documented APIs
- **Alert Subscriptions:** Customizable alert subscriptions for service status changes
- **Mobile Applications:** Mobile access to service status and alert information

9.3.2 Historical Data Access:

- **Performance Dashboards:** Customer access to historical performance data and trends
- **Custom Reports:** Ability to generate custom reports from historical monitoring data
- **Data Export:** Options to export monitoring data for Customer's internal analysis
- **Integration Capabilities:** APIs for integrating service level data with Customer's monitoring systems

---

10. CUSTOMER RESPONSIBILITIES AND OBLIGATIONS

10.1 Customer Cooperation and Support Requirements

10.1.1 Information and Access Requirements: Customer shall provide and maintain:

- **Accurate Contact Information:** Current contact information for technical and business contacts, including 24/7 emergency contacts for Enterprise tier customers
- **System Access:** Reasonable access to Customer's systems and environments as necessary for Provider to deliver the Services
- **Documentation:** Current documentation of Customer's compliance requirements, business processes, and system configurations
- **Feedback and Communication:** Timely feedback regarding service issues, requirements changes, and satisfaction with service delivery

10.1.2 Technical Cooperation:

- **Implementation Support:** Reasonable cooperation during initial implementation and ongoing configuration changes
- **Testing Participation:** Participation in testing activities for updates, patches, and new features
- **Issue Reporting:** Prompt reporting of service issues, security concerns, or potential compliance violations
- **Change Management:** Advance notification of significant changes to Customer's environment that may impact service delivery

10.2 Customer Usage and Compliance Obligations

10.2.1 Acceptable Use Requirements: Customer agrees to use the ComplianceSeal Services in accordance with:

- **Terms of Service:** All applicable terms of service and acceptable use policies
- **Legal Compliance:** All applicable laws, regulations, and industry standards
- **Security Practices:** Provider's recommended security practices and configurations
- **Capacity Limitations:** Reasonable usage within contracted capacity limits

10.2.2 Data and Security Responsibilities:

- **Data Accuracy:** Ensuring accuracy and completeness of data provided to the Services
- **Access Control:** Maintaining appropriate user access controls and authentication mechanisms
- **Security Incident Reporting:** Immediate reporting of suspected security incidents or data breaches
- **Backup Verification:** Regular verification of critical data backup and recovery procedures

10.3 Customer System and Infrastructure Requirements

10.3.1 Technical Requirements: Customer shall maintain:

- **Internet Connectivity:** Reliable internet connectivity with sufficient bandwidth for normal service usage
- **Supported Browsers:** Use of supported web browsers and operating systems as specified in Provider's documentation
- **Security Software:** Current anti-virus and anti-malware software on all systems accessing the Services
- **System Updates:** Current operating system and browser updates and security patches

10.3.2 Network and Infrastructure Standards:

- **Network Security:** Appropriate network security measures including firewalls and intrusion detection systems
- **Performance Requirements:** Network and system performance adequate to support normal service usage
- **Monitoring Capabilities:** Basic monitoring capabilities to identify connectivity or performance issues
- **Disaster Recovery:** Appropriate disaster recovery and business continuity planning for Customer's operations

---

11. MAINTENANCE, UPDATES, AND CHANGE MANAGEMENT

11.1 Scheduled Maintenance Procedures and Notifications

11.1.1 Regular Maintenance Activities: Provider reserves the right to perform scheduled maintenance activities including:

- **Routine System Maintenance:** Regular maintenance of servers, databases, and infrastructure components
- **Security Updates:** Application of security patches and updates to address vulnerabilities
- **Performance Optimization:** System tuning and optimization activities to maintain performance standards
- **Capacity Expansion:** Infrastructure upgrades to support growing service demands

11.1.2 Maintenance Notification Requirements:

- **Standard Maintenance:** Minimum forty-eight (48) hours advance written notice via email and platform notifications
- **Major Maintenance:** Minimum one (1) week advance notice for maintenance expected to exceed four (4) hours
- **Emergency Maintenance:** Reasonable advance notice for critical security or stability issues, with immediate notification if advance notice is not feasible
- **Maintenance Cancellation:** Right to cancel or reschedule maintenance with twelve (12) hours notice if business conditions warrant

11.2 Service Updates and Enhancement Procedures

11.2.1 Update Classification and Procedures:

- **Minor Updates:** Bug fixes and minor feature enhancements deployed during regular maintenance windows
- **Major Updates:** Significant feature additions or changes deployed with extended maintenance windows and customer notification
- **Security Updates:** Critical security patches deployed with minimal notice when necessary to address security vulnerabilities
- **Customer-Requested Updates:** Customizations or modifications requested by Customer with appropriate change control procedures

11.2.2 Update Testing and Deployment:

- **Testing Procedures:** All updates tested in staging environments before production deployment
- **Rollback Capabilities:** Ability to rollback updates in case of unexpected issues or service degradation
- **Phased Deployment:** Major updates deployed in phases to minimize impact and allow for issue identification
- **Customer Acceptance:** Customer acceptance testing period for major updates affecting critical functionality

11.3 Change Management and Communication Protocols

11.3.1 Change Control Process:

- **Change Request Evaluation:** All significant changes evaluated for impact on service levels and customer operations

- **Risk Assessment:** Comprehensive risk assessment for changes with potential service impact
- **Approval Procedures:** Formal approval procedures for changes affecting service delivery or customer data
- **Implementation Planning:** Detailed implementation plans for complex changes with rollback procedures

11.3.2 Customer Communication Requirements:

- **Change Notifications:** Advance notification of all changes affecting service functionality or performance
- **Impact Assessment:** Clear communication of expected impact on customer operations
- **Implementation Timeline:** Detailed timeline for change implementation with key milestones
- **Post-Implementation Support:** Enhanced support availability during and after change implementation

---

12. DATA SECURITY, PRIVACY, AND COMPLIANCE FRAMEWORK

12.1 Data Security Measures and Standards

**12