GOVERNMENT OF THE PEOPLE'S REPUBLIC OF BANGLADESH

Ministry of Environment, Forest and Climate Change

Department of Environment (DOE)

TERMS OF REFERENCE

FOR

Development of Monitoring & Enforcement Automation System (MEAS)

Ministry / Division:	Ministry of Environment, Forest and Climate Change
Department / Organization:	Department of Environment (DOE)
ICT Division Reference:	[If Needed]
BASIS Reference:	[If Needed]
Project Classification:	Software Development & System Integration
Budget Category:	Development Project (CCTF)
Procurement Method:	As per PPA 2006 & PPR 2025

TABLE OF CONTENTS

SECTION A: PROJECT OVERVIEW

A.1 Background

The Department of Environment (DOE) under the Ministry of Environment, Forest and Climate Change is mandated to monitor and enforce environmental regulations across Bangladesh. Currently, DOE's enforcement activities are managed through manual, paper-based processes, creating inefficiencies in case management, notice issuance, penalty calculation, and compliance monitoring.

A.2 Project Title

Development of Monitoring & Enforcement Automation System (MEAS)

A.3 Implementing Agency

Primary Agency:	Department of Environment (DOE)
Technical Oversight:	[If Needed] ICT Division, Ministry of Posts, Telecommunications and Information Technology
Industry Association:	BASIS (Bangladesh Association of Software and Information Services)

A.4 Project Duration

Total Duration:	08 (Eight) months from contract signing
Implementation Period:	As per approved timeline
Warranty Period:	12 months from go-live date

Figure 1: MEAS Case Lifecycle — End-to-End Enforcement Workflow

SECTION B: PROJECT OBJECTIVES AND SCOPE

B.1 Development Objective

To develop a comprehensive web-based Monitoring & Enforcement Automation System (MEAS) that will digitize and automate the enforcement activities of the Department of Environment, ensuring transparency, efficiency, and improved environmental compliance monitoring.

B.2 Immediate Objectives

1. Process Automation: Automate enforcement notice generation and case lifecycle management
2. Digital Archive Creation: Digitize approx. 20,000+ existing enforcement files and documents in DoE's Dhaka, Sylhet & Chittagong Office.
3. System Integration: Establish seamless integration with existing DOE systems
4. Performance Enhancement: Provide real-time monitoring and analytics capabilities
5. Communication Improvement: Implement automated notification systems
6. Compliance Monitoring: Enable efficient penalty calculation and recovery tracking

B.3 Scope of Work

B.3.1 Software Development Components

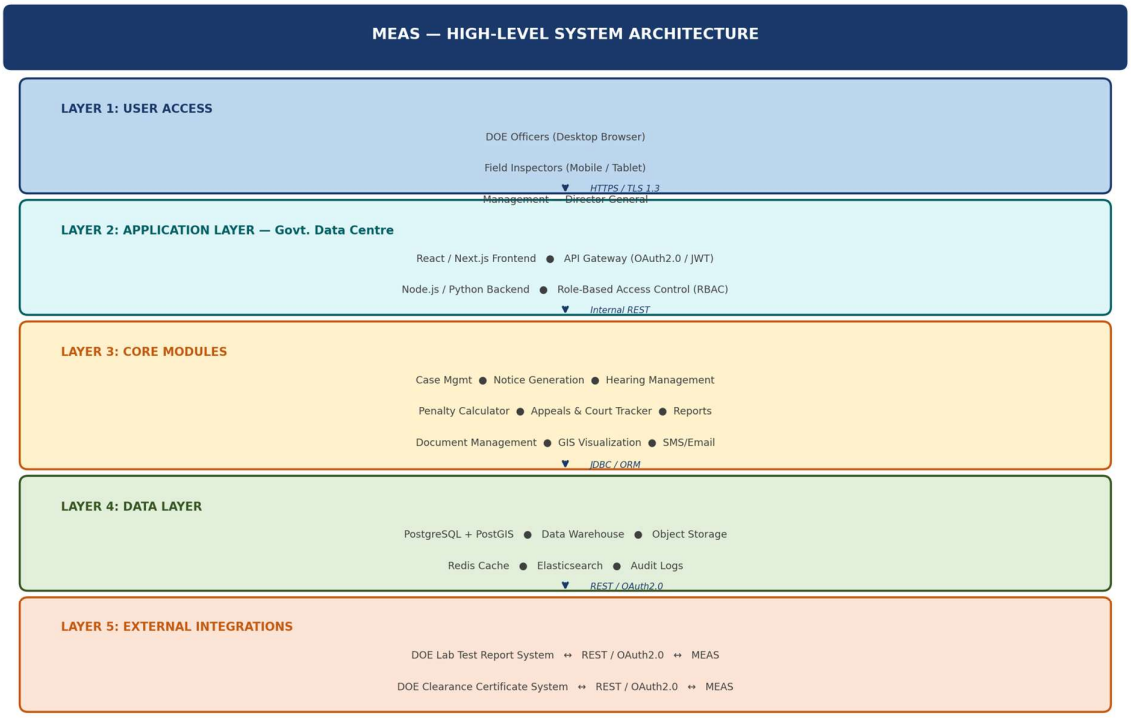
Core Modules:

- Case & Notice Management System
- Hearing Scheduling & Management
- Penalty & Compensation Calculator
- Appeals & Court Case Tracker
- Reporting & Analytics Dashboard
- SMS/Email Notification System
- Document Management System
- GIS-based Compliance Visualization
- Integration with ECC and Elab
- Hosting at BCC

Technical Architecture:

- Frontend: React/Next.js/JS framework (latest stable version)
- Backend: Node.js (NestJS) or Python (Django/DRF) or PHP framework
- Database: PostgreSQL with PostGIS extension/MySQL
- Integration Layer: RESTful APIs with OAuth2.0
- Mobile Support: Responsive web application
- Offline Capability: Limited offline functionality for field operations

Figure 2: MEAS High-Level System Architecture



B.3.2 Data Migration & Digitization

Legacy Data Processing:

- Complete digitization of approx.20,000+ enforcement files in DoE's Dhaka, Sylhet & Chittagong Office.
- Data entry and validation services
- Document scanning and indexing
- Quality assurance and data cleansing
- Historical case reconstruction
- Searchable document archive creation

Migration Requirements:

- Data extraction from existing systems (if any)
- Data transformation and normalization
- Bulk data import utilities
- Data validation and integrity checks
- Migration testing and verification

B.3.3 System Integration Requirements

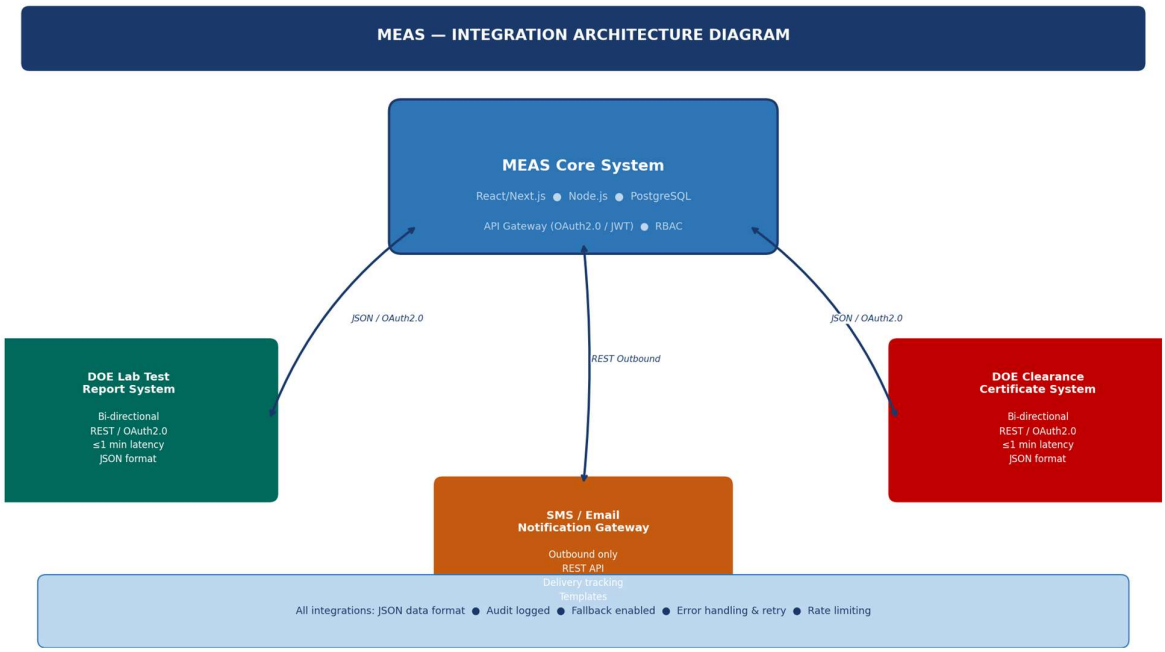
Mandatory Integrations:

- DOE Lab Test Report System (bi-directional)
- DOE Clearance Certificate System (bi-directional)

Integration Specifications:

- RESTful API architecture
- OAuth2.0 authentication with client credentials
- Real-time data synchronization (≤1 minute latency)
- Error handling and retry mechanisms
- Audit logging for all integration activities
- Fallback procedures for system unavailability

Figure 3: Integration Architecture Diagram



B.4 Excluded from Scope

- Hardware procurement (unless specifically mentioned)
- Existing system modifications beyond integration requirements
- Training beyond specified requirements
- Support beyond warranty period (unless contracted separately)

SECTION C: TECHNICAL REQUIREMENTS

C.1 Functional Requirements

C.1.1 Case Management Module

- Case registration and classification system
- Automatic notice generation (1st, 2nd, 3rd notices)
- Case status tracking and updates
- Document attachment and management
- Case assignment and reassignment
- Case closure procedures
- Case search and filtering capabilities

C.1.2 Notice Management System

- Automated notice generation based on case type
- Template management for different notice types
- Digital signature integration
- Notice delivery tracking
- Response deadline management
- Escalation procedures for non-compliance

C.1.3 Hearing Management

- Hearing scheduling and calendar management
- Stakeholder notification system
- Hearing outcome recording
- Digital order generation and distribution
- Evidence management during hearings
- Hearing rescheduling procedures

C.1.4 Penalty & Compensation Module

- Automated penalty calculation based on violation type (AI if needed)
- Penalty escalation for repeat offenders
- Compensation assessment tools
- Payment tracking and reconciliation
- Recovery status monitoring
- Payment reminder system

C.1.5 Appeals & Legal Case Tracking

- Appeal registration and processing
- Ministry-level appeal management
- Court case tracking and documentation
- Stay order management
- Legal timeline tracking
- Outcome recording and implementation

C.1.6 Reporting & Analytics

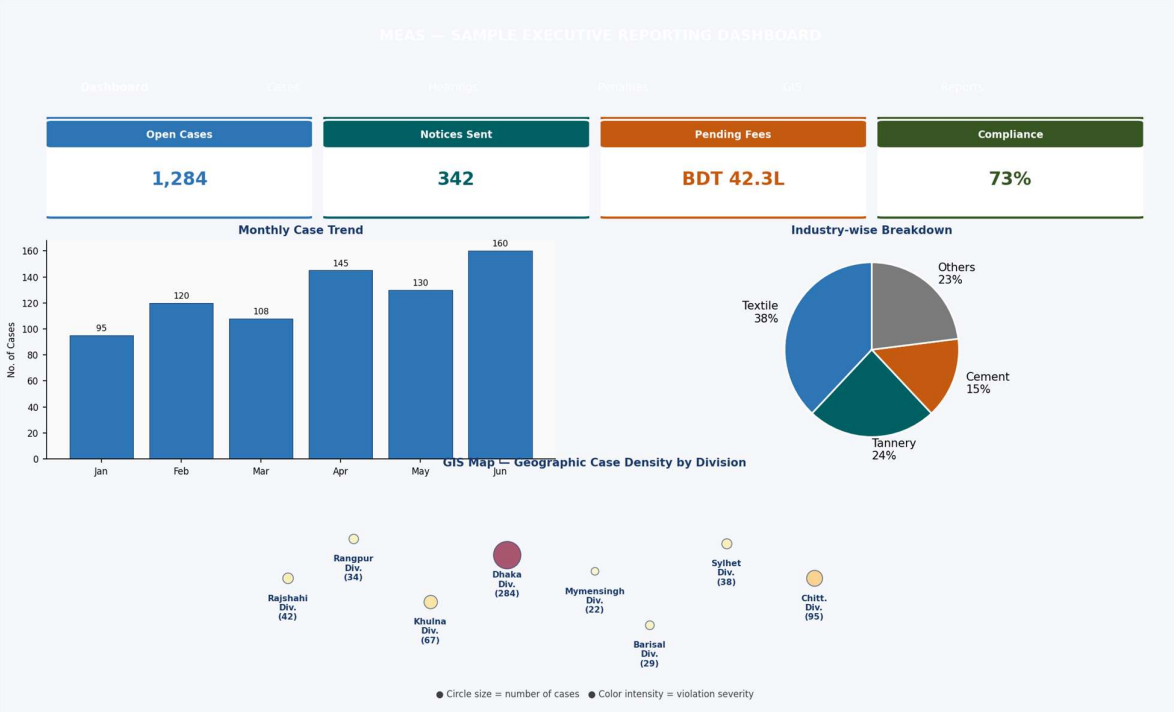
- Real-time dashboard with KPIs

- Executive summary reports
- Compliance rate analysis
- Industry-wise performance metrics
- Geographic distribution of cases
- Trend analysis and forecasting
- Export capabilities (PDF, Excel, CSV)

C.1.7 Communication System

- SMS gateway integration for notifications
- Email system for formal communications
- Template management for communications
- Delivery status tracking
- Escalation notifications
- Reminder systems for deadlines

Figure 4: Sample Executive Reporting Dashboard — Illustrative Layout



C.2 Non-Functional Requirements

C.2.1 Performance Requirements

Metric	Requirement
Concurrent Users	Support minimum 1,000 simultaneous users
Response Time	Maximum 3 seconds for standard operations
Transaction Processing	Handle 50 transactions per second
Database Capacity	Support 20,000+ industries and 50,000+ cases
File Storage	Unlimited document storage capability
Integration Load	Process 50 integration events per second

C.2.2 Security Requirements

Security Control	Specification
Authentication	Multi-factor authentication (MFA) — mandatory
Authorization	Role-based access control (RBAC)
Data Encryption	AES-256 encryption for data at rest and in transit
Network Security	TLS 1.3 for all communications
Audit Logging	Comprehensive audit trails for all activities
Session Management	Secure session handling with timeout
API Security	OAuth2.0 with JWT tokens
Vulnerability Assessment	Regular security testing required

C.2.3 Availability & Reliability

Parameter	Requirement
System Uptime	99.5% availability SLA
Backup & Recovery	Daily automated backups with 4-hour recovery time
Disaster Recovery	Complete DR plan with maximum 24-hour RTO
Load Balancing	Implement load balancing for high availability
Monitoring	24/7 system monitoring and alerting
Maintenance Windows	Scheduled maintenance with minimal downtime

C.2.4 Scalability Requirements

- Horizontal Scaling: Architecture must support horizontal scaling
- Database Scaling: Database clustering and replication support
- Storage Scaling: Expandable storage architecture
- User Growth: Support for 10x user growth without major changes
- Data Growth: Handle exponential data growth over 10 years

C.2.5 Usability Requirements

- Multi-language Support: English and Bangla interface
- Accessibility: WCAG 2.1 AA compliance
- Browser Compatibility: Support for Chrome, Firefox, Safari, Edge (latest versions)
- Mobile Responsiveness: Full functionality on tablets and mobile devices
- User Experience: Intuitive interface with minimal training requirements

C.3 Technical Architecture

C.3.1 System Architecture

- Architecture Pattern: Microservices architecture preferred
- API Gateway: Centralized API gateway for service orchestration
- Service Mesh: Consider service mesh for microservices communication
- Caching: Redis/Memcached for performance optimization
- Message Queue: RabbitMQ/Apache Kafka for asynchronous processing
- Search Engine: Elasticsearch for advanced search capabilities

C.3.2 Database Requirements

- Primary Database: PostgreSQL (latest stable version)/MySQL
- Spatial Extension: PostGIS for geographic data handling/MySQL
- Data Warehouse: Separate analytics database for reporting
- Database Design: Normalized database design with proper indexing
- Backup Strategy: Point-in-time recovery capability
- Replication: Master-slave replication for read operations

C.3.3 Integration Architecture

- API Style: RESTful APIs with OpenAPI 3.0 specification
- Authentication: OAuth2.0 with client credentials flow
- Data Format: JSON for data exchange
- Error Handling: Standardized error responses
- Rate Limiting: API rate limiting to prevent abuse
- Versioning: API versioning strategy for backward compatibility

SECTION D: COMPLIANCE & STANDARDS

D.1 Government Compliance

- Public Procurement Act 2006 and Public Procurement Rules 2025
- ICT Policy 2018 of the Government of Bangladesh
- Digital Security Act 2018 compliance
- Cyber Security Act 2018 compliance
- Right to Information Act 2009 provisions
- Data Protection Act 2023 (if applicable)
- National ICT Standards as defined by ICT Division

D.2 Technical Standards

- ISO/IEC 27001:2022 — Information Security Management
- ISO 9001:2015 — Quality Management Systems
- CMMI Level 3 or equivalent software development process
- OWASP Top 10 security guidelines compliance
- Web Content Accessibility Guidelines (WCAG) 2.1 Level AA
- BASIS Guidelines for software development in Bangladesh

D.3 Development Standards

- Coding Standards: Industry best practices and clean code principles
- Documentation Standards: Complete technical and user documentation
- Testing Standards: Unit testing (80%+ coverage), integration, and system testing
- Version Control: Git-based version control with proper branching strategy
- Code Review: Mandatory peer code review process
- CI/CD Pipeline: Automated build, test, and deployment pipeline [If Needed]

SECTION E: DELIVERABLES AND TIMELINE

Figure 5: Project Implementation Timeline — 9-Month Schedule (Gantt)

SECTION H: INFRASTRUCTURE AND HOSTING

H.1 Hosting Provider Responsibility

H.1.1 Year 1 — Hosting by Selected Firm

Selected Firm, as the implementing partner, shall provide and fully manage the server infrastructure for the MEAS system during the first year (12 months) from the system go-live date. The following conditions apply:

7. **Selected Firm** shall provision, configure, and maintain the server at its own expense for the duration of Year 1.
8. **Selected Firm** shall select the hosting server — either an international Virtual Private Server (VPS) such as AWS, DigitalOcean, Vultr, or Linode, or a national VPS provider such as the Bangladesh Computer Council (BCC) Data Centre or another Government-approved cloud infrastructure — based on the system's technical performance requirements, uptime SLA, and data residency compliance.
9. If **Selected Firm** identifies an international or national VPS provider that is suitable for the MEAS system in terms of performance, reliability, and compliance, the Department of Environment (DOE) is obligated to use that selected server and hosting arrangement. DOE shall have no right to override or substitute this selection during Year 1.
10. All server provisioning, bandwidth, security infrastructure, SSL certificates, DDoS protection, and monitoring costs during Year 1 shall be borne entirely by SixDot Technologies Limited.
11. **Selected Firm** shall ensure a minimum 99.5% uptime SLA, daily automated backups with 30-day retention, 24/7 monitoring, and disaster recovery capability with a maximum 24-hour Recovery Time Objective (RTO) throughout Year 1.

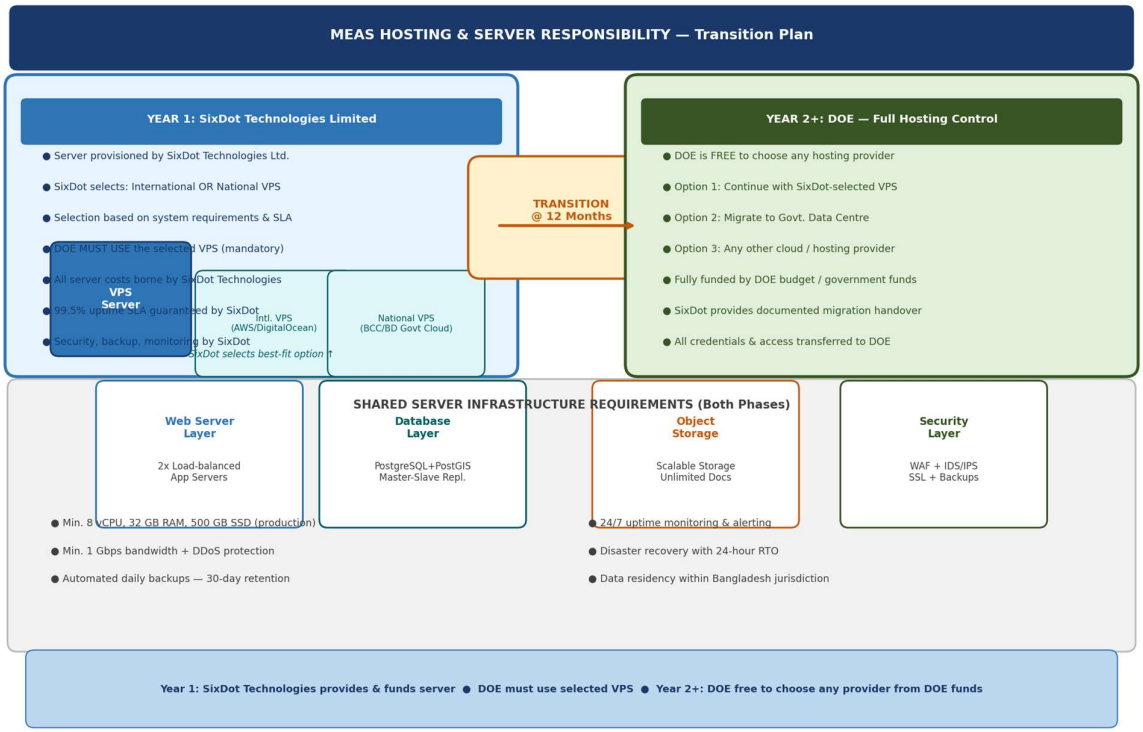
H.1.2 Year 2 Onwards — Hosting by DOE (Free Choice)

After the completion of the first 12 months of hosting by **Selected Firm**, the hosting responsibility shall transition fully to the Department of Environment (DOE) under the following terms:

12. DOE shall be entirely free to choose any hosting provider of its preference — including continuing with the server selected by **Selected Firm**, migrating to the Government Data Centre, or adopting any other national or international cloud provider.
13. All hosting costs from Year 2 onwards shall be financed exclusively from DOE's own government budget allocation or approved development project funds. **Selected Firm** shall bear no hosting expenses beyond the 12-month period.
14. Prior to transition, **Selected Firm** shall provide DOE with complete server access credentials, deployment documentation, configuration files, and a migration support guide to facilitate a seamless handover to the new hosting environment.
15. DOE shall notify **Selected Firm** at least 30 days before the end of Year 1 regarding the decision on hosting continuation or migration, to allow adequate time for transition planning.

H.1.3 Hosting Transition Diagram

Figure 8: MEAS Hosting Responsibility — Year 1 (Selected Firm) to Year 2+ (DOE) Transition



H.2 Hosting Requirements

H.2.1 Primary Hosting

16. Government Data Centre is the preferred long-term location for data residency compliance (from Year 2)
17. Year 1 Backup Option: Hybrid cloud setup with either government-approved national VPS or reputable international VPS as selected by Selected Firm All hosting must comply with government data residency requirements and Bangladesh data protection regulations

H.2.2 Infrastructure Specifications

The following minimum specifications apply to the server infrastructure in both Year 1 (provided by Selected Firm) and Year 2+ (procured by DOE):

18. Production Environment: Minimum 8 vCPU, 32 GB RAM, 500 GB SSD NVMe storage; load-balanced web servers with auto-scaling; master-slave database replication; minimum 1 Gbps bandwidth with DDoS protection
19. Staging Environment: 50% of production capacity; mirror of production for pre-production testing and UAT
20. Development Environment: 25% of production capacity; shared environment for development team

H.3 Technical Infrastructure

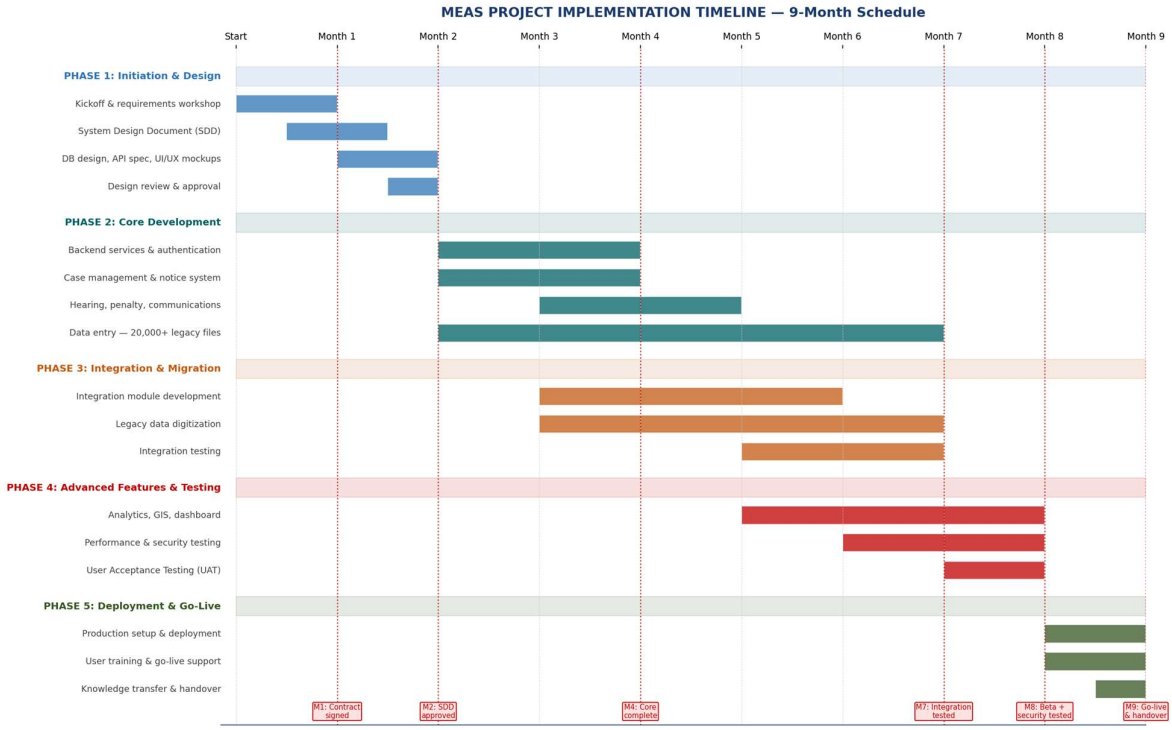
H.3.1 Network Requirements

21. Internet Connectivity: High-speed internet with redundancy (minimum 1 Gbps)
22. VPN Access: Secure VPN for remote development team access
23. Firewall: Enterprise-grade firewall configuration
24. Load Balancer: Application load balancer for traffic distribution
25. CDN: Content Delivery Network for static assets

H.3.2 Security Infrastructure

26. SSL Certificates: Valid SSL certificates for all domains (TLS 1.3)
27. Web Application Firewall (WAF): For application-layer protection
28. Intrusion Detection System (IDS/IPS): For active security monitoring

29. Backup Systems: Automated daily backups with 30-day retention and offsite storage
30. Monitoring Tools: 24/7 system monitoring, alerting, and incident response



E.1 Deliverable Schedule

Phase 1: Project Initiation & Design (Month 1–2)

Week 1–2:

- Project kickoff and team formation
- Requirement validation workshop with DOE stakeholders
- Technical environment setup and tool configuration

Week 3–4:

- System Design Document (SDD) development
- Database design and entity relationship diagrams
- API specifications and integration design
- UI/UX wireframes and design mockups
- Technical architecture documentation

Week 5–6:

- Design review and approval process
- Development environment setup
- Project plan finalization and approval

Phase 1 Deliverables:

- System Design Document (SDD)
- Database Design Document
- API Specification Document
- UI/UX Design Mockups

- Technical Architecture Document
- Project Implementation Plan

Phase 2: Core Development (Month 2–5)

Month 1.5–2:

- Core backend services development
- Database implementation with sample data
- Authentication and authorization module
- Basic frontend framework setup

Month 2–3:

- Case management module development
- Notice generation system implementation
- User management and role-based access control
- Basic reporting module
- Migrated Historical Data Manual Input (20,000+ files)

Month 3–4:

- Hearing management module
- Penalty calculation system
- Communication system (SMS/Email)
- Document management system
- Initial system testing
- Migrated Historical Data Manual Input (20,000+ files)

Phase 2 Deliverables:

- Core MEAS Application (Alpha Version)
- Module-wise Test Reports
- API Documentation
- Database Documentation
- Initial User Manual (Draft)

Phase 3: Integration & Data Migration (Month 4–6)

Month 4–4.5:

- Integration module development
- API development for external systems
- Authentication and security implementation for integrations
- Migrated Historical Data Manual Input (20,000+ files)

Month 4.5–5:

- Data migration tools development
- Legacy data digitization process initiation
- Data entry and validation procedures
- Quality assurance processes
- Migrated Historical Data Manual Input (20,000+ files)

Month 5–6:

- Complete data migration execution
- Integration testing with existing systems
- Data validation and quality checks
- Integration documentation
- Migrated Historical Data Manual Input (15,000+ files)

Phase 3 Deliverables:

- Integration Modules
- Data Migration Tools
- Migrated Historical Data Manual Input (15,000+ files)
- Integration Test Reports
- Data Quality Assessment Report
- Integration Documentation

Phase 4: Advanced Features & Testing (Month 6–7)

Month 6–6.5:

- Advanced reporting and analytics
- GIS integration and visualization
- Dashboard development and customization
- Mobile responsiveness implementation

Month 6.5–7:

- Performance optimization
- Security hardening and testing
- User acceptance testing preparation
- Load testing and stress testing
- Security penetration testing

Phase 4 Deliverables:

- Complete MEAS Application (Beta Version)
- Advanced Analytics Dashboard
- GIS-based Visualization Module
- Performance Test Reports
- Security Assessment Report
- User Acceptance Testing Plan

Phase 5: Deployment & Go-Live (Month 7–8)

Month 7:

- Production environment setup
- Application deployment and configuration
- User training program execution
- System documentation completion

Month 8:

- Go-live support and monitoring

- Issue resolution and bug fixes
- Performance monitoring and optimization
- Knowledge transfer sessions

Phase 5 Deliverables:

- Production-Ready MEAS System
- Complete Documentation Package
- Training Materials and Records
- Go-Live Support Report
- System Performance Report
- Knowledge Transfer Documentation

E.2 Documentation Requirements

E.2.1 Technical Documentation

- System Requirements Specification (SRS) — Updated version
- System Design Document (SDD) with detailed architecture
- Database Design Document with schema and relationships
- API Documentation with complete endpoint specifications
- Integration Guide for external systems
- Deployment Guide with infrastructure requirements
- Security Implementation Guide
- Performance Optimization Guide

E.2.2 User Documentation

- User Manual (English and Bangla versions)
- Administrator Manual for system configuration
- Training Materials for end users
- Quick Reference Guides for common operations
- Troubleshooting Guide for common issues
- FAQ Document based on user queries

E.2.3 Process Documentation

- Development Process Documentation
- Testing Strategy and Test Cases
- Data Migration Process Documentation
- Quality Assurance Procedures
- Change Management Process
- Issue Tracking and Resolution Process

SECTION F: QUALITY ASSURANCE AND TESTING

F.1 Testing Strategy

F.1.1 Testing Levels

Testing Level	Scope / Description
Unit Testing	Minimum 80% code coverage for all modules
Integration Testing	All system integrations and APIs
System Testing	End-to-end functional testing
Performance Testing	Load, stress, and volume testing
Security Testing	Vulnerability assessment and penetration testing
User Acceptance Testing	DOE stakeholder validation

F.1.2 Testing Environment

- Development Testing: Continuous testing during development
- Staging Environment: Production-like environment for final testing
- UAT Environment: Separate environment for user acceptance testing
- Performance Testing Environment: Dedicated environment for load testing

F.1.3 Test Deliverables

- Test Strategy Document
- Test Plan and Test Cases
- Test Execution Reports
- Defect Reports and Resolution Status
- Performance Test Results
- Security Assessment Report
- User Acceptance Test Sign-off

F.2 Quality Standards

- Code Quality: SonarQube or equivalent static code analysis
- Performance Standards: Response time and throughput benchmarks
- Security Standards: OWASP compliance and security best practices
- Documentation Quality: Complete and up-to-date documentation
- User Experience: Usability testing and feedback incorporation

SECTION G: PROJECT TEAM AND RESOURCES

G.1 Required Team Composition

Role	Qty	Category
Project Manager (PMP certified preferred)	1	Management
Technical Lead / Architect	1	Management
Quality Assurance Lead	1	Management
Business Analyst	1	Management
Senior Full-stack Developers	3	Development
Frontend Developers (React)	2	Development
Backend Developers (Node.js/Python)	2	Development
Database Administrator / Developer	1	Development
Integration Specialist	1	Development
Server Admin / DevOps Engineer	1	Development
GIS Specialist	1	Specialized
Security Specialist	1	Specialized
Data Migration Specialist	2	Specialized
UI/UX Designer	1	Specialized
Mobile Developer (if native app required)	1	Specialized
Quality Assurance Engineers	2	Support
Technical Writers	1	Support
Training Coordinator	1	Support
Data Entry Operators (for legacy data)	18–20	Support

G.2 Team Qualifications

G.2.1 Minimum Educational Requirements

- Project Manager: Bachelor's degree in Engineering/Computer Science, PMP certification preferred
- Technical Leads: Master's/Bachelor's degree in Computer Science or related field
- Developers: Bachelor's degree in Computer Science/Engineering with relevant experience
- Specialists: Relevant degree with specialized certifications in their domain

G.2.2 Experience Requirements

Role	Minimum Experience
Project Manager	Minimum 5 years of IT project management experience
Technical Lead	Minimum 5 years of software architecture experience
Senior Developers	Minimum 4 years of relevant technology experience
Junior Developers	Minimum 1–2 years of development experience
Specialists	Minimum 3–5 years in their respective specialization

G.2.3 Technology Expertise Required

- Frontend: React.js/Next.js, HTML5, CSS3, JavaScript/TypeScript, JS Framework
- Backend: Node.js/NestJS, Python/Django, RESTful API development, php
- Database: PostgreSQL, PostGIS, database optimization, MySQL
- Integration: OAuth2.0, JWT, API development and integration
- DevOps: Docker, Kubernetes, CI/CD pipelines, cloud platforms
- Testing: Automated testing frameworks, performance testing tools

SECTION H: INFRASTRUCTURE AND HOSTING

H.1 Hosting Requirements

H.1.1 Primary Hosting

- Government Data Center (Preferred location for data residency compliance)
- Backup Option: Hybrid cloud setup with government-approved cloud providers
- Compliance: All hosting must comply with government data residency requirements

H.1.2 Infrastructure Specifications

Environment	Configuration	Resources
Production	Load-balanced web servers with auto-scaling; min. 2 app servers; master-slave DB; scalable object storage; bandwidth for 1,000+ concurrent users	Full capacity
Staging	Mirror of production environment for pre-production testing and UAT	50% of production
Development	Shared development environment for the team	25% of production

H.2 Technical Infrastructure

H.2.1 Network Requirements

- Internet Connectivity: High-speed internet with redundancy
- VPN Access: Secure VPN for remote development team access
- Firewall: Enterprise-grade firewall configuration
- Load Balancer: Application load balancer for traffic distribution
- CDN: Content Delivery Network for static assets

H.2.2 Security Infrastructure

- SSL Certificates: Valid SSL certificates for all domains
- Web Application Firewall: WAF for application protection
- Intrusion Detection: IDS/IPS for security monitoring
- Backup Systems: Automated backup with offsite storage
- Monitoring Tools: 24/7 system monitoring and alerting

SECTION I: TRAINING AND KNOWLEDGE TRANSFER

I.1 Training Program

I.1.1 Training Categories

Training Programme	Target Audience	Duration
Basic System Navigation	End Users	8 hours
Case Management Operations	End Users	12 hours
Advanced Features and Reporting	End Users	8 hours
Troubleshooting and FAQs	End Users	4 hours
Total — End User Training		32 hours per participant
System Configuration and Setup	Administrators	16 hours
User Management and Security	Administrators	8 hours
Integration Management	Administrators	8 hours
Backup and Recovery Procedures	Administrators	8 hours
Performance Monitoring	Administrators	4 hours
Total — Administrator Training		44 hours per participant
System Architecture Overview	Technical Staff	8 hours
Database Management	Technical Staff	12 hours
API and Integration Management	Technical Staff	8 hours
Security Configuration	Technical Staff	8 hours
Troubleshooting and Maintenance	Technical Staff	8 hours
Total — Technical Training		44 hours per participant

I.1.2 Training Methodology

- Classroom Training: Face-to-face training sessions
- Hands-on Practice: Practical exercises on the system
- Documentation: Comprehensive training materials
- Follow-up Sessions: Refresher training after go-live

I.1.3 Training Deliverables

- Training Plan and Schedule
- Training Materials (English and Bangla)
- Quick Reference Guides
- Training Completion Certificates
- Training Effectiveness Assessment

I.2 Knowledge Transfer

I.2.1 Technical Knowledge Transfer

- Source Code Handover with documentation
- Development Environment Setup guide
- Database Schema and Documentation
- API Documentation and Testing Tools
- Deployment Procedures and scripts
- Troubleshooting Guide for common issues

I.2.2 Operational Knowledge Transfer

- System Administration Procedures
- User Management Processes
- Backup and Recovery Procedures
- Performance Monitoring Guidelines
- Security Management Protocols
- Integration Monitoring and Maintenance

SECTION J: SUPPORT AND MAINTENANCE

J.1 Warranty and Support Period

J.1.1 Warranty Coverage

Parameter	Terms
Duration	12 months from system go-live date
Scope	All developed software components and functionalities
Coverage	Bug fixes, performance issues, and minor enhancements
Response Time (Critical)	4 hours
Response Time (Standard)	24 hours
Resolution Time (Critical)	24 hours
Resolution Time (Standard)	72 hours

J.1.2 Support Levels

Support Level	Period	Availability	Coverage
Level 1	First 3 months post go-live	24/7 support hotline; on-site within 4 hours	All system issues and user queries; immediate critical response
Level 2	Months 4–12 post go-live	Business hours 9AM–6PM; 4-hr response for critical	System issues and major user queries; remote primary mode

J.1.3 Maintenance Services

Included in Warranty:

- Bug Fixes: All software defects and errors
- Performance Optimization: System performance improvements
- Security Updates: Security patches and updates
- Minor Enhancements: Small feature additions as agreed
- Data Backup Monitoring: Ensuring backup procedures work correctly
- System Health Monitoring: Regular system performance checks

Excluded from Warranty:

- Hardware Issues: Hardware failures or upgrades
- Third-party Software: Issues with third-party components
- Major Enhancements: Significant new features or modules
- Training: Additional training beyond specified requirements
- Data Recovery: Recovery due to user error or misuse

J.2 Post-Warranty Support

J.2.1 Annual Maintenance Contract (Optional)

- Duration: 12 months renewable
- Coverage: Ongoing support and maintenance services
- Cost: 15–20% of total project cost annually
- Services: Regular updates, minor enhancements, and support

J.2.2 Extended Support Services

- Feature Enhancements: New feature development as required
- System Upgrades: Technology stack upgrades and modernization
- Performance Optimization: Ongoing performance improvements
- Additional Training: Refresher training for new users
- Consultation Services: Advisory services for system expansion

SECTION K: FINANCIAL TERMS AND CONDITIONS

K.1 Budget and Cost Structure

K.1.1 Project Components Costing

System Analysis, Design, System Development				
Position	**Persons**	**Man Day**	**Duration (Months)**	**Total Cost (BDT)**
Project Manager	1	30		
System Analyst	1	30		
Software Architect	1	30		
Database Designer	1	30		
Technical Document Writer	1	30		
Front Developer	1	30		
Senior Software Developer	2	30		
Security Expert	1	30		
QA Expert	1	30		
GRAND TOTAL				

K.1.2 Payment Schedule (Milestone-Based)

Milestone	Amount (BDT)
System Requirement Study	
System Analysis, Design, System Development	
Integration with ECC and Elab	
Data Entry	
SMS/Email & Notifications	
Hosting at BCC	
TOTAL	

K.1.3 Cost Inclusions

- All software development activities
- Complete data migration services
- Integration with existing systems
- Comprehensive testing and quality assurance
- Training for DOE personnel
- Documentation in English and Bangla
- 12-month warranty support
- Knowledge transfer sessions

K.1.4 Cost Exclusions

- Hardware procurement and setup
- Internet connectivity and bandwidth costs
- Government Data Center hosting charges
- Third-party software licensing (if any)
- Extended support beyond warranty period
- Major scope changes during implementation
- SMS Gateway and Email Gateway

SECTION L: RISK MANAGEMENT

L.1 Technical Risks

L.1.1 Integration Risks

Risk	Probability	Impact	Mitigation
Existing systems may not have proper APIs for integration	Medium	High	Early assessment of existing systems; fallback file-based exchange; alternative integration approaches; close DOE coordination
Data inconsistency between integrated systems	Medium	Medium	Data validation and reconciliation procedures; regular synchronization checks; conflict resolution mechanisms; manual intervention procedures

L.1.2 Performance Risks

Risk	Probability	Impact	Mitigation
System may not meet performance requirements under load	Low	High	Performance testing throughout development; scalable architecture; load testing with realistic data; performance monitoring
Database performance degradation with large datasets	Medium	Medium	Proper database design and indexing; performance tuning; archiving strategies; regular maintenance

L.2 Project Risks

L.2.1 Schedule Risks

Risk	Probability	Impact	Mitigation
Data migration taking longer than expected	High	Medium	Detailed data assessment upfront; parallel processing; additional resources if needed; phased migration
Integration delays due to external system dependencies	Medium	Medium	Early engagement with system owners; parallel development; mock services; clear dependency management

L.2.2 Resource Risks

Risk	Probability	Impact	Mitigation
Key team members leaving during project	Low	High	Knowledge sharing and documentation; cross-training; backup resources; retention strategies
Skill gaps in specific technologies	Low	Medium	Team skill assessment and training; external expert consultation; technology partner engagement; alternative options

L.3 Operational Risks

L.3.1 Data Migration Risks

Risk	Probability	Impact	Mitigation
Data loss or corruption during migration	Low	Very High	Comprehensive backup procedures; phased migration with rollback; validation at each step; multiple backup copies
Poor data quality in legacy systems	High	Medium	Data quality assessment upfront; data cleansing procedures; quality control checkpoints; manual verification processes

L.3.2 User Adoption Risks

Risk	Probability	Impact	Mitigation
Resistance to change from users	Medium	Medium	Comprehensive training programs; user involvement in design; change management activities; ongoing support
Insufficient user training affecting system utilization	Medium	Medium	Comprehensive training plan; multiple training sessions; online help and documentation; post-implementation support

SECTION M: SUCCESS CRITERIA AND EVALUATION

M.1 Success Metrics

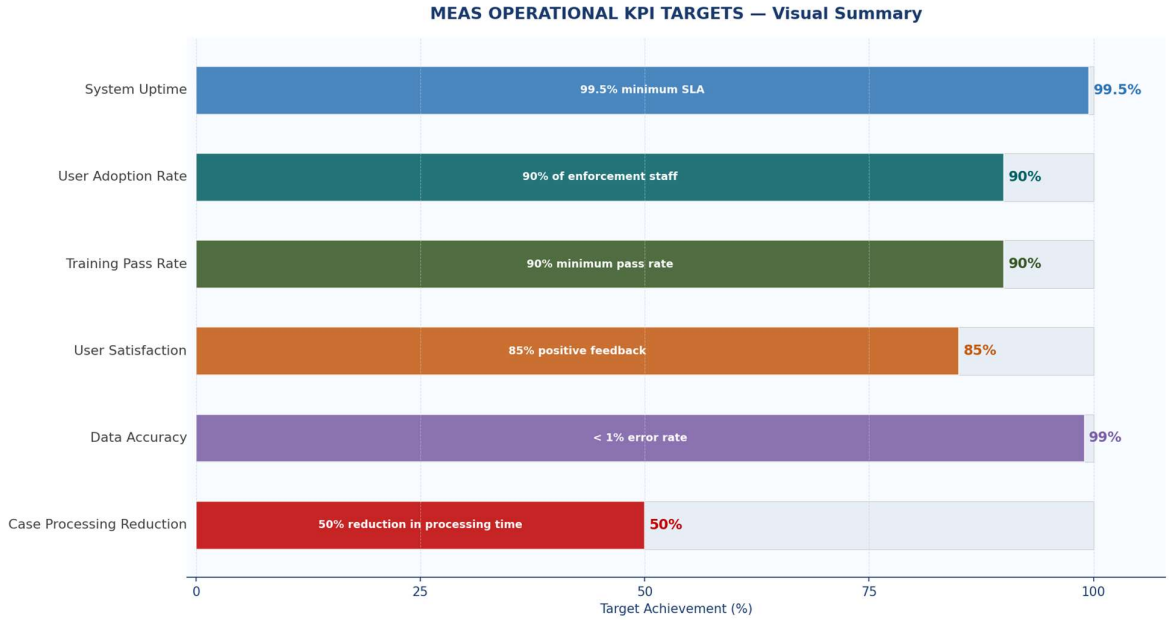
M.1.1 Functional Success Criteria

Criterion	Target
System Completeness	100% of specified functionalities delivered and working
Integration Success	All required integrations functional and stable
Data Migration	100% of legacy data successfully migrated and validated
User Acceptance	UAT sign-off from all DOE user groups
Performance	System meets all specified performance benchmarks
Security	Passes all security tests and compliance requirements

M.1.2 Operational Success Criteria

KPI	Target
System Uptime	Minimum 99.5% availability during first 6 months
User Adoption	Minimum 90% of DOE enforcement staff actively using the system
Process Efficiency	Minimum 50% reduction in case processing time
Data Accuracy	Less than 1% error rate in migrated data
User Satisfaction	Positive feedback from minimum 85% of users
Training Effectiveness	Minimum 90% pass rate in training assessments

Figure 6: Operational KPI Targets — Visual Summary



M.1.3 Technical Success Criteria

Criterion	Target
Code Quality	Minimum 80% test coverage and clean code standards compliance
Documentation	100% of technical and user documentation completed and approved
Security Compliance	Zero critical vulnerabilities in security assessment
Performance Benchmarks	All response time and throughput targets achieved
Integration Stability	Zero data loss or corruption in system integrations
Scalability	System handles 150% of specified load without degradation

M.2 Evaluation Methodology

M.2.1 Evaluation Framework

Phase-wise Evaluation:

- Design Phase: SDD review and approval by technical committee
- Development Phase: Code review and module testing completion
- Testing Phase: Comprehensive test execution and results validation
- Deployment Phase: Production deployment success and stability check
- Go-Live Phase: User acceptance and system performance validation

Continuous Monitoring:

- Weekly Progress Reviews: Against project timeline and milestones
- Monthly Quality Gates: Code quality, testing, and documentation checks
- Quarterly Stakeholder Reviews: Business value and user satisfaction assessment

M.2.2 Evaluation Criteria

Evaluation Category	Weight	Key Assessment Areas
Technical Evaluation	40%	Functionality completeness, performance, security, integration, code quality
Business Evaluation	35%	User requirements, process improvement, business value, user satisfaction, operational efficiency
Project Management Evaluation	25%	Timeline adherence, budget management, risk management, communication, documentation

M.3 Acceptance Criteria

M.3.1 Technical Acceptance

- Functional Testing: All test cases passed with zero critical defects
- Performance Testing: All performance benchmarks achieved
- Security Testing: Security assessment passed with acceptable risk level
- Integration Testing: All integration points working correctly
- User Interface: UI approved by users and meets accessibility standards
- Documentation: Complete technical documentation delivered and approved

M.3.2 Business Acceptance

- User Acceptance Testing: Formal UAT sign-off from all user groups
- Business Process: All business processes supported and improved
- Data Migration: Historical data available and searchable

- Training: Users trained and confident in system operation
- Support: Support procedures in place and working effectively

M.3.3 Final Project Acceptance

- Deliverable Completeness: All contracted deliverables provided
- Quality Standards: All quality criteria met and verified
- Operational Readiness: System ready for full operational use
- Knowledge Transfer: Complete knowledge transfer to DOE team
- Warranty Activation: Support and maintenance procedures activated

SECTION N: COMMUNICATION AND GOVERNANCE

N.1 Project Governance Structure

N.1.1 Project Implementation Committee

Responsibilities:

- Day-to-day project oversight and management
- Technical decision making and issue resolution
- Progress monitoring and reporting
- Resource allocation and coordination
- Quality assurance and compliance monitoring

Meeting Schedule: Monthly or as required for major decisions

N.1.2 Technical Working Group

Responsibilities:

- Technical requirement clarification
- System design review and validation
- Integration planning and coordination
- Technical issue resolution
- Testing coordination and validation

Meeting Schedule: Weekly during active development phases

N.2 Communication Plan

N.2.1 Communication Channels

Formal Communications:

- Project Reports: Weekly progress reports to Project Management Committee
- Executive Summary: Monthly reports to Project Steering Committee
- Milestone Reports: Detailed reports at each milestone completion
- Issue Escalation: Formal escalation process for project issues
- Change Requests: Structured change management process

Informal Communications:

- Daily Standups: Development team coordination meetings
- Technical Discussions: Ad-hoc technical consultations
- User Feedback: Regular feedback collection from end users
- Vendor Coordination: Regular coordination with third-party vendors

N.2.2 Document Management

Document Repository:

- Central project repository for all documents
- Version control for all project artifacts
- Access control based on stakeholder roles
- Regular backup and archive procedures

N.3 Reporting Requirements

N.3.1 Progress Reporting

Weekly Progress Reports (During Active Development):

- Tasks completed in the week
- Tasks planned for next week
- Issues and risks identified
- Resource utilization status
- Milestone progress tracking
- Budget expenditure status

Monthly Executive Reports:

- Overall project status and health
- Milestone achievements and upcoming milestones
- Budget status and financial tracking
- Risk assessment and mitigation status
- Quality metrics and achievements
- Stakeholder feedback and satisfaction

Quarterly Business Reviews:

- Business value realization assessment
- User adoption and satisfaction metrics
- Operational improvement achievements
- Return on investment analysis
- Strategic alignment assessment
- Future planning and roadmap updates

N.3.2 Milestone Reporting

- Deliverable completion status
- Quality assurance results
- User acceptance feedback
- Lessons learned and best practices
- Next phase readiness assessment
- Budget and timeline impact analysis

N.3.3 Issue and Risk Reporting

Weekly Risk Registers:

- New risks identified
- Risk mitigation progress
- Risk impact assessments
- Escalation requirements

Issue Tracking:

- Issue identification and categorization
- Resolution progress and timelines
- Impact assessment and mitigation
- Stakeholder communication

SECTION O: CONTRACT TERMS AND CONDITIONS

O.1 Contract Fundamentals

O.1.1 Contract Type

- Contract Type: Fixed Price Contract with milestone-based payments
- Duration: 8 months from contract signing date
- Extension: Possible extension only for reasons beyond contractor control
- Penalty Clause: Applicable for delays beyond agreed timeline
- Bonus Clause: Early delivery bonus as per government rules

O.1.2 Legal Framework

- Governing Law: Laws of Bangladesh
- Dispute Resolution: As per Public Procurement Act 2006
- Jurisdiction: Courts of Dhaka, Bangladesh
- Language: English and Bangla (where required)
- Currency: Bangladesh Taka (BDT)

O.1.3 Contract Variations

- Change Control Process: Formal change management procedure
- Approval Authority: Project Steering Committee for major changes
- Cost Impact: Detailed cost analysis for all variations
- Timeline Impact: Schedule impact assessment and approval
- Documentation: All changes documented and approved in writing

O.2 Performance Obligations

O.2.1 Service Level Agreements (SLAs)

SLA Parameter	Development Phase	Production Phase (Warranty)
Code Quality	Minimum 80% test coverage maintained	—
Documentation	Complete documentation per module	—
Response to DOE queries	24-hour response during business hours	—
Critical Issue Resolution	48 hours	24 hours
Standard Issue Resolution	—	72 hours
System Availability	—	99.5% uptime excl. scheduled maintenance
Critical Issue Response	—	4 hours
Normal Issue Response	—	24 hours
Progress Reporting	Weekly on schedule	Monthly SLA report

O.2.2 Deliverable Standards

Quality Standards:

- All deliverables subject to quality review and approval
- Adherence to agreed technical and functional specifications
- Compliance with government standards and guidelines
- User acceptance required for all user-facing deliverables
- Complete documentation and knowledge transfer

O.3 Intellectual Property Rights

O.3.1 Ownership Rights

- Custom Software: Complete ownership with DOE upon final payment
- Source Code: Full source code ownership transferred to DOE
- Documentation: All project documentation owned by DOE
- Data: All migrated and generated data remains DOE property
- Third-party Components: Licensed components remain with respective owners

O.3.2 Usage Rights

- DOE Rights: Unlimited usage, modification, and distribution rights
- Contractor Rights: Right to use generic methodologies and frameworks
- Third-party Rights: Proper licensing and usage rights secured
- Open Source: Any open source components properly licensed and documented

O.3.3 Confidentiality and Non-Disclosure

- Confidentiality Agreement: Comprehensive NDA covering all project information
- Data Protection: Strict data protection and privacy measures
- Information Security: Secure handling of all sensitive information
- Non-Disclosure Period: Confidentiality obligations continue beyond contract completion

O.4 Liability and Insurance

- Professional Liability: Contractor liable for professional negligence
- Data Security: Liability for data breaches during development
- System Downtime: Liability for extended system unavailability
- Limitation of Liability: As per standard government contract terms
- Indemnification: Mutual indemnification clauses

SECTION P: LEGAL AND COMPLIANCE REQUIREMENTS

P.1 Regulatory Compliance

P.1.1 Government Regulations

- Public Procurement Act 2006 and Public Procurement Rules 2025
- Information and Communication Technology Act 2006 (Amended 2009, 2013)
- Digital Security Act 2018
- Cyber Security Act 2023
- Right to Information Act 2009
- Company Act 1994 (for contractor legal status)
- Income Tax Ordinance 1984 (for tax compliance)
- Value Added Tax Act 1991 (for VAT compliance)

P.1.2 ICT and Technical Compliance

- National ICT Policy 2018
- Government ICT Standards and Guidelines
- e-Government Master Plan for Digital Bangladesh
- National Cyber Security Strategy 2014
- Digital Bangladesh Guidelines

P.1.3 Environmental and Sectoral Compliance

- Environment Conservation Act 1995
- Environment Court Act 2010
- Environmental Clearance Procedures
- Relevant DOE Rules and Regulations

P.2 Data Protection and Privacy

P.2.1 Data Governance

- Data Classification: Proper classification of all data types
- Data Residency: All data must remain within Bangladesh jurisdiction
- Data Sovereignty: Government data ownership and control
- Cross-border Data Transfer: Prohibited without government approval
- Data Retention: Compliance with government data retention policies

P.2.2 Privacy Protection

- Personal Data Protection: Protection of personal and sensitive information
- Access Controls: Strict access controls for personal data
- Data Anonymization: Anonymization techniques for reporting and analytics
- Consent Management: Proper consent mechanisms where applicable
- Data Subject Rights: Respect for individual privacy rights

P.2.3 Security Compliance

- Government Security Guidelines: Adherence to all government security standards
- Audit Requirements: Regular security audits and assessments
- Incident Reporting: Mandatory reporting of security incidents

- Compliance Monitoring: Ongoing compliance monitoring and verification

P.3 Ethical and Professional Standards

P.3.1 Professional Ethics

- BASIS Code of Conduct: Adherence to BASIS professional standards
- Software Engineering Ethics: IEEE and ACM ethical guidelines
- Professional Integrity: Honest and transparent business practices
- Conflict of Interest: Declaration and management of conflicts of interest
- Fair Business Practices: Compliance with fair trade and business practices

P.3.2 Environmental and Social Responsibility

- Environmental Responsibility: Environmentally sustainable practices
- Social Responsibility: Positive social impact and community engagement
- Workplace Ethics: Fair employment practices and workplace safety
- Diversity and Inclusion: Promoting diversity in project team
- Local Capacity Building: Knowledge transfer and local skill development

SECTION Q: APPENDICES AND REFERENCES

Q.1 Reference Documents

Q.1.1 Government Policy Documents

31. ICT Policy 2018 — Ministry of Posts, Telecommunications and Information Technology
32. e-Government Master Plan for Digital Bangladesh — ICT Division
33. National Cyber Security Strategy 2014 — ICT Division
34. Public Procurement Act 2006 and Rules 2025 — IMED
35. General Financial Rules 2017 — Ministry of Finance

Q.1.2 Technical Standards and Guidelines

36. Government ICT Standards — ICT Division
37. Web Content Accessibility Guidelines (WCAG) 2.1 — W3C
38. ISO/IEC 27001:2022 — Information Security Management
39. OWASP Top 10 Security Guidelines — OWASP Foundation
40. BASIS Guidelines for Software Development — BASIS
41. Software Requirements Specification (SRS) MEAS v1.2 — DOE & Musa Technologies

Q.1.3 Legal and Regulatory References

42. Digital Security Act 2018 — ICT Division
43. Right to Information Act 2009 — Information Commission
44. Environment Conservation Act 1995 — Dept of Environment
45. Data Protection Guidelines (if applicable) — Relevant Authority

Q.2 Technical Specifications

Q.2.1 System Architecture Diagrams

- High-level System Architecture
- Database Entity Relationship Diagram
- Integration Architecture Diagram
- Security Architecture Diagram
- Deployment Architecture Diagram

Q.2.2 Technical Standards Matrix

Component	Technology / Standard	Version / Specification
Frontend Framework	React.js/Next.js/JS framework	Latest Stable Version
Backend Framework	Node.js/NestJS or Python/Django/php framework	Latest LTS Version
Database	PostgreSQL with PostGIS/ MySQL	Version 13+
API Architecture	RESTful APIs	OpenAPI 3.0
Authentication	OAuth2.0 + JWT	RFC 6749, RFC 7519
Encryption	AES-256	FIPS 140-2
Transport Security	TLS	Version 1.3

Development	Git Version Control	Latest Version
Testing	Automated Testing	80%+ Coverage
Documentation	Technical Documentation	Complete & Updated

Q.3 Project Templates and Forms

Q.3.1 Project Management Templates

- Project Charter Template
- Work Breakdown Structure (WBS) Template
- Risk Register Template
- Issue Tracking Template
- Change Request Form
- Progress Report Template
- Milestone Completion Report Template

Q.3.2 Technical Templates

- System Design Document Template
- API Documentation Template
- Test Case Template
- Code Review Checklist
- Deployment Checklist
- Security Assessment Template

Q.3.3 User Documentation Templates

- User Manual Template
- Training Material Template
- FAQ Template
- Troubleshooting Guide Template
- Quick Reference Guide Template

Q.4 Contact Information

Q.4.1 Government Contacts

Department of Environment (DOE):

Address:	Paribesh Bhaban, E-16/A, Agargaon, Sher-e-Bangla Nagar, Dhaka-1207, Bangladesh
Phone:	+8802-223375032
Email:	sakabir76@gmail.com
Website:	www.doe.gov.bd

Project Director:

Name:	[To be filled]
Designation:	[To be filled]
Phone:	[To be filled]
Email:	[To be filled]

Technical Contact:

Name:	[To be filled]
Designation:	Director (IT)
Phone:	[To be filled]
Email:	[To be filled]

Q.4.4 Implementing Partner Contacts

Selected Firm

Company Address:	[To be filled]
Phone:	[To be filled]
Email:	[To be filled]
Website:	[To be filled]

Project Manager:

Name:	[To be filled]
Phone:	[To be filled]
Email:	[To be filled]

Technical Lead:

Name:	[To be filled]
Phone:	[To be filled]
Email:	[To be filled]

SECTION R: APPROVAL AND AUTHORIZATION

R.1 Document Approval Matrix

Role / Designation	Name	Signature	Date
Project Director, DOE			

R.2 Terms of Reference Validation

R.2.1 Technical Validation

- Technical Architecture: Reviewed and approved by DOE technical team
- Functional Requirements: Validated against business requirements
- Integration Requirements: Confirmed with existing system owners
- Security Requirements: Approved by DOE security team
- Performance Requirements: Validated against current and projected usage

R.2.2 Legal and Compliance Validation

- Procurement Compliance: Verified against PPR 2025 requirements
- Legal Review: Reviewed by DOE legal team
- Financial Compliance: Approved by DOE finance team
- ICT Policy Compliance: Verified against government ICT policies
- Data Protection Compliance: Reviewed for data protection requirements

R.2.3 Business Validation

- Business Case: Validated against project objectives and benefits
- User Requirements: Confirmed with DOE enforcement teams
- Process Alignment: Aligned with DOE business processes
- ROI Justification: Return on investment analysis completed
- Risk Assessment: Comprehensive risk analysis and mitigation planning

R.3 Contract Authorization

This Terms of Reference (ToR) document, upon approval by all designated authorities, shall serve as the foundation for:

- Contract Preparation: Detailed contract document development
- Service Level Agreement: SLA definition and finalization
- Project Implementation: Project execution planning and initiation
- Performance Monitoring: Project progress tracking and evaluation
- Change Management: Scope change control and management
- Dispute Resolution: Reference document for any contractual disputes

R.4 Effective Date and Validity

- Effective Date: Upon signature of the last approving authority
- Validity Period: Valid throughout the project duration and warranty period
- Amendment Process: Any changes require approval from Project Steering Committee
- Version Control: This TOR version 1.0 supersedes all previous versions
- Review Schedule: Annual review or as required for major changes

END OF TERMS OF REFERENCE

This Terms of Reference (TOR) document represents the complete and comprehensive requirements for the development and implementation of the Monitoring & Enforcement Automation System (MEAS) for the Department of Environment, Bangladesh. All parties involved in this project are bound by the terms, conditions, specifications, and requirements outlined in this document.

Document Control

Document Title:	Terms of Reference — Monitoring & Enforcement Automation System (MEAS)
Document Version:	1.0
Total Pages:	[To be updated]
Issue Date:	March 2026
Review Date:	As required
Classification:	Official Use Only

Document Distribution

- Department of Environment (DOE) — Original Copy
- Project File — Archive Copy