# SERVICE LEVEL AGREEMENT (SLA)

**Between**

**THAMES INTERNATIONAL CONSULTING LTD**

*(ERP Service Provider)*

And

**Taxpayers / ERP Subscribers**

For

**Nigeria Electronic Invoicing Services**

**Version:** 1.0

**Classification:** Public

**Effective Date:** MAY 2026

**Document Owner:** Service Delivery Department

**Approved By:** Managing Director

**Next Review Date:** MAY 2027

## Document Control

| Item | Details |
|---|---|
| Document Title | Service Level Agreement (SLA) |
| Document Number | SLA-ERP-001 |
| Version | 1.0 |
| Classification | Public |
| Owner | Service Delivery Department |
| Author | Enterprise Solutions Team |
| Approved By | Managing Director |
| Effective Date | May 2026 |
| Review Cycle | Annual |
| Status | Approved |

**Approval Page**

This Service Level Agreement has been reviewed and approved by the authorized representatives of the ERP Service Provider. The document establishes the minimum service commitments provided to taxpayers utilizing the ERP platform for electronic invoicing in accordance with the Federal Inland Revenue Service (FIRS) Merchant Buyer Solution (MBS) framework.

| Name | Position | Signature | Date |
|---|---|---|---|
| Cornelius Adeoye | Managing Director | Cornelius Adeoye | 4th may 2026 |
| Micheal Ipadeola | Head of Technology | Micheal Ipadeola | 4th may 2026 |

**Revision History**

| Version | Date | Author | Description |
|---|---|---|---|
| 0.1 | May 2026 | Enterprise Solutions Team | Initial Draft |
| 0.5 | May 2026 | Technical Review Committee | Internal Review |
| 0.9 | May 2026 | Compliance Team | FIRS Compliance Review |
| 1.0 | May 2026 | Managing Director | Approved Release |

**Distribution List**

This document shall be distributed to:

- Executive Management
- Service Delivery Team
- Technical Support Team
- Information Security Team
- Compliance Department
- Software Development Team
- Quality Assurance Team
- FIRS Accreditation Team
- Taxpayer Organizations (Upon Request)

**Table of Contents**


1. Introduction
2. Purpose
3. Scope
4. Definitions
5. Acronyms
6. Service Description
7. Service Availability
8. Performance Standards
9. Service Support
10. Incident Management
11. Problem Management
12. Change Management
13. Security Management
14. Data Protection
15. Backup and Disaster Recovery
16. Roles and Responsibilities
17. Reporting
18. Compliance
19. Business Continuity
20. Terms and Conditions
21. Appendices

## Chapter 1 – Introduction

### 1.1 Background

This Service Level Agreement (SLA) establishes the service commitments between **THAMES INTERNATIONAL CONSULTING LTD** ("the Service Provider") and organizations, businesses, and taxpayers ("the Customer") utilizing the Enterprise Resource Planning (ERP) platform for electronic invoicing and tax-related transactions within the Federal Republic of Nigeria.

The ERP platform enables taxpayers to generate, validate, transmit, receive, and manage electronic invoices in compliance with the Federal Inland Revenue Service (FIRS) Electronic Invoicing Framework and the Merchant Buyer Solution (MBS) integration requirements.

This SLA defines measurable service levels, operational responsibilities, security obligations, and support commitments to ensure that services are delivered in a timely, reliable, secure, and compliant manner.

The document further establishes the standards for service availability, response times, issue resolution, system maintenance, security controls, data protection, and disaster recovery. These commitments are designed to provide taxpayers with confidence that the ERP platform consistently supports statutory invoicing obligations while maintaining the confidentiality, integrity, and availability of taxpayer information.

In addition to defining operational expectations, this SLA supports continuous service improvement by specifying performance indicators, reporting mechanisms, escalation procedures, and governance processes that facilitate transparent communication between the Service Provider and its customers.

## Chapter 2 – Purpose, Objectives, Scope, Definitions, and Acronyms

### 2.1 Purpose

The purpose of this Service Level Agreement (SLA) is to define the minimum service commitments, responsibilities, operational standards, and performance expectations governing the delivery of the Enterprise Resource Planning (ERP) electronic invoicing solution provided by **THAMES INTERNATIONAL CONSULTING** ("the Service Provider") to taxpayers and organizations ("the Customer") operating within the Federal Republic of Nigeria.

This SLA establishes measurable service standards to ensure that the ERP platform consistently delivers reliable, secure, available, and compliant electronic invoicing services in accordance with the requirements of the Federal Inland Revenue Service (FIRS), the Merchant Buyer Solution (MBS) integration framework, and all other applicable regulatory obligations.

The agreement serves as the formal commitment between the Service Provider and its customers regarding the quality of service expected throughout the lifecycle of the service relationship.

Specifically, this SLA aims to:

- Define the scope of services covered by the ERP platform.
- Establish measurable service availability targets.
- Define response and resolution time commitments.
- Outline security and privacy obligations.
- Describe incident, problem, and change management procedures.
- Define backup and disaster recovery commitments.
- Specify customer responsibilities and provider obligations.
- Promote transparency through measurable performance indicators.
- Support compliance with Nigerian tax and data protection regulations.
- Establish governance procedures for continual service improvement.

### 2.2 Objectives

The objectives of this Service Level Agreement are to ensure that the ERP platform consistently provides high-quality services that enable taxpayers to fulfill their electronic invoicing obligations efficiently and securely.

The key objectives include:

#### 2.2.1 Service Reliability

Ensure uninterrupted availability of the ERP platform through resilient infrastructure, proactive monitoring, preventive maintenance, and continuous performance optimization.

#### 2.2.2 Regulatory Compliance

Support taxpayer compliance with all applicable regulations governing electronic invoicing, taxation, record retention, and data protection, including requirements issued by the Federal Inland Revenue Service (FIRS).

#### 2.2.3 Secure Processing

Protect taxpayer information through industry-recognized information security controls covering authentication, authorization, encryption, monitoring, and audit logging.

#### 2.2.4 Performance Excellence

Maintain high transaction processing performance that allows invoices to be generated, validated, transmitted, and acknowledged within acceptable operational timelines.

#### 2.2.5 Customer Satisfaction

Deliver responsive customer support through defined service desk procedures, escalation processes, and timely issue resolution.

#### 2.2.6 Continuous Improvement

Review operational performance periodically to identify opportunities for service enhancements, process optimization, and technology improvements.

### 2.3 Scope

This SLA applies to all electronic invoicing services delivered through the ERP platform to registered customers and taxpayers.

The agreement covers all production environments used for electronic invoicing and related services.

The services covered include, but are not limited to:

**Invoice Management**

- Creation of electronic invoices
- Invoice editing
- Invoice validation
- Invoice approval
- Invoice cancellation
- Invoice search
- Invoice printing
- Invoice archiving

**Credit and Debit Notes**

- Credit Note Generation
- Debit Note Generation
- Adjustment Processing
- Reference Validation

**Customer Management**

- Customer Registration
- Customer Profile Updates
- Taxpayer Identification Management
- Customer Search

**Product and Service Catalogue**

- Product Registration
- Product Classification
- VAT Assignment

- Price Management

**Tax Management**

- VAT Calculation
- Tax Code Assignment
- Tax Validation
- Tax Reporting

**Electronic Invoice Transmission**

- Invoice Submission
- Status Monitoring
- Response Retrieval
- Retry Processing
- Error Handling

**API Services**

- Authentication
- Token Management
- Secure Data Exchange
- Status Synchronization

**Reporting**

- Sales Reports
- VAT Reports
- Transaction Reports
- Audit Reports
- Invoice Status Reports

**User Administration**

- User Registration
- Role Management

- Access Control
- Password Management
- Multi-Factor Authentication

**Audit Services**

- Activity Logging
- User Audit Trail
- Invoice Audit Trail
- Security Audit

**Notification Services**

- Email Notifications
- SMS Notifications (where enabled)
- System Alerts
- Service Announcements

### 2.4 Services Not Covered

The following services are outside the scope of this SLA unless expressly agreed in writing:

- Customer-owned hardware maintenance.
- Internet connectivity provided by third-party Internet Service Providers.
- Customer local area network (LAN) support.
- Third-party accounting software not integrated with the ERP platform.
- Power supply interruptions within the customer's premises.
- User training beyond the agreed implementation period.
- Custom software development unless covered under a separate agreement.
- Data migration from unsupported legacy systems.
- Third-party software licensing issues.

### 2.5 Intended Audience

This document is intended for:

- Registered Taxpayers
- Finance Departments
- Accountants
- Internal Auditors
- ERP Administrators
- IT Managers
- Compliance Officers
- Service Desk Personnel
- Software Developers
- Infrastructure Engineers
- Information Security Officers
- FIRS Accreditation Review Team
- External Auditors

### 2.6 Definitions

For the purpose of this SLA, the following definitions apply.

| Term | Definition |
|---|---|
| ERP | Enterprise Resource Planning software used to manage business operations and electronic invoicing. |
| Electronic Invoice | A digitally generated tax invoice exchanged electronically between trading parties. |
| Customer | Any organization or taxpayer subscribed to the ERP service. |
| Service Provider | The organization responsible for providing and maintaining the ERP platform. |

| Term | Definition |
|---|---|
| Incident | Any event that disrupts or reduces the quality of an IT service. |
| Problem | The underlying cause of one or more incidents. |
| Availability | The percentage of time the service is operational and accessible. |
| Planned Maintenance | Scheduled maintenance activities announced in advance. |
| Emergency Maintenance | Unplanned maintenance required to restore or protect services. |
| Resolution Time | Time required to permanently resolve an incident. |
| Response Time | Time taken to acknowledge and begin working on a reported incident. |
| SLA | Service Level Agreement defining measurable service commitments. |

### 2.7 Acronyms

| Acronym | Meaning |
|---|---|
| ERP | Enterprise Resource Planning |
| FIRS | Federal Inland Revenue Service |
| MBS | Merchant Buyer Solution |
| API | Application Programming Interface |
| VAT | Value Added Tax |
| NDPA | Nigeria Data Protection Act |
| MFA | Multi-Factor Authentication |
| TLS | Transport Layer Security |
| AES | Advanced Encryption Standard |

| Acronym | Meaning |
| --- | --- |
| RPO | Recovery Point Objective |
| RTO | Recovery Time Objective |
| KPI | Key Performance Indicator |
| DR | Disaster Recovery |
| BCP | Business Continuity Plan |
| SIEM | Security Information and Event Management |

### 3.1 Overview

The Enterprise Resource Planning (ERP) Platform is a secure, cloud-enabled business management solution that provides end-to-end electronic invoicing and financial transaction management services for taxpayers and organizations operating within the Federal Republic of Nigeria.

The platform enables businesses to generate, validate, transmit, receive, archive, and manage electronic invoices in compliance with the Federal Inland Revenue Service (FIRS) Electronic Invoicing Framework and the Merchant Buyer Solution (MBS) specifications.

The ERP integrates accounting, sales, inventory, procurement, taxation, reporting, and compliance into a unified environment, ensuring that all business transactions are accurately captured and reported while maintaining the confidentiality, integrity, and availability of taxpayer information.

The Service Provider shall ensure that all production services are continuously monitored, maintained, and improved to meet the service commitments defined within this Service Level Agreement.

### 3.2 Core Service Components

The ERP platform provides the following core services.

#### 3.2.1 User Authentication and Identity Management

The ERP platform provides secure user authentication to ensure that only authorized personnel have access to taxpayer information and business transactions.

**Features**

- Username and Password Authentication
- Multi-Factor Authentication (MFA)
- Single Sign-On (Optional)
- Password Expiration
- Password Complexity Enforcement
- Account Lockout after Failed Attempts
- Session Timeout

- Concurrent Session Control
- User Profile Management

**Service Commitment**

| Metric | Target |
|---|---|
| Login Availability | 99.9% |
| Authentication Response | ≤ 3 Seconds |
| Password Reset Processing | ≤ 5 Minutes |
| Session Timeout | 15 Minutes of Inactivity |

### 3.2.2 Customer Management Service

The Customer Management Service enables organizations to register, maintain, and manage customer information required for invoice generation and statutory reporting.

**Supported Functions**

- Customer Registration
- Customer Search
- Customer Profile Update
- Customer Tax Identification Number (TIN) Management
- Customer Address Management
- Customer Contact Information
- Customer Status Management
- Customer Classification

**Service Objectives**

The Service Provider shall ensure that customer information is securely stored, validated, and available whenever required for invoice processing.

**Availability Commitment**

99.9%

### 3.2.3 Product and Service Catalogue Management

This service enables businesses to maintain a centralized repository of products and services offered to customers.

**Supported Functions**

- Product Registration
- Product Classification
- Unit of Measure Management
- Pricing Management
- Discount Configuration
- VAT Assignment
- Product Activation
- Product Deactivation

**Performance Commitment**

Product search results shall be returned within three (3) seconds under normal operating conditions.

### 3.2.4 Electronic Invoice Generation Service

This service enables taxpayers to create legally compliant electronic invoices using standardized invoice templates.

The service automatically calculates applicable taxes, validates mandatory invoice fields, and prepares invoices for transmission to the Nigeria e-Invoicing platform.

**Invoice Information Captured**

- Invoice Number
- Invoice Date
- Buyer Information
- Seller Information

- Tax Identification Number (TIN)
- Product Details
- Quantity
- Unit Price
- VAT
- Discounts
- Currency
- Payment Terms
- Total Amount
- Invoice Reference

**Functional Capabilities**

- Create Draft Invoice
- Save Invoice
- Edit Draft
- Validate Invoice
- Submit Invoice
- Print Invoice
- Download PDF
- Email Invoice
- Archive Invoice

**Performance Standards**

| Performance Indicator | Target |
|---|---|
| Invoice Creation | ≤ 5 Seconds |
| Invoice Save | ≤ 3 Seconds |
| Invoice Validation | ≤ 5 Seconds |

| Performance Indicator | Target |
|---|---|
| PDF Generation | ≤ 10 Seconds |

### 3.2.5 Electronic Invoice Validation

Prior to submission, every invoice shall undergo automated validation to ensure compliance with business rules and FIRS requirements.

Validation shall include, but is not limited to:

- Mandatory Field Validation
- TIN Validation
- Customer Validation
- Product Validation
- Tax Validation
- Currency Validation
- Duplicate Invoice Detection
- Invoice Number Validation
- Date Validation
- Amount Validation

Invoices failing validation shall not be transmitted until all identified errors have been corrected.

**Validation Response Time**

Maximum of five (5) seconds.

### 3.2.6 Electronic Invoice Transmission Service

The ERP platform provides secure transmission of validated electronic invoices to the designated Nigeria e-Invoicing infrastructure through approved integration interfaces.

**Transmission Features**

- Secure API Communication

- Digital Authentication
- Message Encryption
- Automatic Retry
- Delivery Confirmation
- Status Synchronization
- Error Notification

**Transmission Workflow**

1. Invoice Validation
2. Digital Signing (where applicable)
3. Secure Transmission
4. Receipt Confirmation
5. Status Update
6. Archiving

**Service Commitment**

| Metric | Target |
|---|---|
| Successful Submission Rate | ≥ 99% |
| API Availability | 99.9% |
| Average Submission Time | ≤ 15 Seconds |

### 3.2.7 Invoice Status Tracking

The ERP platform continuously monitors invoice processing and provides real-time visibility into invoice status.

Possible statuses include:

- Draft
- Pending Validation
- Validation Failed

- Ready for Submission
- Submitted
- Processing
- Accepted
- Rejected
- Cancelled
- Archived

Customers shall be able to search invoices using:

- Invoice Number
- Customer Name
- Date Range
- Invoice Status
- TIN
- Amount

### 3.2.8 Credit Note Management

The ERP enables taxpayers to issue electronic credit notes against previously submitted invoices.

Supported capabilities include:

- Full Credit
- Partial Credit
- Credit Reason Selection
- Reference Invoice Validation
- Credit Note Submission
- Credit Note Tracking

All credit notes shall reference the original invoice and maintain complete audit history.

### 3.2.9 Debit Note Management

The ERP supports electronic debit note generation where additional charges become applicable after invoice issuance.

Functions include:

- Debit Amount Calculation
- Original Invoice Reference
- Tax Recalculation
- Validation
- Submission
- Audit Logging

### 3.2.10 Reporting and Analytics

The ERP provides operational and statutory reports to support financial management and regulatory compliance.

**Available Reports**

- Sales Register
- VAT Summary
- Invoice Register
- Customer Statement
- Tax Report
- Outstanding Invoices
- Payment Report
- Credit Notes Register
- Debit Notes Register
- Submission Status Report
- Failed Submission Report
- Audit Trail Report

Reports shall be exportable in:

- PDF
- Microsoft Excel
- CSV

### 3.2.11 Audit Trail Service

The ERP maintains a comprehensive audit trail of all user activities and business transactions.

The audit trail captures:

- Login Events
- Logout Events
- Invoice Creation
- Invoice Modification
- Invoice Submission
- Credit Note Creation
- User Administration
- Configuration Changes
- API Calls
- Security Events

Audit records shall include:

- User ID
- Timestamp
- IP Address
- Device Information
- Activity Performed
- Previous Value

- New Value
- Result

Audit logs shall be retained in accordance with applicable legal and regulatory requirements.

#### 3.2.12 Notification Service

The ERP shall notify users of significant events through configurable communication channels.

Supported notifications include:

- Invoice Submitted
- Invoice Accepted
- Invoice Rejected
- Credit Note Accepted
- Password Reset
- New User Registration
- Failed Login Attempt
- Scheduled Maintenance
- Security Alerts
- Service Disruptions

Notification channels include:

- Email
- SMS (Optional)
- In-Application Notifications
- API Callbacks (where integrated)

### 3.3 Service Dependencies

The proper functioning of the ERP platform depends on:

- Stable internet connectivity.
- Availability of third-party integration services, including the FIRS e-Invoicing platform where applicable.
- Supported web browsers and client devices.
- Valid user credentials and role-based permissions.
- Availability of hosting infrastructure, databases, and monitoring systems.

Where a dependency outside the Service Provider's control causes degradation or interruption, the Service Provider will make reasonable efforts to mitigate the impact and keep customers informed.

## Chapter 4 – Service Availability and Performance Standards

### 4.1 Overview

The Service Provider is committed to delivering highly available, reliable, and secure electronic invoicing services that enable taxpayers to conduct business operations without unnecessary interruption. The ERP platform is designed using resilient infrastructure, redundant network connectivity, high-availability databases, and proactive monitoring to minimize service disruptions.

Service availability commitments described in this chapter apply to the production environment only and exclude scheduled maintenance windows, force majeure events, and outages caused by third-party infrastructure outside the Service Provider's reasonable control.

The Service Provider shall continuously monitor the platform to ensure compliance with the service levels defined in this Agreement and shall implement corrective actions whenever performance falls below agreed thresholds.

### 4.2 Service Availability Commitment

The ERP platform shall be available to authorized users **99.9% of the time**, measured on a monthly basis.

Availability is calculated using the following formula:

**Availability (%) = [(Total Service Time – Unplanned Downtime) ÷ Total Service Time] × 100**

Where:

- **Total Service Time** means the total number of minutes in the calendar month.
- **Unplanned Downtime** means any unscheduled interruption that prevents customers from accessing production services.

Scheduled maintenance periods approved and communicated in advance are excluded from availability calculations.

**Availability Targets**

| Service Component | Availability Target |
|---|---|
| ERP Application | 99.90% |
| Web Portal | 99.90% |
| Authentication Services | 99.95% |
| Invoice Processing Engine | 99.90% |
| API Gateway | 99.90% |
| Database Services | 99.95% |
| Reporting Module | 99.50% |
| Notification Service | 99.50% |

### 4.3 Service Hours

The ERP platform is intended to support business operations at all times.

| Service | Availability |
|---|---|
| ERP Portal | 24 Hours × 7 Days |
| Invoice Generation | 24 Hours × 7 Days |
| Invoice Validation | 24 Hours × 7 Days |
| Invoice Submission | 24 Hours × 7 Days |
| Invoice Status Tracking | 24 Hours × 7 Days |
| API Services | 24 Hours × 7 Days |
| Reporting Services | 24 Hours × 7 Days |

Customer support availability is described separately in Chapter 5.

### 4.4 Planned Maintenance

Planned maintenance activities are performed to maintain service quality, apply security updates, improve system performance, and introduce new functionality.

**Standard Maintenance Window**

**Sundays between 12:00 AM and 4:00 AM (WAT)**

The Service Provider will:

- Provide at least **48 hours' notice** for planned maintenance.
- Describe the expected impact on services.
- Indicate the anticipated maintenance duration.
- Notify customers once maintenance is complete.

Where possible, maintenance activities shall be carried out without interrupting customer access.

### 4.5 Emergency Maintenance

Emergency maintenance may be required where there is:

- A critical security vulnerability.
- A cyberattack or attempted compromise.
- Data corruption.
- Infrastructure failure.
- Critical software defect.
- Regulatory requirement requiring immediate implementation.

Where emergency maintenance is necessary, customers will be informed as soon as reasonably practicable through one or more communication channels, including email, in-application notifications, and the service status page.

### 4.6 Service Monitoring

The Service Provider shall continuously monitor the ERP platform using automated monitoring tools.

Monitoring includes:

- Server availability
- CPU utilization
- Memory utilization
- Disk usage
- Network latency
- Database performance
- API response time
- Authentication success rate
- Invoice processing success rate
- Security events
- Application logs
- Error rates
- Backup status
- Certificate validity

Alerts shall be generated automatically when predefined thresholds are exceeded, enabling proactive investigation and remediation.

### 4.7 Performance Standards

The ERP platform shall meet the following performance targets under normal operating conditions.

| Function | Performance Target |
|---|---|
| User Login | ≤ 3 Seconds |

| Function | Performance Target |
|---|---|
| Dashboard Load | ≤ 5 Seconds |
| Customer Search | ≤ 3 Seconds |
| Product Search | ≤ 3 Seconds |
| Invoice Creation | ≤ 5 Seconds |
| Invoice Save | ≤ 3 Seconds |
| Invoice Validation | ≤ 5 Seconds |
| Invoice Submission | ≤ 15 Seconds |
| PDF Invoice Generation | ≤ 10 Seconds |
| Report Generation (Standard) | ≤ 30 Seconds |
| Report Export | ≤ 60 Seconds |
| Audit Log Search | ≤ 10 Seconds |
| Password Reset | ≤ 5 Minutes |

Performance targets assume normal network conditions and standard transaction volumes.

### 4.8 Capacity Management

The Service Provider shall maintain sufficient infrastructure capacity to support expected business growth while ensuring consistent performance.

Capacity planning shall include:

- Forecasting transaction volumes.
- Monitoring storage utilization.
- Monitoring database growth.
- Monitoring concurrent user sessions.
- Monitoring API traffic.

- Infrastructure scaling.
- Performance tuning.

Capacity reviews shall be conducted **quarterly** or more frequently where significant growth is observed.

### 4.9 Scalability

The ERP platform shall support horizontal and vertical scaling to accommodate increased demand without significant degradation in service quality.

Scalability measures include:

- Load balancing.
- Auto-scaling of application servers.
- Database optimization.
- Distributed processing.
- Cloud resource expansion.
- Queue-based transaction processing.

The Service Provider shall periodically perform load testing to validate scalability.

### 4.10 Key Performance Indicators (KPIs)

The following KPIs will be measured and reported.

| KPI | Target |
|---|---|
| Monthly Availability | ≥ 99.90% |
| Invoice Submission Success Rate | ≥ 99.00% |
| API Availability | ≥ 99.90% |
| Average Login Response | ≤ 3 Seconds |
| Average Invoice Processing Time | ≤ 15 Seconds |

| KPI | Target |
|---|---|
| Average Incident Response Time | As per SLA |
| Average Incident Resolution Time | As per SLA |
| Failed Invoice Rate | < 1% |
| Successful Backup Completion | 100% |
| Security Incident Resolution | 100% within SLA |

Monthly KPI reports shall be reviewed by Service Delivery Management and corrective actions initiated where targets are not met.

### 4.11 Service Reporting

The Service Provider shall produce periodic service reports including:

- Monthly Availability Report
- Incident Summary Report
- Problem Management Report
- Change Management Report
- Capacity Utilization Report
- Security Incident Report
- Backup and Recovery Report
- Customer Support Performance Report
- API Performance Report
- Continuous Improvement Report

Reports shall be made available to authorized stakeholders upon request or through the customer portal where applicable.

### 4.12 Service Exclusions

The following are excluded from the calculation of SLA performance metrics:

- Scheduled maintenance communicated in advance.
- Force majeure events, including natural disasters, civil unrest, or government-imposed restrictions.
- Failures of customer-owned infrastructure or internet connectivity.
- Outages attributable to third-party providers outside the Service Provider's direct control.
- Customer misconfiguration or misuse of the ERP platform.
- Delays resulting from incorrect or incomplete information supplied by the customer.

**4.13 Continuous Service Improvement**

The Service Provider is committed to continually enhancing service quality through:

- Regular performance reviews.
- Root cause analysis of recurring incidents.
- Customer feedback collection.
- Security assessments.
- Capacity planning.
- Technology upgrades.
- Staff training and certification.
- Periodic review of this SLA.

Continuous improvement initiatives shall be documented, prioritized, and tracked to completion.

## Chapter 5 – Service Support and Help Desk

### 5.1 Overview

The Service Provider shall operate a structured Service Desk to provide timely, professional, and effective support to taxpayers using the ERP platform for electronic invoicing. The Service Desk serves as the primary point of contact for all service requests, incidents, enquiries, complaints, technical assistance, and operational guidance.

Support services are designed to minimize disruption to customer operations while ensuring prompt restoration of normal service following any interruption.

The Service Desk operates in accordance with documented support procedures, incident management processes, and escalation protocols to ensure consistent service delivery.

### 5.2 Service Desk Objectives

The objectives of the Service Desk are to:

- Provide a single point of contact for all customer support interactions.
- Restore interrupted services as quickly as possible.
- Minimize the impact of incidents on customer business operations.
- Maintain accurate records of all customer interactions.
- Escalate unresolved issues appropriately.
- Provide proactive communication during service interruptions.
- Ensure customer satisfaction through timely issue resolution.
- Support compliance with FIRS e-Invoicing operational requirements.

### 5.3 Support Channels

Customers may contact the Service Desk through one or more of the following officially designated channels.

| Support Channel | Purpose | Availability |
|---|---|---|
| Customer Portal | Incident logging, service requests, ticket tracking | 24 × 7 |
| Email | General enquiries and support requests | 24 × 7 |
| Telephone | Immediate technical assistance | Business Hours (24 × 7 for Critical Incidents) |
| Live Chat | Real-time assistance | Business Hours |
| WhatsApp Business (Optional) | Basic enquiries and notifications | Business Hours |
| Remote Support Session | Technical troubleshooting | As Required |

All support requests received outside business hours shall be logged automatically and processed according to their assigned priority.

**5.4 Support Hours**

**Standard Business Support**

| Day | Hours |
|---|---|
| Monday | 8:00 AM – 6:00 PM WAT |
| Tuesday | 8:00 AM – 6:00 PM WAT |
| Wednesday | 8:00 AM – 6:00 PM WAT |
| Thursday | 8:00 AM – 6:00 PM WAT |
| Friday | 8:00 AM – 6:00 PM WAT |

**Extended Support**

Critical Priority incidents affecting invoice submission, platform availability, authentication, or statutory compliance shall receive **24 hours × 7 days** support.

### 5.5 Support Request Categories

The Service Desk shall classify incoming requests into the following categories:

**Incident**

An unplanned interruption or reduction in the quality of a service.

Examples include:

- Users unable to log in.
- Invoice submission failures.
- System errors.
- Performance degradation.
- API failures.

**Service Request**

A request for information, advice, or a standard operational activity.

Examples include:

- Password reset.
- User creation.
- Role assignment.
- Report generation.
- Account unlocking.

**Problem**

The investigation and elimination of the root cause of recurring incidents.

Examples include:

- Repeated invoice validation failures.
- Frequent API timeout issues.
- Database performance degradation.

**Change Request**

A request to modify an existing service.

Examples include:

- New feature deployment.
- Configuration changes.
- User role modifications.
- Integration updates.

**5.6 Incident Severity Levels**

Each incident shall be assigned a severity level based on its impact and urgency.

**Priority 1 – Critical**

**Description**

A complete outage or severe disruption preventing taxpayers from carrying out statutory electronic invoicing obligations.

**Examples**

- ERP unavailable.
- Login service unavailable.
- Invoice submission unavailable.
- Database failure.
- Cybersecurity incident affecting production.

**Business Impact**

Severe

Immediate business disruption.

**Priority 2 – High**

**Description**

Major functionality affected with no acceptable workaround.

**Examples**

- Invoice validation failure.
- API integration failure.
- Payment processing unavailable.
- Reports unavailable.

**Business Impact**

High

Significant operational disruption.

**Priority 3 – Medium**

**Description**

Partial loss of functionality where acceptable workarounds exist.

Examples:

- Slow report generation.
- Email notification delays.
- Minor user interface defects.
- Printing issues.

**Priority 4 – Low**

**Description**

Minor issues having limited operational impact.

Examples:

- Cosmetic interface issues.
- Documentation requests.
- Enhancement suggestions.

- User guidance.

### 5.7 Response and Resolution Matrix

The Service Provider shall acknowledge and resolve incidents within the following target times.

| Priority | Initial Response | Work Commences | Target Resolution |
|---|---|---|---|
| Critical | 15 Minutes | Immediately | Within 4 Hours |
| High | 30 Minutes | Within 30 Minutes | Within 8 Hours |
| Medium | 2 Hours | Within 4 Hours | Within 24 Hours |
| Low | 4 Business Hours | Next Business Day | Within 48 Hours |

Where the target resolution cannot be achieved, the Service Provider shall communicate the reason, provide interim updates, and agree a revised resolution timeline with the customer.

### 5.8 Ticket Lifecycle

Every support ticket shall progress through the following lifecycle:

1. Ticket Logged
2. Ticket Acknowledged
3. Initial Assessment
4. Priority Assigned
5. Investigation
6. Root Cause Analysis
7. Resolution Implemented
8. Customer Validation
9. Ticket Closed
10. Post-Incident Review (where applicable)

All lifecycle activities shall be recorded in the Service Management System.

### 5.9 Escalation Procedure

Where an incident cannot be resolved within the expected timeframe, it shall be escalated as follows.

| Escalation Level | Responsible Team | Typical Responsibility |
|---|---|---|
| Level 1 | Service Desk | Ticket logging, basic troubleshooting, user assistance |
| Level 2 | Application Support | Functional issues, ERP configuration, invoice processing |
| Level 3 | Engineering Team | Software defects, API integration, database issues |
| Level 4 | Infrastructure Team | Network, servers, cloud platform, storage |
| Level 5 | Executive Management | Critical incidents, major outages, regulatory matters |

Escalations shall be based on incident severity, elapsed resolution time, customer impact, and regulatory obligations.

### 5.10 Customer Communication

The Service Provider shall keep customers informed throughout the incident lifecycle.

Communication shall include:

- Acknowledgement of incident receipt.
- Confirmation of assigned priority.
- Investigation progress updates.
- Estimated resolution time.
- Notification upon resolution.
- Post-incident summary for major incidents.

For Critical incidents, updates shall be provided at least every **30 minutes** until service restoration.

### 5.11 Major Incident Management

A Major Incident is any event that significantly affects multiple customers or prevents taxpayers from fulfilling statutory obligations.

Examples include:

- Nationwide ERP outage.
- Database corruption.
- Widespread authentication failure.
- Failure of invoice transmission to the Nigeria e-Invoicing platform.
- Significant cybersecurity incident.

For every Major Incident, the Service Provider shall:

1. Activate the Major Incident Response Team.
2. Notify affected customers promptly.
3. Provide regular status updates.
4. Restore service as quickly as possible.
5. Conduct a Root Cause Analysis (RCA).
6. Issue a Post-Incident Report detailing the cause, actions taken, and preventive measures.

### 5.12 Customer Satisfaction

The Service Provider shall measure customer satisfaction to support continual improvement.

Methods include:

- Ticket closure surveys.
- Quarterly customer satisfaction surveys.

- Net Promoter Score (NPS).
- Feedback forms.
- Service review meetings with key customers.

Feedback shall be analysed and used to improve service quality, processes, training, and customer experience.

### 5.13 Service Review Meetings

The Service Provider shall conduct periodic service review meetings with designated customer representatives to evaluate service performance.

Topics may include:

- SLA achievement.
- Incident trends.
- Recurring issues.
- Planned changes.
- Capacity planning.
- Security updates.
- Customer feedback.
- Continuous improvement initiatives.

Review meetings shall normally be held **quarterly**, or more frequently where required.

### 5.14 Documentation and Knowledge Base

To enable self-service and reduce incident resolution times, the Service Provider shall maintain a knowledge base containing:

- User guides.
- Frequently Asked Questions (FAQs).
- Troubleshooting articles.
- Release notes.

- Configuration guides.
- Integration documentation.
- Security advisories.
- Best practice recommendations.

The knowledge base shall be reviewed and updated regularly to reflect system enhancements and recurring support issues.

## Chapter 6 – Incident Management and Problem Management

### 6.1 Introduction

The Service Provider shall maintain a formal Incident Management and Problem Management process to ensure that service interruptions affecting the ERP platform are detected, recorded, investigated, resolved, and reviewed in a consistent and controlled manner.

The primary objective of Incident Management is to restore normal service operation as quickly as possible while minimizing the impact on taxpayers and ensuring compliance with statutory e-invoicing obligations.

Problem Management complements Incident Management by identifying and eliminating the root causes of recurring incidents, thereby reducing future disruptions and improving overall service quality.

These processes apply to all production services, infrastructure components, integrations, applications, databases, and security systems supporting the ERP platform.

### 6.2 Objectives

The objectives of the Incident and Problem Management process are to:

- Restore services within agreed SLA timelines.
- Minimize operational disruption to taxpayers.
- Ensure all incidents are recorded and tracked.
- Classify incidents according to business impact.
- Escalate incidents appropriately.
- Perform root cause analysis for recurring issues.
- Prevent repeat incidents through corrective and preventive actions.
- Maintain comprehensive incident records for audit and compliance purposes.
- Support continual service improvement.

### 6.3 Scope

This process applies to all incidents affecting:

- ERP Web Portal
- User Authentication Services
- Invoice Generation
- Invoice Validation
- Invoice Transmission
- API Gateway
- Database Services
- Reporting Services
- Notification Services
- Integration Services
- Cloud Infrastructure
- Network Connectivity
- Information Security Controls

### 6.4 Incident Definition

An **Incident** is any unplanned interruption to an IT service or any reduction in the quality of a service that impacts the ability of taxpayers to use the ERP platform.

Examples include:

- System outage.
- Invoice submission failure.
- Login failure.
- Slow application performance.
- API timeout.
- Database connection error.

- Corrupted invoice data.
- Security alert.
- Integration failure.
- Authentication error.

### 6.5 Incident Detection

Incidents may be identified through one or more of the following channels:

| Source | Description |
|---|---|
| Customer Reports | Users report issues through the Service Desk, portal, email, or telephone. |
| Automated Monitoring | Monitoring tools detect failures and generate alerts automatically. |
| System Logs | Errors identified from application, database, or infrastructure logs. |
| Security Monitoring | Security tools detect suspicious or malicious activities. |
| API Monitoring | Failed API calls or abnormal response times trigger alerts. |
| Scheduled Health Checks | Routine inspections identify potential issues before they affect customers. |

All detected incidents shall be recorded in the Service Management System.

### 6.6 Incident Logging

Every incident shall be assigned a unique reference number and the following information shall be captured:

- Incident ID
- Date and Time Reported
- Reporter Name
- Customer Organization

- Contact Information
- Affected Service
- Description of Incident
- Symptoms Observed
- Business Impact
- Priority
- Assigned Support Team
- Current Status
- Resolution Details
- Closure Date
- Root Cause (where applicable)

Incident records shall be retained in accordance with regulatory and audit requirements.

### 6.7 Incident Classification

Incidents shall be classified to facilitate effective routing and reporting.

**Functional Classification**

- Application
- Database
- Network
- Security
- Authentication
- Infrastructure
- Integration
- Performance
- Reporting
- User Error

- Third-Party Dependency

**Business Classification**

- Financial Impact
- Operational Impact
- Compliance Impact
- Security Impact
- Customer Experience Impact

### 6.8 Incident Prioritization Matrix

Incident priority shall be determined using the combined assessment of **Business Impact** and **Urgency**.

| Business Impact | Urgency | Priority |
|---|---|---|
| High | High | Critical |
| High | Medium | High |
| Medium | Medium | Medium |
| Low | Low | Low |

The assigned priority determines the response and resolution targets defined in Chapter 5.

### 6.9 Incident Management Workflow

The standard Incident Management process consists of the following stages:

1. Incident Detection
2. Incident Logging
3. Initial Diagnosis
4. Priority Assignment
5. Investigation
6. Escalation (if required)

7. Resolution and Recovery
8. Customer Verification
9. Incident Closure
10. Post-Incident Review (for Major Incidents)

All stages shall be documented within the Service Management System to provide an auditable history.

**6.10 Major Incident Management**

A **Major Incident** is any incident that causes significant disruption to critical services or affects multiple customers.

Examples include:

- Complete ERP outage.
- Failure of invoice transmission to the Nigeria e-Invoicing platform.
- Authentication service failure.
- Database corruption.
- Ransomware or other cybersecurity attack.
- Cloud infrastructure failure.

For a Major Incident, the Service Provider shall:

1. Declare the incident as "Major".
2. Activate the Major Incident Response Team.
3. Notify executive management.
4. Inform affected customers.
5. Provide updates at intervals not exceeding 30 minutes.
6. Prioritize restoration of service.
7. Conduct a formal Root Cause Analysis (RCA).
8. Produce a Post-Incident Report within five (5) business days.

### 6.11 Escalation Process

Where an incident cannot be resolved within the expected timeframe or requires specialist expertise, it shall be escalated through the following levels:

| Escalation Level | Responsible Team | Responsibility |
|---|---|---|
| Level 1 | Service Desk | Initial logging, diagnosis, and resolution of common issues |
| Level 2 | Application Support | ERP configuration, functional issues, business process support |
| Level 3 | Software Engineering | Software defects, API integration, database issues |
| Level 4 | Infrastructure Operations | Servers, storage, cloud services, networking |
| Level 5 | Executive Management | Critical incidents, regulatory issues, customer communications |

Escalation decisions shall consider business impact, urgency, regulatory obligations, and elapsed resolution time.

### 6.12 Problem Management

Problem Management focuses on identifying and removing the underlying causes of recurring incidents to prevent future disruptions.

A Problem may be initiated when:

- Similar incidents recur frequently.
- No permanent fix exists.
- Multiple incidents share a common cause.
- An incident has a significant business impact.

Each Problem shall be assigned a unique Problem Record and tracked through to closure.

### 6.13 Root Cause Analysis (RCA)

For Major Incidents and recurring Problems, a formal Root Cause Analysis shall be conducted.

The RCA process shall include:

1. Collection of relevant logs and evidence.
2. Reconstruction of the incident timeline.
3. Identification of contributing factors.
4. Determination of the root cause.
5. Assessment of business impact.
6. Development of corrective actions.
7. Identification of preventive measures.
8. Approval of the RCA report by the Service Delivery Manager.

RCA reports shall be retained for audit purposes and reviewed during service improvement meetings.

### 6.14 Known Error Database (KEDB)

The Service Provider shall maintain a **Known Error Database (KEDB)** containing:

- Problem ID
- Description of the issue
- Root cause
- Temporary workaround
- Permanent resolution
- Related incidents
- Status
- Date resolved

The KEDB shall be used by support personnel to accelerate diagnosis and resolution of recurring issues.

### 6.15 Corrective and Preventive Actions (CAPA)

Following the resolution of a Problem, the Service Provider shall implement appropriate Corrective and Preventive Actions (CAPA).

Examples include:

- Software patches.
- Configuration updates.
- Infrastructure upgrades.
- Process improvements.
- Additional staff training.
- Monitoring enhancements.
- Documentation updates.

CAPA activities shall be tracked to completion and reviewed for effectiveness.

### 6.16 Incident Closure

An incident may be closed only when:

- Service has been fully restored.
- The customer has been informed of the resolution.
- Resolution details have been documented.
- Related records have been updated.
- Any follow-up actions have been assigned.
- The closure has been approved by the responsible support team.

Closed incidents may be reopened if the issue recurs within a reasonable period.

### 6.17 Reporting and Review

The Service Provider shall produce periodic reports on incident and problem management, including:

- Number of incidents by priority.

- Average response time.
- Average resolution time.
- Major incident summaries.
- Root cause trends.
- Repeat incident analysis.
- Problem resolution statistics.
- Customer satisfaction metrics.

These reports shall be reviewed by management to identify opportunities for continual service improvement.

## Chapter 7 – Change Management and Release Management

### 7.1 Introduction

The Service Provider recognizes that changes to software, infrastructure, databases, integrations, security configurations, and operational procedures are necessary to maintain, enhance, and secure the ERP platform. However, unmanaged changes can introduce service disruptions, security vulnerabilities, compliance risks, and operational instability.

Accordingly, the Service Provider shall operate a formal Change Management and Release Management process to ensure that all changes are planned, assessed, tested, approved, implemented, and reviewed in a controlled manner.

This process seeks to minimize the risk of service interruption while enabling the continuous improvement of the ERP platform and supporting compliance with applicable FIRS e-Invoicing requirements.

### 7.2 Objectives

The objectives of the Change Management process are to:

- Ensure all changes are properly evaluated before implementation.
- Minimize service disruptions resulting from changes.
- Protect the confidentiality, integrity, and availability of taxpayer data.
- Ensure regulatory compliance is maintained following system changes.
- Provide full traceability of all changes.
- Improve system stability and reliability.
- Reduce emergency changes through effective planning.
- Ensure rollback procedures are available for failed implementations.

### 7.3 Scope

This policy applies to changes affecting:

- ERP Application Software

- Database Structure
- API Integrations
- Invoice Processing Engine
- Authentication Services
- User Roles and Permissions
- Cloud Infrastructure
- Network Devices
- Firewalls
- Security Configurations
- Reporting Services
- Backup Infrastructure
- Disaster Recovery Systems
- Third-Party Integrations
- Production Configurations

### 7.4 Change Categories

All changes shall be classified into one of the following categories.

#### 7.4.1 Standard Changes

Standard Changes are routine, low-risk, pre-approved changes performed according to documented procedures.

Examples include:

- User account creation.
- Password reset.
- Updating contact details.
- Scheduled security patch installation.
- Routine certificate renewal.

- Scheduled backups.

These changes require minimal approval and follow predefined procedures.

### 7.4.2 Normal Changes

Normal Changes involve modifications that require formal assessment, testing, and approval before implementation.

Examples include:

- New ERP functionality.
- Database schema modifications.
- API enhancements.
- Performance optimizations.
- Integration with external systems.
- New reporting features.

These changes require Change Advisory Board (CAB) approval.

### 7.4.3 Emergency Changes

Emergency Changes are implemented to address critical incidents or security risks that cannot wait for the standard approval process.

Examples include:

- Critical security vulnerability.
- Active cyberattack.
- Production system failure.
- Critical invoice processing defect.
- Regulatory change requiring immediate implementation.

Emergency Changes shall be documented and reviewed retrospectively after implementation.

### 7.5 Change Management Process

Every change shall follow the lifecycle below.

1. Change Request Submission.
2. Initial Review.
3. Impact Assessment.
4. Risk Assessment.
5. Technical Design.
6. Testing.
7. Change Advisory Board Review.
8. Approval.
9. Implementation Planning.
10. Deployment.
11. Validation.
12. Post-Implementation Review.
13. Documentation Update.
14. Closure.

No production change shall be implemented without following the approved process unless classified as an Emergency Change.

### 7.6 Change Request

Every proposed change shall be documented using a Change Request (CR) containing:

- Change Request ID.
- Date Submitted.
- Requestor.
- Description of Change.
- Business Justification.

- Affected Services.
- Technical Impact.
- Security Impact.
- Compliance Impact.
- Estimated Downtime.
- Rollback Plan.
- Testing Plan.
- Proposed Implementation Date.
- Risk Rating.
- Required Approvals.

Each Change Request shall be uniquely identified and retained for audit purposes.

**7.7 Change Impact Assessment**

Before approval, every change shall undergo an assessment to determine its impact on:

- Service Availability.
- Performance.
- Data Integrity.
- Security.
- Customer Operations.
- Integration Services.
- Regulatory Compliance.
- Disaster Recovery.
- Business Continuity.

The outcome of the assessment shall determine the level of approval required.

### 7.8 Risk Assessment

Each proposed change shall be assigned a risk level based on:

- Complexity.
- Scope.
- Business Impact.
- Security Implications.
- Likelihood of Failure.
- Recovery Complexity.
- Customer Impact.

**Risk Classification**

| Risk Level | Description | Approval Required |
|---|---|---|
| Low | Minimal operational impact | Service Manager |
| Medium | Moderate operational impact | Change Advisory Board |
| High | Significant business or security impact | CAB + Executive Approval |
| Critical | High regulatory or operational impact | Executive Management |

### 7.9 Change Advisory Board (CAB)

The Service Provider shall maintain a Change Advisory Board (CAB) responsible for reviewing significant changes.

The CAB shall include representatives from:

- Service Delivery.
- Software Development.
- Infrastructure Operations.
- Information Security.
- Compliance.
- Quality Assurance.

- Business Operations.

The CAB shall review:

- Business justification.
- Risk assessment.
- Security impact.
- Compliance impact.
- Testing evidence.
- Rollback procedures.
- Implementation schedule.

CAB meetings shall be held regularly, with emergency sessions convened when required.

**7.10 Testing Requirements**

No production deployment shall occur unless appropriate testing has been completed.

Testing shall include, where applicable:

- Unit Testing.
- Integration Testing.
- System Testing.
- User Acceptance Testing (UAT).
- Performance Testing.
- Security Testing.
- Regression Testing.
- API Testing.
- Failover Testing.

Testing results shall be documented and approved prior to deployment.

### 7.11 Release Management

Release Management ensures that approved changes are packaged, tested, and deployed in a controlled and repeatable manner.

Release activities include:

- Release planning.
- Build management.
- Version control.
- Configuration verification.
- Deployment scheduling.
- Production deployment.
- Validation.
- Customer notification.

Each release shall be assigned a unique version number and accompanied by release notes detailing new features, resolved issues, known limitations, and deployment instructions.

### 7.12 Deployment Procedures

Deployments to the production environment shall follow documented procedures, including:

1. Pre-deployment backup.
2. Verification of deployment package.
3. Change approval confirmation.
4. Notification to stakeholders.
5. Deployment execution.
6. Post-deployment validation.
7. Functional verification.
8. Performance verification.

9. Security verification.
10. Customer communication.

Deployments shall be scheduled to minimize impact on customers, preferably during approved maintenance windows.

### 7.13 Rollback Procedures

A documented rollback plan shall exist for every production change.

The rollback plan shall specify:

- Conditions requiring rollback.
- Steps to restore the previous version.
- Estimated rollback duration.
- Responsible personnel.
- Communication procedures.
- Validation after rollback.

Rollback testing shall be performed for significant releases.

### 7.14 Emergency Change Procedure

Where an Emergency Change is required, the following minimum controls shall apply:

- Approval by an authorized senior manager.
- Documentation of the reason for the emergency.
- Implementation by authorized personnel.
- Validation after deployment.
- Notification to affected customers where appropriate.
- Retrospective CAB review within five (5) business days.

### 7.15 Documentation and Audit

The Service Provider shall maintain comprehensive records of all changes, including:

- Approved Change Requests.
- CAB meeting minutes.
- Testing evidence.
- Deployment logs.
- Rollback records.
- Release notes.
- Post-Implementation Reviews.
- Customer communications.

Change records shall be retained in accordance with legal, regulatory, and organizational retention policies.

### 7.16 Key Performance Indicators (KPIs)

The effectiveness of Change and Release Management shall be monitored using the following KPIs:

| KPI | Target |
|---|---|
| Successful Change Implementation Rate | ≥ 98% |
| Emergency Changes | ≤ 5% of Total Changes |
| Failed Changes Requiring Rollback | ≤ 2% |
| Changes Implemented Within Approved Window | ≥ 99% |
| Post-Implementation Incidents | ≤ 2% of Releases |
| Release Documentation Completion | 100% |

These KPIs shall be reviewed monthly and used to drive continual improvement.

### 7.17 Continual Improvement

The Service Provider shall periodically review the Change Management and Release Management process to identify opportunities for improvement. Reviews shall consider:

- Change success rates.
- Customer feedback.
- Incident trends.
- Audit findings.
- Security assessments.
- Regulatory updates.
- Lessons learned from previous releases.

Recommendations shall be documented, approved, and implemented through the organization's continual service improvement programme.

## Chapter 8 – Information Security Management

### 8.1 Introduction

The Service Provider recognizes that information security is fundamental to maintaining the trust of taxpayers, protecting confidential business information, and ensuring compliance with statutory and regulatory obligations.

Accordingly, the Service Provider shall establish, implement, maintain, and continually improve an Information Security Management System (ISMS) designed to protect the confidentiality, integrity, and availability of information processed, stored, and transmitted through the ERP platform.

The Information Security Management framework applies to all personnel, contractors, consultants, third-party service providers, systems, applications, infrastructure, cloud environments, databases, APIs, and supporting technologies involved in the delivery of electronic invoicing services.

### 8.2 Security Objectives

The objectives of the Information Security Management Program are to:

- Protect taxpayer information from unauthorized access, disclosure, alteration, or destruction.
- Ensure continuous availability of electronic invoicing services.
- Maintain the integrity and accuracy of financial and tax information.
- Comply with all applicable regulatory and contractual obligations.
- Prevent, detect, respond to, and recover from cybersecurity incidents.
- Promote a culture of security awareness throughout the organization.
- Continuously improve the organization's cybersecurity posture.

### 8.3 Information Security Governance

The Service Provider shall establish an Information Security Governance framework that defines accountability, oversight, and decision-making responsibilities.

**Governance Structure**

| Role | Responsibilities |
|---|---|
| Board / Executive Management | Provide strategic oversight and approve security policies. |
| Chief Information Security Officer (CISO) / Information Security Manager | Develop and manage the security program. |
| IT Operations Team | Implement technical security controls and maintain infrastructure. |
| Software Development Team | Ensure secure software development and remediation of vulnerabilities. |
| Compliance Officer | Monitor compliance with legal and regulatory requirements. |
| Internal Audit | Conduct independent reviews of security controls. |
| All Employees | Comply with security policies and report security incidents. |

Information security responsibilities shall be documented and communicated to all personnel.

**8.4 Security Policies**

The Service Provider shall maintain documented information security policies covering:

- Information Security Policy
- Acceptable Use Policy
- Password Policy
- Access Control Policy
- Data Classification Policy
- Cryptographic Policy
- Secure Development Policy

- Backup Policy
- Incident Response Policy
- Business Continuity Policy
- Vendor Security Policy
- Remote Access Policy
- Mobile Device Policy
- Logging and Monitoring Policy
- Vulnerability Management Policy

Policies shall be reviewed at least annually or whenever significant changes occur.

### 8.5 Identity and Access Management

Access to ERP services shall be restricted to authorized users based on the principle of **least privilege** and **need-to-know**.

#### Authentication Controls

The ERP platform shall support:

- Unique user accounts.
- Strong password enforcement.
- Multi-Factor Authentication (MFA) for privileged users.
- Password expiry and history controls.
- Account lockout after repeated failed login attempts.
- Session timeout after inactivity.
- Secure password reset procedures.

#### Authorization

Access rights shall be granted according to defined roles.

Typical roles include:

- System Administrator

- Finance Officer
- Sales Officer
- Auditor
- Compliance Officer
- Customer Support Officer
- Read-Only User

Role assignments shall be reviewed periodically.

### 8.6 Password Management

Passwords shall comply with the following minimum requirements:

| Requirement | Standard |
|---|---|
| Minimum Length | 12 Characters |
| Uppercase Letters | Required |
| Lowercase Letters | Required |
| Numbers | Required |
| Special Characters | Required |
| Password History | Last 10 Passwords |
| Maximum Validity | 90 Days |
| Account Lockout | After 5 Failed Attempts |
| Lockout Duration | 30 Minutes |

Passwords shall never be stored in plain text and shall be protected using industry-standard cryptographic hashing techniques.

### 8.7 Data Classification

Information processed by the ERP platform shall be classified to ensure appropriate protection.

| Classification | Description | Examples |
|---|---|---|
| Public | Information approved for public disclosure. | Marketing materials, public notices. |
| Internal | Operational information for internal use. | Internal procedures, training documents. |
| Confidential | Sensitive business information. | Contracts, financial records. |
| Restricted | Highly sensitive information requiring the highest level of protection. | Taxpayer records, authentication credentials, encryption keys. |

Handling procedures shall be defined for each classification level.

### 8.8 Cryptography and Encryption

Sensitive information shall be protected using strong cryptographic controls.

**Data in Transit**

- Transport Layer Security (TLS) version 1.2 or higher shall be used for all communications.
- APIs shall require secure HTTPS connections.
- Certificates shall be issued by trusted Certificate Authorities and renewed before expiration.

**Data at Rest**

- Sensitive databases, file systems, and backups shall be encrypted using AES-256 or an equivalent industry-recognized encryption standard.
- Encryption keys shall be securely generated, stored, rotated, and retired in accordance with documented key management procedures.

### 8.9 Network Security

The Service Provider shall implement layered network security controls to protect the ERP environment.

Controls include:

- Firewalls.
- Network segmentation.
- Intrusion Detection and Prevention Systems (IDS/IPS).
- Secure VPN for administrative access.
- DDoS protection.
- Secure DNS services.
- Web Application Firewall (WAF).
- Continuous network monitoring.

Firewall rules shall be reviewed regularly and unauthorized network traffic shall be blocked.

### 8.10 Endpoint Security

All servers, workstations, and administrative endpoints shall be protected through:

- Anti-malware software.
- Endpoint Detection and Response (EDR).
- Disk encryption.
- Device hardening.
- Patch management.
- Application whitelisting (where appropriate).
- USB and removable media controls.

Only authorized and managed devices shall be permitted to access administrative systems.

### 8.11 Secure Software Development

The ERP platform shall be developed using secure software development practices throughout the software development lifecycle (SDLC).

Key controls include:

- Secure coding standards.
- Peer code reviews.
- Static Application Security Testing (SAST).
- Dynamic Application Security Testing (DAST).
- Dependency and software composition analysis.
- Vulnerability remediation before production release.
- Security approval as part of the release process.

Security requirements shall be incorporated into system design, development, testing, and deployment activities.

### 8.12 Vulnerability Management

The Service Provider shall maintain a vulnerability management program to identify, assess, and remediate security weaknesses.

The program shall include:

- Routine vulnerability scanning.
- Penetration testing.
- Patch management.
- Risk assessment.
- Tracking of remediation activities.
- Verification testing after remediation.

**Patch Targets**

| Severity | Target Remediation Time |
|---|---|
| Critical | Within 24 Hours |
| High | Within 7 Days |
| Medium | Within 30 Days |
| Low | Within 90 Days |

### 8.13 Logging and Monitoring

Security-relevant events shall be logged and monitored to detect unauthorized or suspicious activities.

Examples include:

- Successful and failed login attempts.
- Privileged account usage.
- User administration activities.
- Invoice creation, modification, and submission.
- API authentication events.
- Database access.
- Configuration changes.
- Security alerts.

Logs shall be protected from unauthorized modification and retained in accordance with regulatory and business requirements.

### 8.14 Security Incident Response

The Service Provider shall maintain a documented Security Incident Response Plan.

The plan shall include:

1. Preparation.

2. Detection and Analysis.
3. Containment.
4. Eradication.
5. Recovery.
6. Post-Incident Review.

Security incidents shall be recorded, investigated, and reported to appropriate stakeholders. Where legally required, regulatory authorities and affected customers shall be notified within applicable timeframes.

**8.15 Security Awareness and Training**

All personnel with access to the ERP environment shall receive information security awareness training upon employment and at least annually thereafter.

Training topics shall include:

- Password security.
- Phishing awareness.
- Data protection obligations.
- Acceptable use.
- Secure handling of taxpayer information.
- Incident reporting procedures.
- Social engineering threats.

Participation shall be recorded and training effectiveness periodically evaluated.

**8.16 Third-Party Security**

Third-party vendors providing hosting, cloud infrastructure, payment services, or other supporting services shall be subject to appropriate due diligence and security assessments.

The Service Provider shall ensure that contracts with third parties include appropriate security and confidentiality obligations.

### 8.17 Security Audits and Continuous Improvement

The Information Security Management System shall be reviewed periodically through:

- Internal audits.
- External audits (where applicable).
- Vulnerability assessments.
- Penetration testing.
- Management reviews.
- Risk assessments.
- Lessons learned from incidents.

Audit findings shall be documented, corrective actions assigned, and progress monitored until completion.

## Chapter 9 – Data Protection, Privacy, and Regulatory Compliance

### 9.1 Introduction

The Service Provider is committed to protecting the privacy and personal information of taxpayers, customers, employees, business partners, and other data subjects whose information is processed through the Enterprise Resource Planning (ERP) platform.

This chapter establishes the principles, controls, and operational measures implemented by the Service Provider to ensure compliance with the **Nigeria Data Protection Act (NDPA), 2023**, applicable regulations issued by the **Nigeria Data Protection Commission (NDPC)**, the **Federal Inland Revenue Service (FIRS)** Electronic Invoicing Framework, and other relevant statutory obligations.

The Service Provider recognizes that taxpayer information is highly sensitive and shall implement appropriate technical and organizational measures to ensure its confidentiality, integrity, availability, and lawful processing throughout its lifecycle.

### 9.2 Objectives

The objectives of the Data Protection and Privacy Programme are to:

- Ensure the lawful, fair, and transparent processing of personal data.
- Protect taxpayer information from unauthorized access, disclosure, alteration, or loss.
- Demonstrate compliance with the NDPA and applicable FIRS requirements.
- Promote accountability in the processing of personal information.
- Define clear responsibilities for data protection.
- Minimize privacy risks through appropriate safeguards.
- Support data subject rights.
- Ensure secure retention and disposal of information.

### 9.3 Scope

This policy applies to all personal data processed by the ERP platform, including information relating to:

- Taxpayers.
- Customers.
- Suppliers.
- Employees.
- Contractors.
- Business Partners.
- Authorized Users.
- Support Personnel.

The policy covers data processed through:

- ERP Applications.
- Mobile Applications (where applicable).
- Customer Portal.
- APIs.
- Cloud Infrastructure.
- Databases.
- Backup Systems.
- Reporting Platforms.
- Support Systems.

**9.4 Applicable Legal and Regulatory Framework**

The Service Provider shall comply with all applicable legal and regulatory requirements, including but not limited to:

- Nigeria Data Protection Act (NDPA), 2023.
- Regulations and guidance issued by the Nigeria Data Protection Commission (NDPC).
- Federal Inland Revenue Service (FIRS) Electronic Invoicing Framework.
- Applicable tax laws and regulations.

- Electronic transaction legislation.
- Contractual obligations agreed with customers.

The Service Provider shall monitor regulatory developments and update its policies and procedures as necessary.

### 9.5 Data Protection Principles

The Service Provider shall process personal data in accordance with the following principles:

**Lawfulness, Fairness, and Transparency**

Personal data shall be processed only where there is a lawful basis, in a manner that is fair to the data subject, and with appropriate transparency regarding the processing activities.

**Purpose Limitation**

Personal data shall be collected for specified, explicit, and legitimate purposes and shall not be processed in a manner incompatible with those purposes.

**Data Minimization**

Only personal data that is adequate, relevant, and limited to what is necessary for the intended purpose shall be collected and processed.

**Accuracy**

Reasonable steps shall be taken to ensure that personal data is accurate, complete, and kept up to date.

**Storage Limitation**

Personal data shall be retained only for as long as necessary to fulfil legal, regulatory, contractual, and operational requirements.

**Integrity and Confidentiality**

Appropriate technical and organizational measures shall be implemented to protect personal data against unauthorized access, disclosure, alteration, accidental loss, or destruction.

**Accountability**

The Service Provider shall maintain records and evidence demonstrating compliance with applicable data protection obligations.

### 9.6 Categories of Data Processed

The ERP platform may process the following categories of information:

**Customer Information**

- Organization Name.
- Registered Address.
- Contact Information.
- Taxpayer Identification Number (TIN).
- Customer Identification Details.

**User Information**

- Name.
- Job Title.
- Email Address.
- Telephone Number.
- User ID.
- Login History.

**Financial Information**

- Invoice Details.
- Payment Information.
- Tax Calculations.
- Transaction History.
- Account Statements.

**Technical Information**

- IP Address.
- Browser Type.
- Device Information.
- Session Logs.
- API Requests.
- Audit Logs.

Only information necessary for the delivery of ERP and electronic invoicing services shall be processed.

**9.7 Lawful Basis for Processing**

The Service Provider shall ensure that each processing activity is supported by an appropriate lawful basis, such as:

- Performance of a contract.
- Compliance with a legal obligation.
- Legitimate business interests, balanced against the rights and freedoms of the data subject.
- Consent, where required.
- Protection of vital interests, where applicable.

The lawful basis shall be documented for each category of processing.

**9.8 Data Subject Rights**

The Service Provider shall establish procedures to enable data subjects to exercise their rights under applicable law, including:

- Right to be informed.
- Right of access.
- Right to rectification.

- Right to erasure, where applicable.
- Right to restrict processing.
- Right to object to processing, where applicable.
- Right to data portability, where applicable.
- Right to lodge a complaint with the appropriate supervisory authority.

Requests from data subjects shall be acknowledged promptly and handled within the timeframes prescribed by law.

**9.9 Data Retention**

Personal data shall be retained only for as long as necessary to meet legal, regulatory, contractual, and business requirements.

Indicative retention periods are as follows:

| Data Category | Minimum Retention Period |
|---|---|
| Electronic Invoices | 7 Years |
| Financial Records | 7 Years |
| Audit Logs | 7 Years |
| User Activity Logs | 2 Years |
| Customer Account Records | Duration of Contract + 7 Years |
| Support Tickets | 3 Years |
| Security Incident Records | 5 Years |
| Backup Archives | As defined in the Backup Policy |

Upon expiration of the retention period, data shall be securely deleted or anonymized, unless a longer retention period is required by law or legal proceedings.

### 9.10 Cross-Border Data Transfers

Where personal data is transferred outside Nigeria, the Service Provider shall ensure that appropriate safeguards are in place, including:

- Transfer to jurisdictions providing an adequate level of data protection; or
- Contractual safeguards and technical measures that ensure equivalent protection.

Cross-border transfers shall be documented and periodically reviewed.

### 9.11 Privacy by Design and by Default

Privacy considerations shall be integrated into the design, development, deployment, and maintenance of the ERP platform.

This includes:

- Data minimization.
- Role-based access controls.
- Encryption.
- Secure defaults.
- Logging and monitoring.
- Regular privacy impact assessments for significant changes.

### 9.12 Data Breach Management

Any suspected or confirmed personal data breach shall be managed in accordance with the Service Provider's Incident Response Plan.

The process shall include:

1. Identification and containment of the breach.
2. Assessment of the scope and impact.
3. Notification to internal stakeholders.
4. Notification to the Nigeria Data Protection Commission and other relevant authorities where legally required.

5. Communication with affected customers and data subjects, where appropriate.
6. Investigation and root cause analysis.
7. Implementation of corrective and preventive actions.
8. Documentation and post-incident review.

All breaches shall be recorded in a Data Breach Register.

### 9.13 Data Protection Roles and Responsibilities

The Service Provider shall assign clear responsibilities for data protection.

| Role | Responsibility |
|---|---|
| Managing Director | Overall accountability for compliance. |
| Data Protection Officer (DPO) | Oversight of data protection programme and advisory role. |
| Information Security Manager | Implementation of technical security controls. |
| Compliance Officer | Monitoring regulatory compliance. |
| Department Heads | Ensuring compliance within their business units. |
| Employees | Following policies and reporting suspected breaches. |

### 9.14 Compliance Monitoring and Audit

The Service Provider shall conduct periodic reviews to verify compliance with this chapter and applicable legal obligations.

Activities may include:

- Internal compliance audits.
- Privacy impact assessments.
- Security assessments.
- Review of data processing activities.
- Monitoring of data subject requests.

- Review of third-party processors.
- Management review meetings.

Findings shall be documented, and corrective actions tracked to completion.

**9.15 Continual Improvement**

The Service Provider shall regularly review and enhance its data protection and privacy programme to reflect:

- Changes in legislation.
- Regulatory guidance.
- Technology developments.
- Security threats.
- Audit findings.
- Customer feedback.
- Lessons learned from incidents.

Improvement actions shall be documented and monitored as part of the organization's governance framework.

## Chapter 10 – Backup, Disaster Recovery, and Business Continuity

### 10.1 Introduction

The Service Provider recognizes that uninterrupted access to electronic invoicing services is critical to taxpayers' statutory obligations and business operations. To ensure resilience, the Service Provider has established comprehensive Backup, Disaster Recovery (DR), and Business Continuity (BC) arrangements designed to minimize service disruption, safeguard taxpayer information, and restore services within agreed recovery objectives.

This chapter defines the policies, procedures, and technical controls implemented to protect the ERP platform against data loss, infrastructure failure, cyber incidents, and other disruptive events.

### 10.2 Objectives

The objectives of the Backup, Disaster Recovery, and Business Continuity Programme are to:

- Ensure the availability of electronic invoicing services during disruptive events.
- Protect taxpayer data from accidental or malicious loss.
- Minimize downtime following system failures.
- Restore critical services within defined Recovery Time Objectives (RTOs).
- Limit data loss through defined Recovery Point Objectives (RPOs).
- Maintain compliance with legal and regulatory obligations.
- Regularly test recovery capabilities to ensure effectiveness.

### 10.3 Scope

This programme applies to all critical components supporting the ERP platform, including:

- Application servers.
- Database servers.
- Storage systems.
- API gateways.

- Authentication services.
- Reporting services.
- Integration services.
- Network infrastructure.
- Security appliances.
- Cloud environments.
- Backup repositories.
- Configuration repositories.
- System documentation.

**10.4 Backup Policy**

The Service Provider shall maintain automated backup processes to ensure the integrity and recoverability of all critical business information.

**Backup Principles**

- Backups shall be performed automatically using approved backup solutions.
- Backup integrity shall be verified after each backup operation.
- Backup data shall be encrypted both during transmission and while stored.
- Backup repositories shall be protected against unauthorized access.
- Multiple backup generations shall be retained to support point-in-time recovery.
- Backup failures shall generate alerts for immediate investigation.

**10.5 Backup Schedule**

The following backup schedule shall apply unless otherwise approved by management.

| Backup Type | Frequency | Retention Period |
|---|---|---|
| Transaction Log Backup | Every 15 Minutes | 7 Days |

| Backup Type | Frequency | Retention Period |
|---|---|---|
| Incremental Backup | Daily | 30 Days |
| Full Database Backup | Daily | 90 Days |
| Weekly Full Backup | Weekly | 12 Months |
| Monthly Archive Backup | Monthly | 7 Years |
| Configuration Backup | Daily | 90 Days |
| Application Source Code Repository Backup | Daily | Permanent (Version Controlled) |

Backup schedules shall be reviewed periodically to ensure they remain appropriate for business needs.

**10.6 Backup Storage**

Backups shall be stored using a layered approach to improve resilience.

**Primary Backup Repository**

- Located within the primary production environment.
- Used for operational restores.

**Secondary Backup Repository**

- Stored in a geographically separate location or alternate cloud region.
- Used for disaster recovery scenarios.

**Long-Term Archive**

- Encrypted archival storage.
- Protected against accidental modification or deletion.
- Used to satisfy regulatory retention requirements.

Access to backup media shall be restricted to authorized personnel.

### 10.7 Recovery Objectives

The Service Provider commits to the following recovery objectives for critical ERP services.

| Service | Recovery Time Objective (RTO) | Recovery Point Objective (RPO) |
|---|---|---|
| ERP Web Portal | ≤ 4 Hours | ≤ 15 Minutes |
| Invoice Processing | ≤ 2 Hours | ≤ 15 Minutes |
| Authentication Service | ≤ 2 Hours | ≤ 15 Minutes |
| API Gateway | ≤ 2 Hours | ≤ 15 Minutes |
| Database Services | ≤ 4 Hours | ≤ 15 Minutes |
| Reporting Services | ≤ 8 Hours | ≤ 1 Hour |
| Notification Services | ≤ 8 Hours | ≤ 1 Hour |

The Service Provider shall periodically review these objectives to ensure continued alignment with customer expectations and regulatory requirements.

### 10.8 Disaster Recovery Strategy

The Disaster Recovery Strategy is designed to restore critical ERP services following a disruptive event.

The strategy includes:

- Redundant infrastructure.
- Geographically separated backup locations.
- Cloud-based recovery capabilities.
- Automated infrastructure provisioning where feasible.
- Database replication.
- Secure restoration procedures.
- Prioritized recovery of critical services.

Recovery activities shall follow documented Disaster Recovery Procedures approved by management.

### 10.9 Disaster Recovery Activation

The Disaster Recovery Plan may be activated in response to events including, but not limited to:

- Data centre failure.
- Extended power outage.
- Major network failure.
- Cybersecurity incident (e.g., ransomware).
- Database corruption.
- Natural disaster.
- Fire.
- Flood.
- Civil disturbance.
- Failure of critical cloud infrastructure.

Activation shall be authorized by designated management personnel.

### 10.10 Disaster Recovery Process

The Disaster Recovery process shall include the following stages:

1. Incident Detection.
2. Situation Assessment.
3. Disaster Declaration.
4. Activation of the Disaster Recovery Team.
5. Communication to Stakeholders.
6. Recovery of Critical Infrastructure.
7. Restoration of ERP Services.
8. Validation of Service Availability.
9. Customer Notification.

10. Transition Back to Normal Operations.
11. Post-Disaster Review.

Each stage shall be documented and recorded for audit purposes.

**10.11 Disaster Recovery Team**

The Service Provider shall establish a Disaster Recovery Team comprising representatives from:

- Executive Management.
- Service Delivery.
- Infrastructure Operations.
- Database Administration.
- Software Engineering.
- Information Security.
- Network Operations.
- Compliance.
- Customer Support.

The team shall be responsible for coordinating recovery activities, communicating with stakeholders, and ensuring that recovery objectives are achieved.

**10.12 Business Continuity Management**

The Service Provider shall maintain a Business Continuity Management (BCM) programme to ensure that critical business functions continue during and after disruptive events.

The BCM programme shall include:

- Business Impact Analysis (BIA).
- Risk Assessment.
- Business Continuity Plans.
- Recovery Strategies.

- Crisis Management Procedures.
- Communication Plans.
- Training and Awareness.
- Regular Testing and Exercises.

Business Continuity Plans shall be reviewed at least annually and following significant organizational or technological changes.

**10.13 Crisis Communication**

During a significant disruption, the Service Provider shall communicate promptly with affected customers and stakeholders.

Communication may include:

- Nature of the incident.
- Services affected.
- Expected impact.
- Estimated recovery timeline.
- Interim workarounds (where available).
- Progress updates.
- Confirmation of service restoration.

For major incidents, updates shall be provided at intervals not exceeding one (1) hour unless otherwise agreed.

**10.14 Testing and Exercising**

The Service Provider shall regularly test Backup, Disaster Recovery, and Business Continuity arrangements to ensure effectiveness.

Testing activities may include:

- Backup restoration tests.
- Disaster Recovery simulations.

- Tabletop exercises.
- Failover testing.
- Business Continuity exercises.
- Cyber incident response simulations.

The results of each exercise shall be documented, reviewed, and used to improve recovery capabilities.

**10.15 Continuous Improvement**

Following each recovery exercise or actual disruption, the Service Provider shall conduct a formal review to identify lessons learned and opportunities for improvement.

The review shall consider:

- Achievement of RTO and RPO targets.
- Effectiveness of communication.
- Performance of recovery procedures.
- Technical issues encountered.
- Customer feedback.
- Recommendations for improvement.

Corrective actions shall be tracked to completion and monitored by management.

## Chapter 11 – Service Reporting, Performance Measurement, and Continual Improvement

### 11.1 Introduction

The Service Provider is committed to maintaining transparency, accountability, and continuous improvement in the delivery of electronic invoicing services. To achieve this, the Service Provider shall establish formal processes for measuring service performance, monitoring compliance with agreed Service Level Targets, reporting operational metrics, reviewing service quality, and implementing improvement initiatives.

Performance reporting provides customers with visibility into service delivery while enabling the Service Provider to identify trends, manage risks, and continually enhance operational effectiveness.

### 11.2 Objectives

The objectives of Service Reporting and Performance Management are to:

- Measure compliance with agreed Service Levels.
- Monitor operational performance of the ERP platform.
- Provide customers with accurate and timely performance reports.
- Identify opportunities for service improvement.
- Support regulatory and contractual compliance.
- Promote transparency and accountability.
- Improve customer satisfaction.
- Enable evidence-based management decisions.

### 11.3 Performance Monitoring Framework

The Service Provider shall continuously monitor the performance of all critical ERP services using automated monitoring systems and operational dashboards.

Monitoring shall include:

- Service availability.

- System uptime.
- Application performance.
- API response times.
- Database performance.
- Network latency.
- Invoice processing times.
- Authentication performance.
- Backup status.
- Security events.
- Capacity utilization.
- Support ticket trends.
- Error rates.

Monitoring shall operate twenty-four (24) hours per day, seven (7) days per week.

**11.4 Key Performance Indicators (KPIs)**

The Service Provider shall measure and report on the following Key Performance Indicators (KPIs):

| KPI | Target |
|---|---|
| Monthly Service Availability | ≥ 99.90% |
| Authentication Service Availability | ≥ 99.95% |
| API Availability | ≥ 99.90% |
| Invoice Submission Success Rate | ≥ 99.00% |
| Average Login Response Time | ≤ 3 Seconds |
| Average Invoice Validation Time | ≤ 5 Seconds |
| Average Invoice Submission Time | ≤ 15 Seconds |

| KPI | Target |
|---|---|
| Critical Incident Response Time | ≤ 15 Minutes |
| High Priority Incident Resolution | ≤ 8 Hours |
| Customer Satisfaction Score | ≥ 90% |
| Backup Success Rate | 100% |
| Security Patch Compliance | 100% within approved timelines |

Performance against these KPIs shall be reviewed monthly and corrective actions initiated where targets are not achieved.

**11.5 Service Reports**

The Service Provider shall prepare periodic reports detailing service performance and operational metrics.

**Monthly Service Performance Report**

The Monthly Service Performance Report shall include:

- Overall service availability.
- SLA compliance summary.
- Incident statistics.
- Problem management summary.
- Change management activities.
- Planned maintenance completed.
- Emergency maintenance activities.
- Security incidents.
- Capacity utilization.
- Customer support statistics.
- Service improvement initiatives.
- Risks and recommendations.

**Quarterly Management Report**

The Quarterly Management Report shall include:

- KPI trend analysis.
- Capacity planning outcomes.
- Customer satisfaction analysis.
- Major incident reviews.
- Root cause analysis summaries.
- Security posture review.
- Compliance status.
- Strategic improvement initiatives.

**Annual Service Review**

The Annual Service Review shall include:

- Overall SLA performance.
- Annual availability statistics.
- Business continuity testing results.
- Disaster recovery testing outcomes.
- Audit findings.
- Regulatory compliance status.
- Major achievements.
- Planned improvements for the following year.

### 11.6 Service Review Meetings

The Service Provider shall conduct formal Service Review Meetings with designated customer representatives to evaluate service performance and discuss improvement opportunities.

**Meeting Frequency**

| Meeting Type | Frequency |
|---|---|
| Operational Review | Monthly |
| Service Review | Quarterly |
| Executive Review | Annually |

Meeting agendas may include:

- Review of SLA performance.
- KPI achievements.
- Incident trends.
- Problem management updates.
- Planned changes.
- Security updates.
- Customer feedback.
- Capacity planning.
- Regulatory developments.
- Continuous improvement initiatives.

Minutes of each meeting shall be recorded and retained.

### 11.7 Customer Satisfaction Management

Customer satisfaction shall be measured using multiple feedback mechanisms, including:

- Ticket closure surveys.
- Periodic customer satisfaction surveys.
- Net Promoter Score (NPS).
- Service review meetings.
- Customer complaints.

- Compliments and testimonials.

Survey results shall be analysed to identify trends and opportunities for improving service quality.

**11.8 Non-Conformance Management**

Where service performance fails to meet agreed SLA targets, the Service Provider shall initiate a Non-Conformance Management process.

The process shall include:

1. Identification of the non-conformance.
2. Assessment of business impact.
3. Root cause analysis.
4. Development of corrective actions.
5. Assignment of responsibilities.
6. Monitoring of implementation.
7. Verification of effectiveness.
8. Closure upon successful completion.

Records of non-conformances shall be retained for audit purposes.

**11.9 Corrective and Preventive Actions (CAPA)**

The Service Provider shall maintain a formal Corrective and Preventive Action (CAPA) programme.

Corrective Actions shall address identified issues after they occur.

Preventive Actions shall reduce the likelihood of recurrence through:

- Process improvements.
- Technology upgrades.
- Additional monitoring.
- Staff training.

- Documentation updates.
- Risk mitigation measures.

CAPA activities shall be tracked to completion and reviewed by management.

**11.10 Internal Audits**

The Service Provider shall conduct periodic internal audits to verify compliance with:

- Service Level Agreement requirements.
- Operational procedures.
- Information security controls.
- Data protection obligations.
- Business continuity arrangements.
- Regulatory requirements.

Audit findings shall be documented, and corrective actions assigned with defined completion dates.

**11.11 Benchmarking**

The Service Provider shall periodically benchmark its service performance against:

- Industry best practices.
- Customer expectations.
- Regulatory requirements.
- Internal performance targets.
- Comparable service providers.

Benchmarking results shall inform strategic planning and service enhancement initiatives.

### 11.12 Continual Service Improvement (CSI)

The Service Provider shall operate a Continual Service Improvement (CSI) programme to enhance service quality, operational efficiency, and customer satisfaction.

Improvement opportunities may arise from:

- Incident analysis.
- Problem management.
- Customer feedback.
- Audit findings.
- Security assessments.
- Technology advancements.
- Regulatory changes.
- Performance reporting.

Each improvement initiative shall include:

- Description of the opportunity.
- Expected benefits.
- Implementation plan.
- Responsible owner.
- Target completion date.
- Success criteria.

Progress shall be monitored and reported to senior management.

### 11.13 Management Review

Senior Management shall conduct formal reviews of the SLA and associated service performance at least annually.

The Management Review shall consider:

- Achievement of SLA objectives.
- KPI performance.

- Customer satisfaction.
- Audit outcomes.
- Security incidents.
- Business continuity exercises.
- Regulatory changes.
- Resource requirements.
- Strategic risks.
- Recommendations for improvement.

Actions arising from the review shall be documented and tracked to completion.

**11.14 Document Review and Revision**

This SLA shall be reviewed:

- Annually.
- Following significant service changes.
- Following major incidents.
- Following regulatory changes.
- Following audit recommendations.
- Upon mutual agreement between the Service Provider and customers.

Revisions shall be documented in the Document Revision History and communicated to affected stakeholders.

## Chapter 12 – Legal Terms, General Provisions, and Appendices

### 12.1 Introduction

This Service Level Agreement (SLA) establishes the operational and service commitments between the Service Provider and its customers for the provision of ERP-based electronic invoicing services. This chapter sets out the legal provisions governing the relationship between the parties, together with the supporting appendices that form an integral part of this Agreement.

Unless otherwise agreed in writing, this SLA shall apply to all production services delivered by the Service Provider through the ERP platform.

### 12.2 Confidentiality

Both parties acknowledge that, during the course of providing and receiving services under this Agreement, confidential information may be disclosed or made available.

Each party agrees to:

- Treat confidential information with the highest degree of care.
- Use confidential information solely for the purposes of performing obligations under this Agreement.
- Prevent unauthorized disclosure of confidential information.
- Restrict access to personnel who require the information for legitimate business purposes.
- Ensure that employees and contractors are subject to appropriate confidentiality obligations.

Confidential information includes, but is not limited to:

- Taxpayer information.
- Financial records.
- Electronic invoices.
- Technical documentation.
- Source code.
- System configurations.

- Security procedures.
- Authentication credentials.
- Business strategies.
- Commercial information.

The obligation of confidentiality shall survive the termination or expiration of this Agreement.

**12.3 Intellectual Property Rights**

All intellectual property rights relating to the ERP platform, software, documentation, processes, methodologies, trademarks, logos, and supporting materials shall remain the exclusive property of the Service Provider or its licensors.

Nothing contained in this SLA shall transfer ownership of intellectual property to the customer.

Customers retain ownership of:

- Business data.
- Financial information.
- Customer records.
- Electronic invoices.
- Taxpayer information.
- Uploaded documents.

The Service Provider shall process customer data solely for the purposes of delivering the contracted services.

**12.4 Compliance with Laws**

The Service Provider shall comply with all applicable laws, regulations, and industry requirements relevant to the delivery of electronic invoicing services, including but not limited to:

- Nigeria Data Protection Act (NDPA), 2023.

- Regulations issued by the Nigeria Data Protection Commission (NDPC).
- Federal Inland Revenue Service (FIRS) Electronic Invoicing Framework.
- Applicable tax legislation.
- Anti-money laundering regulations where applicable.
- Cybersecurity and electronic transaction legislation.
- Other relevant statutory obligations.

Customers shall also comply with applicable laws relating to the use of the ERP platform.

**12.5 Limitation of Liability**

The Service Provider shall use reasonable skill, care, and diligence in providing the services.

Except where prohibited by applicable law, the Service Provider shall not be liable for:

- Indirect or consequential losses.
- Loss of profits.
- Loss of goodwill.
- Loss of business opportunities.
- Loss resulting from customer misuse of the ERP platform.
- Interruptions caused by third-party service providers beyond the Service Provider's reasonable control.
- Force majeure events.

Nothing in this Agreement shall exclude liability for fraud, gross negligence, willful misconduct, or any liability that cannot be excluded by law.

**12.6 Force Majeure**

Neither party shall be liable for failure or delay in performing its obligations where such failure results from events beyond its reasonable control.

Force majeure events include:

- Natural disasters.
- Floods.
- Earthquakes.
- Fire.
- Epidemics or pandemics.
- War.
- Terrorist attacks.
- Civil unrest.
- Government restrictions.
- Nationwide internet failures.
- Utility failures.
- Labour disputes affecting critical infrastructure.

The affected party shall notify the other party promptly and take reasonable steps to minimize the impact of the event.

**12.7 Suspension of Services**

The Service Provider reserves the right to suspend services where:

- The customer breaches this Agreement.
- Continued service presents a security risk.
- Fraudulent or unlawful activity is detected.
- Regulatory authorities require suspension.
- Planned maintenance is necessary.
- Emergency maintenance is required to preserve service integrity.

Where practicable, reasonable notice shall be provided before suspension.

**12.8 Termination**

Either party may terminate the Agreement in accordance with the terms of the underlying service contract.

Grounds for termination may include:

- Material breach of contractual obligations.
- Persistent failure to meet agreed obligations.
- Insolvency.
- Fraudulent activities.
- Mutual written agreement.
- Regulatory directives.

Upon termination:

- Customer data shall be returned or made available for export, where applicable.
- Data retention and deletion shall be carried out in accordance with applicable laws and contractual obligations.
- Access credentials shall be revoked.
- Confidential information shall continue to be protected.

**12.9 Dispute Resolution**

The parties shall endeavour to resolve any dispute arising under this Agreement through good faith negotiations.

Where a dispute cannot be resolved through negotiation, the following escalation process shall apply:

1. Operational Representatives.
2. Service Delivery Manager.
3. Executive Management.
4. Mediation.
5. Arbitration or litigation before a court of competent jurisdiction, where necessary.

Nothing in this section prevents either party from seeking urgent injunctive or equitable relief where appropriate.

### 12.10 Governing Law and Jurisdiction

This Service Level Agreement shall be governed by and construed in accordance with the laws of the **Federal Republic of Nigeria**.

The courts of competent jurisdiction within Nigeria shall have jurisdiction over disputes arising from this Agreement, unless the parties mutually agree to an alternative dispute resolution mechanism.

### 12.11 Amendment of the SLA

This SLA may be amended where:

- There are significant changes to the ERP services.
- Regulatory or legal requirements change.
- New FIRS e-Invoicing requirements are introduced.
- Both parties agree in writing to revise the Agreement.

All amendments shall be documented in the Document Revision History and communicated to affected stakeholders before taking effect.

### 12.12 Entire Agreement

This SLA shall be read together with:

- Master Service Agreement (MSA), where applicable.
- Subscription Agreement.
- Privacy Policy.
- Data Processing Agreement (where applicable).
- Information Security Policy.
- Business Continuity Plan.

- Disaster Recovery Plan.
- Acceptable Use Policy.

Where there is any inconsistency, the Master Service Agreement shall prevail unless otherwise agreed in writing.

**12.13 Notices**

All formal notices under this Agreement shall be made in writing and delivered through approved communication channels, including:

- Official email addresses.
- Registered courier services.
- Customer portal notifications.
- Other methods agreed upon by the parties.

Notices shall be deemed received on the date of confirmed delivery or acknowledgment.

**12.14 Severability**

If any provision of this Agreement is determined by a court or competent authority to be invalid, illegal, or unenforceable, the remaining provisions shall remain in full force and effect.

The parties shall replace any invalid provision with one that most closely reflects the original intent while remaining legally enforceable.

**12.15 Waiver**

Failure by either party to enforce any provision of this Agreement shall not constitute a waiver of that provision or any other rights under the Agreement.

## Appendix A – Glossary of Terms

| Term | Definition |
|---|---|
| API | Application Programming Interface |
| ERP | Enterprise Resource Planning |
| FIRS | Federal Inland Revenue Service |
| MBS | Merchant Buyer Solution |
| NDPA | Nigeria Data Protection Act |
| NDPC | Nigeria Data Protection Commission |
| SLA | Service Level Agreement |
| RPO | Recovery Point Objective |
| RTO | Recovery Time Objective |
| KPI | Key Performance Indicator |
| MFA | Multi-Factor Authentication |
| CAB | Change Advisory Board |
| RCA | Root Cause Analysis |
| CAPA | Corrective and Preventive Action |
| UAT | User Acceptance Testing |

## Appendix B – Acronyms

| Acronym | Meaning |
|---|---|
| AES | Advanced Encryption Standard |
| API | Application Programming Interface |
| BCP | Business Continuity Plan |

| Acronym | Meaning |
|---|---|
| BCM | Business Continuity Management |
| CAB | Change Advisory Board |
| DR | Disaster Recovery |
| ERP | Enterprise Resource Planning |
| IDS/IPS | Intrusion Detection/Prevention System |
| ISMS | Information Security Management System |
| KPI | Key Performance Indicator |
| MFA | Multi-Factor Authentication |
| NDPA | Nigeria Data Protection Act |
| NDPC | Nigeria Data Protection Commission |
| RPO | Recovery Point Objective |
| RTO | Recovery Time Objective |
| SLA | Service Level Agreement |
| TLS | Transport Layer Security |
| VPN | Virtual Private Network |
| WAF | Web Application Firewall |

## Appendix C – Incident Priority Matrix

| Priority | Business Impact | Initial Response | Target Resolution |
|---|---|---|---|
| Critical | Complete service outage | 15 Minutes | 4 Hours |
| High | Major service degradation | 30 Minutes | 8 Hours |
| Medium | Partial functionality affected | 2 Hours | 24 Hours |

| Priority | Business Impact | Initial Response | Target Resolution |
|---|---|---|---|
| Low | Minor issue or enquiry | 4 Business Hours | 48 Hours |

**Appendix D – Contact and Escalation Directory**

| Role | Contact Details |
|---|---|
| Managing Director | 09030690129 |
| Service Delivery Manager | 08119560801 |
| Technical Support Manager | 08119560801 |
| Data Protection Officer | 08164984004 |
| Compliance Officer | 09058331110 |
| Emergency Support Line | 08164984004 |
| Support Email | Cornelius.adeoye@thamesng.com |
| Customer Portal | www.thamesintl.com |

**Appendix E – Service Review Calendar**

| Activity | Frequency |
|---|---|
| SLA Performance Review | Monthly |
| Customer Service Review | Quarterly |
| Information Security Review | Quarterly |
| Business Continuity Test | Annually |
| Disaster Recovery Test | Annually |
| Internal Audit | Annually |

| Activity | Frequency |
|---|---|
| Management Review | Annually |
| SLA Review | Annually or as required |

**Document Approval**

| Role | Name | Signature | Date |
|---|---|---|---|
| Prepared By | Adeoye Adewale | Adeoye Adewale | 13/04/2026 |
| Reviewed By | Micheal Ipadeola | Micheal Ipadeola | 28/04/2026 |
| Approved By | Corneliu Adeoye | Corneliu Adeoye | 04/05/2026 |