GOVERNMENT OF THE PEOPLE'S REPUBLIC OF BANGLADESH

INFORMATION AND COMMUNICATION TECHNOLOGY DIVISION

Ministry of Posts, Telecommunications and Information Technology

NATIONAL CLOUD POLICY OF BANGLADESH 2026

V. 1.0

January 2026

Table Of Contents

ACRONYMS AND ABBREVIATIONS

The following acronyms and abbreviations are used throughout this Policy. Where terms have specific technical or legal meanings in the Bangladesh context, those meanings take precedence over general industry usage.

Acronym	Expansion
ABAC	Attribute-Based Access Control
AES	Advanced Encryption Standard
API	Application Programming Interface
APM	Application Performance Monitoring
ARB	Architecture Review Board
AZ	Availability Zone
BCC	Bangladesh Computer Council
BDCCL	Bangladesh Data Centre Company Limited
BNDA	Bangladesh National Digital Architecture
BNDIA	Bangladesh National Data Governance and Interoperability Architecture
BPaaS	Business Process as a Service
BYOK	Bring Your Own Key
CaaS	Container as a Service
CAB	Change Advisory Board
CASB	Cloud Access Security Broker
CDC	Change Data Capture
CDN	Content Delivery Network
CDO	Chief Data Officer
CI/CD	Continuous Integration / Continuous Deployment
CII	Critical Information Infrastructure
CIS	Center for Internet Security
CISO	Chief Information Security Officer
CMDB	Configuration Management Database
CSO	Cyber Safety Ordinance
CSPM	Cloud Security Posture Management
CVSS	Common Vulnerability Scoring System
DAST	Dynamic Application Security Testing
DDoS	Distributed Denial of Service
DLP	Data Loss Prevention
DNS	Domain Name System
DPIA	Data Protection Impact Assessment
DPI	Digital Public Infrastructure
DR	Disaster Recovery
ECDSA	Elliptic Curve Digital Signature Algorithm
ELK	Elasticsearch, Logstash, Kibana
FaaS	Function as a Service
FIDO2	Fast Identity Online 2

FinOps	Cloud Financial Operations
FQDN	Fully Qualified Domain Name
G-CCF	Government Cloud Control Framework
G-Cloud	Government Cloud
GCTB	Government Cloud Technical Baseline
GPU	Graphics Processing Unit
GRC	Governance, Risk, and Compliance
HIDS	Host-based Intrusion Detection System
HSM	Hardware Security Module
HYOK	Hold Your Own Key
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
IaC	Infrastructure as Code
ICTD	Information and Communication Technology Division
IdP	Identity Provider
IDS/IPS	Intrusion Detection System / Intrusion Prevention System
IoT	Internet of Things
ISO	International Organization for Standardization
JIT	Just-In-Time (access)
KMS	Key Management Service
KPI	Key Performance Indicator
LB	Load Balancer
MFA	Multi-Factor Authentication
MLOps	Machine Learning Operations
mTLS	Mutual Transport Layer Security
MTTD	Mean Time to Detect
MTTR	Mean Time to Recover
NAT	Network Address Translation
NCAD	National Cloud Assurance Dashboard
NCPR	National Cloud Provider Registry
NCSA	National Cybersecurity Agency
NDC	National Data Center
NDGA	National Data Governance Authority
NDGO	National Data Governance Ordinance
NDR	Network Detection and Response
NIST	National Institute of Standards and Technology
NOC	Network Operations Center
NRDEX	National Responsible Data Exchange
NSB	National Service Bus
NSOC	National Security Operations Center
OIDC	OpenID Connect
OT/ICS	Operational Technology / Industrial Control Systems
OTP	One-Time Password
PaaS	Platform as a Service
PAM	Privileged Access Management

PDPO	Personal Data Protection Ordinance
PET	Privacy-Enhancing Technology
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PoC	Proof of Concept
PQC	Post-Quantum Cryptography
PUE	Power Usage Effectiveness
RACI	Responsible, Accountable, Consulted, Informed
RBAC	Role-Based Access Control
RPC	Remote Procedure Call
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SAST	Static Application Security Testing
SBOM	Software Bill of Materials
SCA	Software Composition Analysis
SDLC	Software Development Life Cycle
SIEM	Security Information and Event Management
SITA	Secure Interoperability and Trust Architecture
SLA	Service Level Agreement
SLI	Service Level Indicator
SLO	Service Level Objective
SOAR	Security Orchestration, Automation and Response
SOC	Security Operations Center
SOP	Standard Operating Procedure
SPRB	Security and Privacy Review Board
SRE	Site Reliability Engineering
SSO	Single Sign-On
TCO	Total Cost of Ownership
TEE	Trusted Execution Environment
TLS	Transport Layer Security
TPM	Trusted Platform Module
TPS	Transactions Per Second
UEBA	User and Entity Behavior Analytics
VPC	Virtual Private Cloud
WAF	Web Application Firewall
WORM	Write Once, Read Many
ZTA	Zero Trust Architecture

GLOSSARY OF KEY TERMS & DEFINITIONS

This glossary provides definitions for key terms used throughout this Policy. Definitions are vendor-neutral and focus on how terms affect governance, procurement, architecture, and assurance in the Bangladesh context. Where terms are defined in applicable legislation (PDPO, NDGO, CSO), those legal definitions take precedence.

Cloud Computing

On-demand network access to a shared pool of configurable computing resources (compute, storage, network, services) that can be rapidly provisioned and released with minimal management effort. Policy specifies service models, deployment models, shared responsibility, and security baselines.

Infrastructure as a Service (IaaS)

Cloud service model where the provider supplies virtualized computing infrastructure (compute, storage, network) and the customer controls operating systems, runtime environments, and applications. Government remains responsible for OS hardening, patching, and application security.

Platform as a Service (PaaS)

Cloud service model where the provider manages the underlying infrastructure and runtime environment. Government remains accountable for application logic, data protection, and access control. Reduces operational burden but requires clear responsibility allocation.

Software as a Service (SaaS)

Cloud service model where the provider manages the complete application stack. Government must ensure contractual controls for data handling, access management, audit rights, and exit procedures. Highest provider responsibility but also highest dependency.

Function as a Service (FaaS)

Serverless computing model with event-driven execution of discrete functions. Requires strong governance for secrets management, identity, and observability to prevent shadow functions and privilege drift.

Business Process as a Service (BPaaS)

Cloud delivery of complete business processes including underlying technology. Typically combines SaaS with managed services for specific operational functions.

Government Cloud (G-Cloud)

Cloud services operated for government use under Bangladesh jurisdiction, including sovereign hosting environments at NDC and BDCCL and accredited domestic providers.

Sovereign Cloud Zone

A logically and operationally controlled cloud region or zone located in Bangladesh where data residency is enforced, encryption keys are controlled under Bangladesh jurisdiction, and audit and lawful access conditions are governed by Bangladesh law.

Private Cloud

Cloud infrastructure operated solely for a single organization. May be managed internally or by a third party, and may be hosted on-premises or externally, but maintains exclusive tenancy.

Public Cloud

Cloud infrastructure available to the general public or large industry groups. For government use, public cloud services must be accredited against national security, privacy, and residency requirements before deployment of government workloads.

Hybrid Cloud

Composition of two or more distinct cloud deployment models bound together by standardized or proprietary technology enabling data and application portability. Requires unified governance and identity management.

Community Cloud

Cloud infrastructure shared by several organizations with common concerns (mission, security, compliance, policy). May be managed by organizations or third parties.

Data Classification

The process of categorizing data based on sensitivity, regulatory requirements, and risk to determine appropriate handling controls. This Policy uses D0-D4 classification levels from Open to National Critical.

Data Residency

Requirements specifying the geographic location where data must be stored and processed. For D2-D4 data, residency within Bangladesh jurisdiction is typically required.

Data Sovereignty

The principle that data is subject to the laws of the jurisdiction where it is located. This Policy ensures that government data remains under Bangladesh legal control.

Cross-Border Processing

Any processing of data that occurs outside Bangladesh jurisdiction, including storage, computation, access, or transfer. Subject to restrictions based on data classification.

Data Fiduciary

Under PDPO, the entity that determines the purposes and means of processing personal data. Government agencies are typically Data Fiduciaries for citizen-facing services.

Data Processor

Under PDPO, an entity that processes personal data on behalf of a Data Fiduciary. Cloud providers typically act as Data Processors when processing government data.

Zero Trust Architecture (ZTA)

Security model based on the principle of 'never trust, always verify' that requires continuous verification of every access request regardless of network location or previous authentication status.

Identity and Access Management (IAM)

Framework of policies and technologies ensuring that the right individuals access the right resources at the right times for the right reasons. Foundation for access control in cloud environments.

Privileged Access Management (PAM)

Controls for managing and monitoring access to privileged accounts with elevated permissions. Includes just-in-time elevation, session recording, and break-glass procedures.

Multi-Factor Authentication (MFA)

Authentication requiring two or more independent factors (knowledge, possession, inherence). Mandatory for privileged access and access to D2+ data.

Role-Based Access Control (RBAC)

Access control based on organizational roles. Users are assigned to roles, and roles are granted permissions.

Attribute-Based Access Control (ABAC)

Access control based on attributes of users, resources, and environment. Enables fine-grained, context-aware authorization.

Federation

Technology enabling identity and authentication to be shared across multiple systems or organizations using standards like SAML or OIDC.

Encryption at Rest

Cryptographic protection of data while stored on persistent media (disks, databases, backups). Mandatory for D2+ data using AES-256 or equivalent.

Encryption in Transit

Cryptographic protection of data while being transmitted over networks. TLS 1.2 or higher is mandatory for all government cloud communications.

Key Management Service (KMS)

System for creating, storing, managing, and controlling cryptographic keys. For D3+ data, KMS must be under Bangladesh jurisdiction.

Hardware Security Module (HSM)

Physical device providing secure key storage and cryptographic operations with tamper resistance. Required for highest-sensitivity key management.

Bring Your Own Key (BYOK)

Model where the customer generates and maintains ownership of encryption keys used by the cloud provider. Provides key control while using provider encryption services.

Hold Your Own Key (HYOK)

Model where the customer retains keys externally and the provider cannot decrypt data without customer authorization. Strongest key sovereignty control.

Recovery Time Objective (RTO)

Maximum acceptable time to restore service after a disruption. Determined by business impact analysis and criticality tier.

Recovery Point Objective (RPO)

Maximum acceptable data loss measured in time. Determines backup frequency and replication requirements.

Service Level Objective (SLO)

Target value for a service level indicator (e.g., 99.9% availability). Basis for operational commitments and monitoring.

Service Level Agreement (SLA)

Formal agreement between provider and customer specifying service commitments, measurements, and remedies for non-performance.

Disaster Recovery (DR)

Capabilities and procedures to restore services after major outages or disasters. Includes tested failover procedures and documented runbooks.

Site Reliability Engineering (SRE)

Discipline applying software engineering to operations problems, emphasizing automation, monitoring, and error budgets.

Security Information and Event Management (SIEM)

System aggregating and analyzing security events from multiple sources to detect threats and support incident response.

Security Operations Center (SOC)

Facility and team responsible for monitoring, detecting, and responding to security incidents. Integration with NSOC required for CII systems.

Cloud Security Posture Management (CSPM)

Tools and processes for continuous monitoring and remediation of cloud security misconfigurations.

Vulnerability Management

Process for identifying, evaluating, treating, and reporting security vulnerabilities. Includes scanning, prioritization, and remediation tracking.

Penetration Testing

Authorized simulated attack to evaluate security controls. Required annually for C2+ criticality services.

Data Protection Impact Assessment (DPIA)

Systematic assessment of data processing operations to identify and mitigate privacy risks. Required for high-risk processing under PDPO.

DevSecOps

Integration of security practices throughout the software development lifecycle, from design through operations. Security is a shared responsibility, not a gate.

Static Application Security Testing (SAST)

Analysis of source code to identify security vulnerabilities before execution. Part of secure development pipeline.

Dynamic Application Security Testing (DAST)

Testing of running applications to identify vulnerabilities. Complements SAST with runtime analysis.

Software Composition Analysis (SCA)

Analysis of third-party and open-source components to identify vulnerabilities and licensing issues.

Software Bill of Materials (SBOM)

Inventory of components comprising a software artifact. Required for C2+ criticality to enable vulnerability tracking.

Infrastructure as Code (IaC)

Managing infrastructure through machine-readable definition files rather than manual configuration. Enables version control, testing, and auditability.

Digital Public Infrastructure (DPI)

Shared digital building blocks (identity, payments, data exchange, registries) enabling broad service delivery across government and private sector.

Bangladesh National Digital Architecture (BNDA)

National framework defining standards, patterns, and building blocks for digital government including interoperability requirements.

National Service Bus (NSB)

Integration platform enabling secure, standardized communication between government systems.

National Responsible Data Exchange (NRDEX)

Platform and framework for governed data sharing between agencies with consent management and audit trails.

Critical Information Infrastructure (CII)

Systems and assets whose incapacity or destruction would have debilitating impact on national security, economy, or public welfare. Designated under CSO with enhanced security requirements.

CHAPTER 1: INTRODUCTION

1.1 Purpose and Scope of the Policy

Bangladesh is accelerating its digital transformation to improve public service delivery, expand financial and social inclusion, and enable trusted data exchange across government agencies and the broader digital ecosystem. Cloud computing has emerged as a foundational capability for delivering scalable, resilient, and cost-effective digital public services, as well as for enabling the shared building blocks of Digital Public Infrastructure (DPI), including identity verification systems, payment platforms, data registries, and interoperability services that form the backbone of modern governance.

This Policy establishes a unified, enforceable, and technically comprehensive framework for the adoption, deployment, operation, and governance of cloud services across the Government of Bangladesh. The framework addresses the full spectrum of cloud computing considerations, from Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) to Software as a Service (SaaS), Container as a Service (CaaS), Function as a Service (FaaS), and Business Process as a Service (BPaaS). The Policy applies to all deployment models including public cloud, private cloud, community cloud, hybrid cloud, and multi-cloud architectures.

The Policy serves multiple interconnected purposes. First, it provides binding governance for cloud adoption decisions, ensuring that ministries, divisions, departments, and agencies make informed choices regarding cloud service providers, deployment models, and workload placement based on data classification, security requirements, and national interest considerations. Second, it establishes technical baselines and control requirements that ensure consistent security posture, privacy protection, and operational resilience across all government cloud deployments. Third, it creates accountability mechanisms through defined institutional roles, compliance monitoring, and enforcement procedures that ensure policy adherence.

Furthermore, the Policy establishes the technical and governance foundations for integrating cloud infrastructure with the Bangladesh National Digital Architecture (BNDA) and the National Service Bus (NSB), enabling seamless interoperability across government systems. It provides the framework for operationalizing the National Responsible Data Exchange (NRDEX) platform, which facilitates secure, purpose-based data sharing through standardized Application Programming Interfaces (APIs). The Policy also addresses the integration of advanced trust services, including the Blockchain Remote Procedure Call (RPC) layer and TPS Exchange services, which provide cryptographic assurance for high-value government transactions.

1.2 Policy Authority and Legal Mandate

This Policy is issued by the Information and Communication Technology (ICT) Division under its constitutional mandate to formulate policies, plans, and programmes relating to information and communication technology for the Government of the People's Republic of Bangladesh. The Policy derives its authority from and operates in conjunction with the following legislative instruments and strategic frameworks:

The National Data Governance Ordinance, 2025 (NDGO) creates the National Data Governance Authority (NDGA) and establishes the Bangladesh National Data Governance and Interoperability Architecture (BNDIA). The NDGO mandates interoperability across government systems, defines data classification frameworks, establishes Chief Data Officers at institutional levels, and creates enforcement mechanisms for data governance compliance. Section 21 of the NDGO legally establishes BNDIA as the architectural backbone for

Bangladesh's Digital Public Infrastructure, providing the legal foundation for cloud-based data exchange and interoperability services.

The Personal Data Protection Ordinance, 2025 (PDPO) fundamentally redefines the relationship between citizens and their personal data, establishing personal data as the owned property of data subjects. The PDPO grants comprehensive data subject rights including the Right to Access under Section 10, the Right to Data Portability through Federated Interoperable Ecosystems under Section 11, the Right to Correction and Erasure under Section 12, the Right to Consent Withdrawal under Section 13, and mandates System-Wide Propagation of data updates across all connected systems under Section 14. These provisions create specific technical requirements that cloud implementations must address, including consent management, data minimization, purpose limitation, and erasure capabilities.

The Cyber Safety Ordinance, 2025 (CSO) introduces the Critical Information Infrastructure (CII) designation and establishes the National Security Operations Center (NSOC) under the National Cybersecurity Agency (NCSA). The CSO defines CII as any infrastructure whose damage or disruption would impact public safety, economic security, or national sovereignty. Cloud systems supporting government functions, particularly those handling citizen data or enabling essential services, may be designated as CII, subjecting them to heightened security standards, mandatory NSOC connectivity, regular security audits, vulnerability assessments, and incident reporting requirements.

The National Digital Transformation Strategy provides the strategic roadmap for Bangladesh's transition from digitization of analog processes toward the creation of integrated Digital Public Infrastructure. The Strategy articulates the phased progression from the Secure Trusted Architecture for Responsible Exchange (STAR) phase to full implementation of the Digital Secure Trusted Architecture for Responsible Exchange (DSTAR), establishing clear milestones for cloud infrastructure deployment, interoperability enablement, and trust service implementation.

1.3 Scope and Applicability

1.3.1 Covered Entities

This Policy applies to all ministries, divisions, departments, agencies, statutory bodies, local government entities, and state-owned enterprises that:

Process government data in any form, including administrative records, operational data, policy documents, and financial information, regardless of sensitivity classification.

Provide digital public services to citizens, businesses, or other government entities, whether directly or through intermediaries such as Union Digital Centers.

Operate or consume shared platforms under the Bangladesh National Digital Architecture (BNDA), including API gateways, National Service Bus, NRDEX connectors, and common identity services.

The Policy also applies to vendors, system integrators, managed service providers, and any third parties that design, host, operate, maintain, or access government cloud workloads and data. Contracts shall flow down applicable requirements to subcontractors, ensuring consistent controls throughout the service delivery chain.

1.3.2 In-Scope Systems and Workloads

The following system categories and workload types fall within the scope of this Policy:

Citizen-Facing Digital Services: Portals, mobile applications, service centers, digital channels, and any systems that directly interact with citizens or businesses to deliver government services.

Core Government Registries: Identity-linked registries, licensing systems, land records, health registries, education records, taxation systems, and their integration services. These registries constitute foundational data assets requiring enhanced protection.

Interoperability Platforms: API gateways, National Service Bus components, NRDEX connectors and services, identity federation infrastructure, and event streaming platforms that enable data exchange across government.

Collaboration and Productivity Systems: Email systems, document management platforms, workflow automation, enterprise resource planning (ERP), and other line-of-business systems where government data is processed.

Analytics and AI/ML Platforms: Data lakes, data warehouses, business intelligence systems, machine learning training and inference platforms, and event streaming systems used for analytics and decision support.

IoT and Edge Workloads: Sensor networks, remote monitoring systems, disaster telemetry, smart infrastructure, and sectoral control systems where cloud is used for monitoring, command, or analytics.

1.3.3 Exclusions and Boundaries

While this Policy establishes the framework for government cloud adoption, the following areas are addressed by separate instruments or require additional specific guidance:

Defense and Intelligence Systems: Classified defense systems and intelligence community infrastructure are governed by separate security frameworks. This Policy applies to unclassified administrative systems within defense establishments.

Critical Infrastructure Control Systems: Operational technology (OT) and industrial control systems (ICS) for power, water, transportation, and other critical infrastructure require specialized security considerations addressed through sector-specific guidance aligned with this Policy.

Private Sector Cloud Adoption: This Policy directly governs government cloud adoption. Private sector organizations are encouraged to adopt relevant security and interoperability provisions, particularly where they process government data or provide services to government agencies.

1.4 Risk Scenarios Addressed

This Policy explicitly addresses the following risk scenarios and corner cases that experience has shown require clear policy guidance:

1.4.1 Data Sovereignty and Foreign Access Risks

Cross-Border Processing and Foreign Lawful Access: SaaS and public cloud services may involve foreign entities with access to government data, including support personnel access, remote administration, and exposure to third-country legal demands such as subpoenas.

Data Replication and Caching: CDN edge caches, object storage replication, backup copies, and log aggregation can create unintentional cross-border transfer of data, potentially violating residency requirements without explicit awareness.

Telemetry as Personal Data: Logs, traces, metrics, and security events may contain personal identifiers and must be governed under PDPO obligations, requiring careful consideration of where telemetry data is processed and stored.

1.4.2 Security and Isolation Risks

Encryption Key Control and Sovereignty: Requirements for KMS/HSM use, key residency, key rotation, and customer-controlled keys (BYOK/HYOK) must be clearly defined to ensure cryptographic protection remains under government control.

Multi-Tenancy and Isolation Failure: Shared cloud infrastructure creates risks including hypervisor escape, side-channel attacks, noisy neighbor performance impacts, and container breakout scenarios that must be addressed through appropriate isolation controls.

Identity Federation Failures: Misconfigured SSO/OIDC/SAML implementations can lead to privilege escalation or account takeover, requiring robust identity architecture and continuous validation.

1.4.3 Operational and Continuity Risks

Supply Chain Compromise: Dependency confusion, compromised build pipelines, unsigned artifacts, and lack of SBOMs create risks of malicious code introduction that must be addressed through secure software supply chain practices.

Exit and Continuity: Vendor lock-in, egress cost shocks, provider insolvency, and loss of operational knowledge can compromise government's ability to maintain services, requiring proactive exit planning and portability measures.

Disconnected Operations: Edge caching, offline-first service modes, and delayed synchronization requirements for remote and low-connectivity areas must be addressed to ensure inclusive service delivery.

Shared Platform Risks: Multi-ministry platforms require separation-of-duty and tenant isolation controls to prevent inappropriate access across organizational boundaries.

1.5 Policy Objectives

This Policy aims to achieve the following strategic objectives that align with Bangladesh's broader digital transformation agenda and support the nation's aspirations for achieving the Sustainable Development Goals (SDGs) by 2030 targets:

The Policy seeks to enable Digital Public Infrastructure by establishing the cloud foundations necessary for scalable, secure, and interoperable DPI building blocks. This includes providing the infrastructure layer for identity systems, payment platforms, consent management frameworks, and data exchange mechanisms that form the core of citizen-centric digital governance. The cloud infrastructure shall support the Bangladesh National Digital Architecture (BNDA) and enable seamless integration with the National Service Bus (NSB) for standardized data exchange across government systems.

The Policy aims to ensure data sovereignty and maintain lawful control over citizen data and government information. This requires establishing clear rules for data residency, ensuring that sensitive and critical data categories are processed within Bangladesh's territorial jurisdiction, and maintaining cryptographic key custody under sovereign control. The Policy recognizes that true data sovereignty extends beyond physical data location to encompass control over encryption keys, access policies, and the legal framework governing data processing.

The Policy establishes a comprehensive security baseline that implements defense-in-depth principles and Zero Trust Architecture (ZTA) across government cloud deployments. This includes mandatory requirements for Identity and Access Management (IAM), Privileged Access Management (PAM), network segmentation, encryption in transit and at rest, Hardware Security Module (HSM) backed key management, continuous security monitoring, and integration with the National Security Operations Center (NSOC) for threat detection and incident response coordination.

The Policy ensures privacy protection by design, embedding PDPO compliance requirements into cloud architecture decisions, procurement specifications, and operational procedures. This includes implementing consent management frameworks, enabling data subject rights through technical mechanisms, conducting Data Protection Impact Assessments (DPIAs) for high-risk processing activities, and establishing breach notification procedures that meet regulatory timelines and requirements.

The Policy promotes operational excellence through standardized service management practices, Site Reliability Engineering (SRE) principles, comprehensive observability stacks, and mature incident response capabilities. This includes establishing Service Level Objectives (SLOs) and Service Level Indicators (SLIs) for government services, implementing continuous compliance monitoring, and maintaining disaster recovery and business continuity capabilities that ensure service resilience during disruptions.

The Policy ensures cost efficiency and sustainability through Financial Operations (FinOps) practices that provide visibility into cloud spending, enable capacity planning, and prevent cost overruns. The Policy also addresses Green Cloud considerations, requiring energy efficiency metrics, sustainable procurement practices, and measurable environmental performance from cloud infrastructure and operations.

1.6 Definitions and Interpretation

For the purposes of this Policy, terms shall have the meanings assigned in the National Data Governance Ordinance, 2025, the Personal Data Protection Ordinance, 2025, the Cyber Safety Ordinance, 2025, unless the context requires otherwise. Where this Policy uses terms that are defined differently across these instruments, the definition most aligned with the context of cloud computing and digital infrastructure shall apply. The following key definitions provide essential context for interpreting this Policy:

Cloud Computing refers to on-demand network access to a shared pool of configurable computing resources including compute capacity, storage, networking, and services that can be

rapidly provisioned and released with minimal management effort, typically with metered usage. This definition encompasses all service models including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), Container as a Service (CaaS), Function as a Service (FaaS), and Business Process as a Service (BPaaS).

Government Cloud (G-Cloud) refers to cloud computing environments that are specifically designed, operated, and governed to meet the security, compliance, and sovereignty requirements of government agencies. Government Cloud may be operated by designated government entities such as the Bangladesh Data Centre Company Limited (BDCCL) or the National Data Center (NDC), or by accredited Cloud Service Providers operating under government-approved security frameworks.

Digital Public Infrastructure (DPI) refers to shared, secure, and interoperable digital systems that serve as foundational building blocks for service delivery across government and the private sector. DPI typically includes identity systems, payment platforms, data exchange mechanisms, consent management frameworks, and registries that enable broad-based service delivery while maintaining citizen privacy and government accountability.

Zero Trust Architecture (ZTA) refers to a security approach that assumes no implicit trust in any user, device, or network segment, regardless of whether they are inside or outside the traditional network perimeter. ZTA requires explicit verification of identity and authorization for every access request, implements least privilege access principles, and maintains continuous monitoring of security posture and behavioral patterns.

Critical Information Infrastructure (CII) refers to any computer resource, the damage or disruption of which would have a debilitating impact on national security, economy, public health, public safety, or any other function of government. The designation of CII and associated security obligations are governed by the Cyber Safety Ordinance, 2025, and administered by the National Cybersecurity Agency (NCSA).

CHAPTER 2: NATIONAL CONTEXT AND DIGITAL TRANSFORMATION ALIGNMENT

2.1 Bangladesh's Digital Transformation Journey

Bangladesh stands at a pivotal juncture in its digital transformation journey. The nation has witnessed remarkable progress in digital adoption over the past two decades, with over 120 million internet users and a rapidly growing digital economy that increasingly drives economic growth, social inclusion, and government efficiency.

However, the current digital landscape presents both significant opportunities and pressing challenges that necessitate advanced technological interventions. The existing digital ecosystem faces challenges of fragmented data islands, wherein isolated registries for National Identity, taxation, land records, education, and healthcare operate without real-time coordination or data sharing capabilities. This fragmentation results in duplication of digital assets across government agencies, increased operational costs from redundant systems, vulnerability to data breaches from inconsistent security practices, and inability to deliver seamless end-to-end digital services that citizens expect.

The absence of secure interoperability mechanisms between government agencies impedes efficient service delivery and creates friction for citizens navigating multiple bureaucratic touchpoints. Citizens must repeatedly provide the same information to different agencies, verification processes are slow and manual, and the lack of trusted data exchange prevents the creation of streamlined, citizen-centric services that leverage authoritative data from multiple sources.

The Fourth Industrial Revolution (4IR) exposes both new challenges and transformative opportunities for nations worldwide. Cloud computing, together with artificial intelligence, blockchain technology, and the Internet of Things, represents one of the core foundational technologies driving this global transformation. Only countries with strategic capability in these emerging technologies can successfully meet the challenges and exploit the opportunities presented by the digital age. Recognizing this imperative, the Government of Bangladesh has committed to leveraging cloud computing as a fundamental enabler for preparing the nation for future challenges and benefiting its citizens in achieving the Sustainable Development Goals by 2030 and Vision 2041.

2.2 Existing Sovereign Cloud Assets and Infrastructure

Bangladesh has made significant investments in establishing sovereign cloud infrastructure that provides the foundation for government cloud services. The National Data Center (NDC), operated under the Bangladesh Computer Council (BCC), represents the primary sovereign hosting facility for government workloads requiring the highest levels of data sovereignty and security assurance. The NDC provides Infrastructure as a Service capabilities including compute, storage, and networking resources that meet government security requirements and maintain data residency within Bangladesh's territorial jurisdiction.

The Bangladesh Data Centre Company Limited (BDCCL), operating as the designated Government Cloud service integrator, provides managed cloud services including IaaS, PaaS, and managed application hosting for government agencies. BDCCL's Government Cloud infrastructure is specifically designed to meet the security, compliance, and sovereignty requirements of government workloads, with direct integration points to the Bangladesh National Digital Architecture (BNDA) and the National Service Bus (NSB). BDCCL provides standardized landing zones, identity federation services, and operational support that reduce the

burden on individual agencies while ensuring consistent security posture across government deployments.

Meghna Cloud and other accredited domestic cloud service providers complement sovereign government infrastructure by providing additional capacity, specialized services, and alternative options for workloads that do not require exclusive sovereign hosting. These providers operate under accreditation frameworks established by this Policy and must demonstrate compliance with government security baselines, data residency requirements, and audit obligations. The ecosystem of accredited providers creates competitive options for government agencies while maintaining the governance controls necessary for public sector cloud adoption.

The Info-Sarker network connects government offices nationwide, providing the network backbone for government cloud connectivity. This network is undergoing comprehensive reform and upgrade to enhance resilience, redundancy, and nationwide coverage. Current limitations in network monitoring and bandwidth allocation are being addressed through SNMP-ready infrastructure and modern Network Management Systems (NMS), ensuring that cloud workloads can be accessed reliably across the government network footprint.

2.3 Alignment with Digital Public Infrastructure Framework

This Policy is designed to enable and support the implementation of Bangladesh's Digital Public Infrastructure vision as articulated in the National Digital Transformation Strategy. The Strategy establishes a phased progression from the Secure Trusted Architecture for Responsible Exchange (STAR) to the Digital Secure Trusted Architecture for Responsible Exchange (DSTAR), with cloud infrastructure serving as the foundational layer for DPI component deployment.

The STAR phase, covering the period from 2025 to 2026, focuses on establishing foundational governance frameworks, regulatory compliance mechanisms, and critical infrastructure deployment. During this phase, cloud infrastructure shall support the deployment of the SITA Gateway (System Integration for Trusted Access) across initial ministries, connecting agencies including the National Board of Revenue, Bangladesh Bureau of Statistics, Bangladesh Public Procurement Authority, Planning Commission, and the Office of the Comptroller and Auditor General. The phase establishes the Bangladesh National Digital Architecture under the National Data Governance Authority and launches National Data Exchange pilots with initial cross-sector API implementations.

The Sectoral Gateway architecture introduces a critical layer between individual service agencies and the core NDGIA infrastructure. This gateway provides protocol translation and format standardization across different legacy systems, request routing and load balancing for efficient resource utilization, security proxy services including authentication, authorization, and audit logging, and data transformation services to ensure compatibility with BNDA standards. Cloud infrastructure must support this gateway architecture with appropriate network segmentation, API management capabilities, and observability tooling.

The transition to DSTAR represents the culmination of Bangladesh's DPI vision, introducing advanced technological capabilities while consolidating governance frameworks. Key components requiring cloud infrastructure support include the National Responsible Data Exchange (NRDEX) platform for secure, API-based data sharing with purpose-based access controls and comprehensive audit trails; the Unified Identity Layer enabling interoperability between National Identity, Birth Registration, Passport, and Business ID systems with system-wide propagation of updates; the National Security Operations Center (NSOC) for real-time monitoring of network and data anomalies across all DPI components; and the Trust and

Certificate Chain Authority (TRUST-CCA) ensuring authenticity and integrity of data transactions through Public Key Infrastructure (PKI).

The cloud infrastructure shall support the Blockchain RPC Layer that provides cryptographic assurance for high-value government transactions. This layer enables trust services including immutable audit trails, attestation services, and verifiable credentials that support government operations requiring non-repudiation and tamper-evidence. The TPS Exchange services provide transaction processing capabilities that integrate with the broader DPI ecosystem while maintaining security and compliance requirements. These advanced trust services require cloud infrastructure with specific capabilities for cryptographic operations, including Hardware Security Module (HSM) integration and secure key management.

2.4 Legal and Regulatory Framework Alignment

2.4.1 National Data Governance Ordinance, 2025 (NDGO) Compliance

The NDGO creates the comprehensive institutional and legal framework for data governance in Bangladesh. The Ordinance establishes the National Data Governance Authority (NDGA) as the central coordinating body for data governance across government and the private sector. Key provisions affecting cloud implementation include the mandate for interoperability under Section 21, which legally establishes the Bangladesh National Data Governance and Interoperability Architecture (BNDIA) as the architectural backbone for data exchange; the data classification requirements that determine workload placement and security controls; the requirement for Chief Data Officers at institutional levels to oversee data governance compliance; and the enforcement mechanisms for data governance violations.

Cloud implementations must support NDGO compliance through technical mechanisms including data classification tagging in cloud metadata that enables automated policy enforcement; access control policies aligned with data governance requirements and role-based permissions; audit logging that demonstrates compliance with governance rules including data access, modifications, and sharing events; and API implementations that conform to BNDIA interoperability standards for cross-agency data exchange. The Policy establishes specific technical requirements for each data classification category, ensuring that cloud workload placement and security controls align with NDGO obligations.

2.4.2 Personal Data Protection Ordinance, 2025 (PDPO) Compliance

The PDPO establishes comprehensive privacy rights for data subjects and corresponding obligations for data controllers and processors. Cloud services processing personal data must implement technical and organizational measures to support PDPO compliance. Key requirements include the implementation of consent management frameworks that capture, store, and enforce consent preferences across cloud services with full audit trails; technical mechanisms enabling data subject rights including automated access request responses, data export in portable formats, correction propagation across systems, and erasure verification; Data Protection Impact Assessments (DPIAs) for processing activities that present high risks to data subjects, with documented risk mitigation measures; privacy by design and privacy by default in cloud architecture decisions, ensuring that data collection is minimized and protection is automatic; and breach notification capabilities meeting the regulatory timelines specified in the PDPO, including detection, assessment, and communication procedures.

Section 14 of the PDPO mandates System-Wide Propagation of data updates, requiring that corrections or deletions to personal data are propagated across all connected systems. This creates specific technical requirements for cloud implementations, including event-driven architectures that propagate data changes across services and agencies, synchronization mechanisms that

ensure consistency across distributed systems with appropriate conflict resolution, and deletion verification procedures that confirm removal across all storage locations including backups, replicas, and archived data. Cloud architectures must be designed to support these propagation requirements while maintaining operational efficiency and system stability.

2.4.3 Cyber Safety Ordinance, 2025 (CSO) Compliance

The CSO establishes the cybersecurity framework for Bangladesh, including Critical Information Infrastructure designation and protection requirements. Cloud systems supporting essential government functions may be designated as CII, triggering enhanced security obligations. Key CSO requirements affecting cloud implementations include mandatory connectivity to the National Security Operations Center (NSOC) for CII-designated systems, enabling real-time threat monitoring and coordinated incident response; vulnerability assessment and penetration testing requirements conducted by qualified assessors at specified intervals; incident reporting obligations with defined timelines for initial notification and detailed reporting to competent authorities; security audit requirements and compliance monitoring with documented remediation procedures for identified gaps; and business continuity and disaster recovery requirements for essential services with tested failover procedures.

The CSO recognizes the citizen's right to continuous internet access as part of cyber protection, acknowledging the internet as essential infrastructure for modern life and economic participation. This provision has implications for cloud service availability requirements, particularly for citizen-facing services that support essential activities. Cloud deployments must implement appropriate resilience measures to ensure service availability consistent with CSO expectations, including geographic redundancy, automated failover, and capacity planning that accommodates peak demand scenarios.

2.5 Vision for Cloud-Enabled Digital Bangladesh

This Policy envisions a Bangladesh where cloud computing serves as the foundational infrastructure for a digitally empowered society that delivers inclusive, efficient, and trustworthy public services. By 2030, the Government Cloud ecosystem shall enable seamless delivery of over 800 digital government services, with at least 50 percent of services fully digitized and accessible through multiple channels. The cloud infrastructure shall support the processing of millions of daily transactions across identity verification, payment processing, data exchange, and citizen service delivery while maintaining the highest standards of security, privacy, and operational resilience.

The vision encompasses a government cloud ecosystem characterized by sovereignty and trust, where citizen data remains under sovereign control with appropriate data residency, key management, and legal jurisdiction; interoperability and efficiency, where standardized APIs and data exchange patterns eliminate duplication and enable cross-agency service delivery with data accessed from authoritative sources rather than copied across systems; security and resilience, where Zero Trust Architecture, comprehensive monitoring, and tested disaster recovery capabilities protect government operations against both cyber threats and natural disasters; innovation and agility, where modern cloud-native architectures enable rapid deployment of new services and continuous improvement of existing ones without lengthy procurement and development cycles; and sustainability and cost-effectiveness, where efficient resource utilization, optimized spending, and green computing practices ensure responsible stewardship of public resources while delivering maximum value to citizens.

CHAPTER 3: VISION, STRATEGIC OUTCOMES, AND GUIDING PRINCIPLES

3.1 Policy Vision Statement

The Government of Bangladesh shall establish and operate a secure, sovereign, interoperable, and citizen-centric Government Cloud ecosystem that enables efficient public service delivery, protects citizen data, supports Digital Public Infrastructure, and positions Bangladesh as a regional leader in cloud-enabled digital governance while maintaining strict compliance with national laws governing data protection, cyber safety, and data governance.

This vision recognizes that cloud computing is not merely a technical infrastructure choice but a strategic enabler of government transformation. The Government Cloud shall serve as the digital foundation upon which efficient, transparent, and responsive governance is built, enabling civil servants to focus on policy outcomes rather than infrastructure management, and enabling citizens to access services conveniently while maintaining confidence that their data is protected.

3.2 Strategic Outcomes

The successful implementation of this Policy shall deliver measurable outcomes across multiple dimensions that contribute to Bangladesh's digital transformation objectives:

3.2.1 Service Delivery Excellence

Government digital services shall achieve availability targets exceeding 99.5 percent for standard services and 99.9 percent for essential and critical services. Citizens shall experience consistent, responsive service delivery regardless of geographic location or access channel. Service latency targets shall ensure that citizen-facing transactions complete within acceptable timeframes, with continuous monitoring and optimization to maintain service quality.

3.2.2 Security and Trust

Government cloud environments shall maintain robust security postures with no critical security incidents resulting from policy non-compliance. Security baselines shall be uniformly applied across all cloud deployments, with continuous compliance monitoring and rapid remediation of identified vulnerabilities. Citizen trust in government digital services shall increase through demonstrated commitment to data protection and transparent security practices.

3.2.3 Operational Efficiency

Cloud adoption shall deliver measurable efficiency gains including reduced time-to-deployment for new services, lower total cost of ownership compared to traditional on-premises infrastructure, and improved utilization of computing resources. Shared platform services shall reduce duplication of effort across government, with agencies consuming common capabilities rather than building redundant systems.

3.2.4 Interoperability and Integration

Government systems shall achieve seamless interoperability through standardized APIs and data exchange patterns aligned with the Bangladesh National Digital Architecture. Cross-agency data sharing shall operate securely and efficiently through the National Responsible Data Exchange platform, eliminating manual data reconciliation and enabling real-time service delivery that spans multiple government agencies.

3.2.5 Capacity Development

Government shall develop and maintain skilled human capital capable of designing, operating, and governing cloud environments. This includes technical specialists in cloud architecture, security, and operations; governance professionals capable of ensuring compliance and managing risk; and leadership capable of making informed strategic decisions regarding cloud adoption and investment.

3.3 Guiding Principles

The following principles shall guide all decisions regarding cloud adoption, architecture, procurement, operation, and governance within the Government of Bangladesh. These principles are derived from international best practices, aligned with Bangladesh's legal framework, and designed to ensure that cloud adoption delivers intended benefits while managing associated risks.

3.1 Sovereignty and Lawful Control

3.1.1 Principle Statement

Government must maintain effective legal and operational control over sensitive data and critical workloads. Cloud adoption shall not compromise Bangladesh's sovereignty over its digital assets, and shall be designed to ensure that government retains the ability to access, control, and protect its data under Bangladesh law.

3.1.2 Implementable Directives

Workload Placement: Workloads containing restricted or sensitive data shall be placed in sovereign cloud zones as required by data classification. Placement decisions shall be documented and justified based on risk assessment.

Encryption Key Control: Encryption keys for restricted workloads (D3 and above) shall be controlled under Bangladesh jurisdiction. Key management systems shall be located within Bangladesh, and key access shall be subject to Bangladesh legal process only.

Cross-Border Processing: Cross-border processing of government data shall be explicitly authorized and auditable. Any data transfer outside Bangladesh shall be documented, risk-assessed, and subject to appropriate safeguards.

Administrative Access: Administrative access to systems containing restricted data shall be limited to personnel under Bangladesh jurisdiction. Remote administration from foreign locations shall be prohibited for high-sensitivity systems.

Lawful Access Procedures: Procedures for lawful access to cloud-hosted government data shall be defined and subject to appropriate legal process under Bangladesh law. Foreign legal demands shall not result in data disclosure without Bangladesh government authorization.

3.1.3 Sovereignty Assessment Criteria

Assessment Factor	Sovereign Cloud Zone	Accredited Public Cloud	Non-Resident Cloud
Data Residency	Bangladesh only	Bangladesh zone/region	Foreign jurisdiction
Key Custody	Bangladesh-controlled	BYOK with BD custody	Provider-managed
Administrative Access	BD personnel only	BD personnel + controlled foreign	Provider personnel
Legal Jurisdiction	Bangladesh law exclusive	Bangladesh law primary	Foreign law exposure
Audit Access	Full government access	Contractual audit rights	Limited or none
Eligible Data Classes	D0-D4	D0-D2 (D3 with controls)	D0-D1 only

3.2 Interoperability-by-Default

3.2.1 Principle Statement

Public services require consistent integration and reuse across agencies. Cloud deployments shall be designed from the outset for interoperability with other government systems, avoiding architectural decisions that impede data sharing, service composition, or future system evolution.

3.2.2 Implementable Directives

API-First Design: All new systems shall expose well-documented APIs following government API standards. APIs shall use open standards (REST, GraphQL, OpenAPI 3.0) and avoid proprietary protocols that limit interoperability.

Data Exchange Standards: Data exchange shall use agreed schemas and standards aligned with BNDA specifications. Semantic interoperability shall be achieved through common data models, controlled vocabularies, and standard identifiers.

BNDA-Aligned Integration: Integration shall leverage BNDA-aligned services including National Service Bus (NSB), API gateways, and NRDEX connectors. Systems shall not implement point-to-point integrations that bypass standard integration patterns.

Identity Federation: Authentication shall use federated identity services and standard protocols (SAML 2.0, OIDC). Systems shall not implement standalone identity silos that require separate credentials.

Event-Driven Architecture: Where appropriate, systems shall support event-driven integration patterns enabling loose coupling and real-time data synchronization across government platforms.

3.2.3 Interoperability Levels

Interoperability Level	Description	Requirements
Technical	Systems can exchange data	Standard protocols, API specifications, network connectivity

Syntactic	Systems interpret data structure	Common data formats (JSON, XML), schema compliance
Semantic	Systems understand data meaning	Shared vocabularies, ontologies, identifier schemes
Organizational	Organizations align processes	Governance agreements, data sharing protocols, SLAs
Legal	Legal frameworks enable sharing	NDGO compliance, PDPO safeguards, sector regulations

3.3 Security-by-Design and Zero Trust

3.3.1 Principle Statement

Cloud environments expand the attack surface and eliminate the traditional network perimeter. Security must be embedded in design rather than added as an afterthought, and implicit trust based on network location must be eliminated in favor of continuous verification and least privilege access.

3.3.2 Zero Trust Architecture Requirements

No Implicit Trust: Network location shall not confer trust. All access requests shall be authenticated and authorized regardless of whether they originate from inside or outside traditional network boundaries.

Continuous Verification: Authentication and authorization shall be continuous, not one-time. Context-aware access policies shall evaluate risk signals (device posture, location, behavior) for each access decision.

Least Privilege: Access shall be limited to the minimum necessary for the specific task. Standing privileged access shall be eliminated in favor of just-in-time privilege elevation.

Micro-Segmentation: Networks shall be segmented to limit lateral movement. East-west traffic between services shall be authenticated and encrypted, with deny-by-default network policies.

Assume Breach: Security architecture shall assume that breaches will occur and design for detection, containment, and recovery. Defense-in-depth ensures that compromise of one layer does not enable full system compromise.

3.3.3 Security-by-Design Directives

Secure Defaults: Systems shall be secure by default, requiring explicit action to reduce security controls rather than explicit action to enable them. Configurations shall fail closed, denying access in error conditions.

Defense-in-Depth: Multiple layers of security controls shall be implemented so that failure of one control does not result in complete compromise. Layers include network, identity, application, and data protection controls.

Strong Authentication: Multi-factor authentication shall be mandatory for administrative access and for access to sensitive data (D2 and above). Phishing-resistant MFA (FIDO2/WebAuthn) shall be used for privileged users.

Encryption: Encryption shall be mandatory for data in transit (TLS 1.2+) and for sensitive data at rest (D2 and above). Encryption shall use approved algorithms and government-controlled keys for restricted data.

Continuous Monitoring: Security monitoring shall be continuous, not periodic. SIEM integration, anomaly detection, and automated alerting shall enable rapid detection and response to security events.

3.4 Privacy-by-Design and PDPO Compliance

3.4.1 Principle Statement

Personal data processing must be lawful, transparent, and minimized. Cloud systems shall embed privacy protection in architecture and default configurations, enabling compliance with the Personal Data Protection Ordinance while supporting legitimate government functions.

3.4.2 Privacy Engineering Directives

Data Minimization: Systems shall collect and retain only the personal data necessary for the specified purpose. Excessive data collection shall be prohibited, and retention periods shall be defined and enforced.

Purpose Limitation: Personal data shall be processed only for the purposes for which it was collected or for compatible purposes with appropriate legal basis. Processing for new purposes shall require fresh authorization.

Consent Management: Where consent is the legal basis for processing, systems shall implement granular consent collection, storage, and withdrawal capabilities. Consent records shall be auditable.

Data Subject Rights: Systems shall implement technical capabilities to support data subject rights including access, correction, erasure (where legally permissible), portability, and objection. Response workflows shall meet PDPO timelines.

Retention Controls: Retention policies shall be implemented technically, not just procedurally. Automated data lifecycle management shall ensure that personal data is deleted or anonymized when retention periods expire.

Privacy Impact Assessment: Data Protection Impact Assessments (DPIA) shall be conducted for high-risk processing activities before deployment. DPIAs shall be documented and reviewed by designated privacy officers.

3.4.3 Telemetry and Log Governance

Logs, traces, metrics, and security events may contain personal identifiers and must be governed under PDPO obligations:

Telemetry Classification: Telemetry data shall be classified according to the personal data it contains. Telemetry containing identifiers shall be treated as personal data with appropriate protections.

Log Minimization: Logs shall record the minimum information necessary for operational and security purposes. Personal identifiers shall be pseudonymized or removed where full identifiers are not required.

Log Residency: Logs containing personal data or sensitive operational information shall be stored in accordance with data residency requirements. Cross-border log aggregation shall be evaluated for compliance.

3.5 Resilience and Continuity

3.5.1 Principle Statement

Government services must remain available and recoverable despite failures, disasters, and cyber incidents. Cloud architectures shall be designed for resilience from the outset, with defined recovery objectives and tested continuity procedures.

3.5.2 Implementable Directives

Recovery Objectives: Critical services shall have defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) based on business impact analysis. Architecture and investment shall be aligned to achieve these objectives.

Multi-Zone Deployment: Services requiring high availability shall be deployed across multiple availability zones to survive zone failures. Single points of failure shall be eliminated for critical services.

Disaster Recovery: Disaster recovery capabilities shall be implemented for critical systems, with geographically separated DR sites and tested failover procedures. DR testing shall be conducted at least annually.

Immutable Backups: Backups for critical systems shall be immutable (write-once) to protect against ransomware and malicious deletion. Backup integrity shall be verified through regular restoration testing.

Cyber Recovery: Recovery procedures shall address cyber incidents including ransomware, with isolated recovery environments and validated clean restore points. Cyber recovery exercises shall be conducted regularly.

3.5.3 Service Criticality Tiers

Tier	Description	RTO Target	RPO Target	Availability Target

C0 - Advisory	Non-critical, informational	72 hours	24 hours	95%
C1 - Standard	Business support, operational	24 hours	8 hours	99%
C2 - Important	Citizen services, core operations	4 hours	1 hour	99.5%
C3 - Critical	Essential services, high impact	1 hour	15 minutes	99.9%
C4 - Mission Critical	Life safety, national security	15 minutes	Near-zero	99.99%

3.6 Portability and Exit Readiness

3.6.1 Principle Statement

Lock-in increases cost and risk. Government shall maintain the ability to change cloud providers, migrate between deployment models, and exit cloud arrangements without undue difficulty or cost. Portability requirements shall be embedded in procurement, architecture, and contracts.

3.6.2 Implementable Directives

Open Standards: Systems shall use open standards and avoid proprietary formats, protocols, and APIs where open alternatives exist. Deviation from open standards shall require documented justification and exit planning.

Containerization: Workloads shall be containerized where feasible to enable portability across cloud environments. Container images shall avoid provider-specific dependencies.

Infrastructure as Code: Infrastructure shall be defined through code (Terraform, Pulumi, or equivalent) enabling recreation in alternative environments. IaC templates shall be version-controlled and maintained.

Data Portability: Data export capabilities shall be verified and tested. Data shall be stored in open formats. Egress costs and procedures shall be understood and documented.

Exit Planning: Contracts shall include exit clauses specifying transition assistance, data return, egress cost transparency, and minimum transition periods. Exit plans shall be tested for critical systems.

Skills Independence: Government shall maintain internal skills sufficient to manage cloud operations without complete dependence on vendor support. Critical knowledge shall not be held exclusively by external parties.

3.7 Auditability and Evidence-Based Assurance

3.7.1 Principle Statement

Controls must be demonstrable, not aspirational. Cloud environments shall maintain comprehensive audit trails, configuration baselines, and compliance evidence enabling independent verification of security and governance controls.

3.7.2 Implementable Directives

Tamper-Evident Logging: Audit logs shall be tamper-evident with integrity protection. Administrative actions, data access events, and security-relevant activities shall be logged with sufficient detail for forensic analysis.

Configuration Baselines: Configuration baselines shall be documented and continuously monitored for drift. Deviations from approved configurations shall be detected, alerted, and remediated.

Asset Inventory: Complete inventory of cloud assets shall be maintained, including compute resources, storage, databases, network components, and applications. Shadow IT shall be detected and brought under governance.

Compliance Evidence: Compliance with Policy requirements shall be evidenced through automated collection of configuration data, scan results, and operational metrics. Evidence shall be retained for audit purposes.

Independent Verification: Critical controls shall be subject to independent verification through internal audit, external assessment, or automated compliance monitoring. Self-attestation shall be supplemented by independent review.

3.8 Shared Platforms and Reuse

3.8.1 Principle Statement

Government-wide efficiencies require shared services. Where feasible, ministries shall consume common platforms and shared services rather than building duplicative capabilities, enabling cost efficiency, security consistency, and operational excellence.

3.8.2 Implementable Directives

Shared Platform Priority: Before procuring or building new capabilities, agencies shall evaluate whether existing shared platforms can meet requirements. Duplication of shared service functionality shall require documented justification.

Common Security Services: Identity management, security monitoring, vulnerability scanning, and other security services shall be consumed from shared platforms where available, ensuring consistency and efficiency.

Platform Governance: Shared platforms shall have clear governance including service level commitments, change management, and accountability for platform performance and security.

Tenant Isolation: Shared platforms shall implement appropriate tenant isolation ensuring that data and operations of one agency are not accessible to others without explicit authorization.

3.9 Sustainability (Green Cloud)

3.9.1 Principle Statement

Energy and resource efficiency are national priorities. Cloud adoption shall contribute to environmental sustainability through efficient resource utilization, responsible procurement, and measurable environmental performance.

3.9.2 Implementable Directives

Energy Efficiency Metrics: Data centers and cloud platforms shall track and report Power Usage Effectiveness (PUE) and other energy metrics. Procurement shall favor providers with demonstrated energy efficiency.

Right-Sizing: Workloads shall be right-sized to avoid over-provisioning. Autoscaling shall be implemented to match resource consumption to actual demand, avoiding idle capacity.

Resource Optimization: Regular optimization reviews shall identify opportunities to reduce resource consumption through architecture improvements, workload consolidation, and efficient coding practices.

Lifecycle Management: Hardware lifecycle management shall consider environmental impact. E-waste shall be disposed of responsibly in compliance with environmental regulations.

Sustainability Reporting: Annual sustainability reports shall document cloud environmental performance including energy consumption, carbon emissions, and efficiency improvements.

3.10 Principles Summary Matrix

Principle	Primary Objective	Key Control Domain	Verification Method
Sovereignty	Maintain lawful control	Data residency, key custody	Audit, attestation
Interoperability	Enable integration	APIs, standards, protocols	Conformance testing
Security/Zero Trust	Protect assets	IAM, encryption, monitoring	Continuous assessment
Privacy-by-Design	Protect personal data	Minimization, rights support	DPIA, compliance audit
Resilience	Ensure availability	DR, backup, redundancy	DR testing, SLO monitoring
Portability	Prevent lock-in	Standards, IaC, contracts	Exit testing, review
Auditability	Enable verification	Logging, baselines, evidence	Independent audit
Shared Platforms	Improve efficiency	Service catalogue, governance	Utilization metrics
Sustainability	Environmental responsibility	PUE, optimization, lifecycle	Sustainability reporting

CHAPTER 4: INSTITUTIONAL AND GOVERNANCE FRAMEWORK

4.1 Governance Objectives

Cloud adoption in Government creates shared platforms, shared security boundaries, and shared data processing across ministries, departments, divisions, agencies, statutory bodies, and state-owned enterprises. The distributed nature of cloud computing, combined with the critical importance of government data and services, necessitates a comprehensive governance framework that balances central coordination with operational agility. The governance framework established by this policy shall ensure consistent risk management across all government cloud deployments, applying uniform standards while accommodating sector-specific requirements; enforceable controls that can be monitored, audited, and remediated when deviations occur; interoperability and reuse across Digital Public Infrastructure components, preventing duplication and enabling seamless data exchange; procurement integrity and lock-in avoidance, ensuring competitive markets and government flexibility; and operational resilience and continuous compliance, maintaining service availability while demonstrating adherence to policy requirements.

The governance framework recognizes that cloud computing introduces new shared responsibility models where security, privacy, and operational obligations are distributed between government agencies and cloud service providers. The framework establishes clear accountability boundaries, evidence requirements, and coordination mechanisms to ensure that shared responsibility does not become diffused responsibility where critical obligations fall through gaps.

4.1.1 Cloud Adoption Posture

Bangladesh shall pursue a hybrid, multi-provider approach anchored in sovereign cloud capability. The default posture is:

- Cloud-first for new services: New digital services shall be designed for cloud deployment unless a documented exception is approved.
- Sovereign-by-design: Workloads containing restricted data or constituting critical information infrastructure shall be deployed in accredited sovereign cloud zones (e.g., NDC/BDCCL/Meghna sovereign environments) unless explicitly exempted.
- Modernization over lift-and-shift: Migrations should prioritize refactoring to secure, maintainable architectures; lift-and-shift may be used as an interim step with a defined modernization plan.
- Platformization: Ministries should consume common platform services (PaaS, managed databases, API management, observability) to reduce duplication and security gaps.
- Evidence-based operations: Production workloads shall be operated with defined SLOs, observability, and incident response processes.

4.1.2 Government Cloud Operating Model (Target)

A federated operating model shall be adopted, combining central shared platforms with agency execution:

- Central platform teams provide shared services: identity federation, API gateways, NRDEX core services, logging/SIEM integration, baseline security tooling, and standardized landing zones.
- Agency product teams own service delivery: application lifecycle, data stewardship, and service SLOs.
- Security and privacy assurance functions establish baselines, perform independent review, and coordinate incident response.
- A cloud governance forum (aligned to national data governance bodies) arbitrates exceptions, approves high-risk architectures, and monitors compliance.

4.1.3 Workload Decision Factors

Before selecting a deployment model or provider, each workload shall be assessed against the following factors. Evidence shall be recorded.

- Data classification and sensitivity (including personal data categories, national security constraints, and sectoral secrecy obligations).
- Criticality and availability requirements (SLIs/SLOs, RTO/RPO, citizen impact, and service continuity).
- Interoperability dependencies (NRDEX integration, identity federation, payment integration, registry access).
- Threat model (external threat exposure, insider risk, supply chain risk, multi-tenant isolation risk).
- Latency and connectivity constraints (including rural/remote service delivery and offline requirements).
- Regulatory and audit requirements (including PDPO/NDGO/CSO compliance and sectoral regulator guidance).
- Portability and exit feasibility (data export, API portability, IaC, container images, and contractual exit).
- Cost model (including egress fees, storage growth, observability overhead, support costs, and lifecycle costs).
- Sustainability metrics (energy efficiency, right-sizing potential, and hardware lifecycle).

4.1.4 Corner Cases and Exceptions

The following scenarios frequently cause cloud governance failures. They are explicitly within scope of this policy and must be handled by documented controls:

- SaaS support access and foreign lawful access risk: administrator access by vendor personnel, remote troubleshooting, and third-country subpoenas.
- Telemetry and observability data containing identifiers: logs and traces can constitute personal data or sensitive data.
- Data replication and caching: CDN edge caches, object storage replication, backups, and DR copies may create unintended data transfer.
- Emergency access ('break-glass') accounts and shared admin credentials: must be time-bound, monitored, and audited.
- Service accounts, non-human identities, and API keys: must be governed (rotation, least privilege, secret storage, and logging).
- Legacy COTS (Commercial Off-The-Shelf) licensing and hardware-tied systems: require transition plans; virtualization-only solutions may not be compliant long-term.
- Air-gapped or high-security networks: require specialized patterns for update delivery, artifact signing, and secure data transfer.
- Edge operations under intermittent connectivity: require offline-first designs, delayed synchronization, and conflict resolution.
- Cross-agency multi-tenancy: requires strict tenant isolation, separation of duties, and data access boundaries.

4.1.5 Mandatory Assurance Gates

For workloads above baseline risk thresholds (including restricted data or critical services), the following assurance gates shall be completed before go-live:

- Architecture review against the Government Cloud reference architecture and interoperability requirements.
- Security baseline review, including identity model, network segmentation, encryption and key governance, logging, and DR readiness.
- Privacy engineering review and completion of DPIA where required; confirmation of data retention and rights-handling mechanisms.
- Operational readiness review: SLOs defined, alerting configured, runbooks established, incident response integration tested.
- Exit and portability review: data export procedures, recovery mechanisms, and provider transition plans documented.

4.1.6 Cross-Border Processing and Transfer Controls

Cross-border processing shall be treated as a high-risk event and must be explicitly assessed. Where cross-border transfer is permitted under applicable law, the following minimum controls shall apply:

- Documented lawful basis and data-sharing authorization consistent with PDPO/NDGO; record of processing maintained.
- Contractual controls: defined subprocessor list, audit rights, breach notification obligations, and restrictions on foreign lawful access.
- Technical controls: encryption in transit; encryption at rest where feasible; customer-controlled keys for sensitive data; segregation of support access.
- Operational controls: access logging, anomaly detection, and periodic review of data transfers and replication settings.
- Exit controls: demonstrable deletion on termination, verified backups handling, and data export capability.

4.1.7 Portability, Egress, and Lock-In Avoidance Requirements

- All procurements shall require a documented exit plan and data export procedures in machine-readable formats.
- Workloads shall use portable artifacts where feasible (e.g., container images, standard runtimes, open database engines or export tools).
- Infrastructure shall be described using Infrastructure as Code (IaC) to enable reproducible environments.
- Egress costs and data gravity risks shall be evaluated at design time; architectures should minimize unnecessary data movement.
- For shared DPI services, API specifications and schemas shall be published and versioned to prevent proprietary coupling.

4.2 Institutional Roles and Responsibilities at National Level

The following institutional roles are established or affirmed for the purposes of this Policy. These roles are designed to complement rather than duplicate the statutory authorities created by the National Data Governance Ordinance, 2025, the Personal Data Protection Ordinance, 2025, and the Cyber Safety Ordinance, 2025. The governance structure recognizes the primacy of these legal instruments while providing operational coordination for cloud-specific implementation.

4.2.1 Information and Communication Technology Division

The Information and Communication Technology Division (ICTD), operating under the Ministry of Posts, Telecommunications and Information Technology, serves as the policy owner and national programme sponsor for government cloud adoption. ICTD shall issue and maintain this Policy and associated technical baselines; coordinate budget allocation for government cloud infrastructure and capacity development; mandate adoption timelines and compliance requirements across government; resolve inter-ministerial disputes regarding cloud governance; and represent Bangladesh in international forums on cloud policy and digital infrastructure.

4.2.2 Bangladesh Computer Council

Bangladesh Computer Council (BCC) shall serve as the technical standards steward for government cloud, responsible for developing and maintaining reference architectures and

technical baselines; providing technical audit support and capability assessment; coordinating capability development programmes for government cloud skills; and maintaining the Government Cloud Control Baseline and associated evidence models. BCC shall work to ensure that technical standards are practical, implementable, and aligned with international best practices while meeting Bangladesh's specific requirements.

4.2.3 Bangladesh Data Centre Company Limited

Bangladesh Data Centre Company Limited (BDCCL) shall serve as the primary Government Cloud service operator, providing Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) offerings for government consumption. BDCCL shall operate the Government Cloud service catalogue and marketplace, enabling agencies to discover and consume approved cloud services; provide managed services including landing zones, identity federation, security monitoring integration, and operational support; maintain service level commitments aligned with the service tier framework established in this Policy; and support the migration factory by providing onboarding assistance and technical enablement for agencies transitioning to Government Cloud.

4.2.4 National Data Center

The National Data Center (NDC) shall serve as the primary Cloud Governance and Implementation Authority for the Government of Bangladesh. In addition to its role as a sovereign hosting facility, the NDC shall:

- **Exercise Regulatory Oversight:** Establish and maintain the Government Cloud Technical Baseline, manage the National Cloud Provider Registry (NCPR), and issue accreditation to cloud service providers.
- **Manage the Migration Pipeline:** Maintain the authoritative government workload inventory and coordinate migration waves across ministries.
- **Monitor Compliance:** Operate the National Cloud Assurance Dashboard (NCAD) and enforce remediation of non-compliant agencies or providers.
- **Arbitrate Disputes:** Serve as the first point of resolution for inter-agency cloud governance disputes before escalation to the ICT Division.

NDC, operating under Bangladesh Computer Council, shall provide sovereign hosting for the highest sensitivity and criticality workloads. NDC shall host D4 (National Critical) and D3 (Restricted) workloads requiring the strongest sovereignty controls; provide sovereign control plane integration points for hybrid and multi-cloud architectures; maintain the highest security standards including physical security, personnel security, and operational security controls appropriate for Critical Information Infrastructure; and support disaster recovery requirements for critical government systems through geographically separated backup facilities.

4.2.7 National Cybersecurity Agency

The National Cybersecurity Agency (NCSA), established under the Cyber Safety Ordinance, 2025, shall exercise its statutory functions in relation to government cloud security. NCSA responsibilities relevant to this Policy include designating Critical Information Infrastructure and imposing associated security obligations; operating the National Security Operations Center (NSOC) and coordinating threat intelligence sharing; establishing security assessment and audit requirements for CII-designated cloud systems; coordinating incident response for

significant security incidents affecting government cloud infrastructure; and maintaining the national vulnerability disclosure and coordination programme.

4.2.8 National Data Governance Authority

The National Data Governance Authority (NDGA), established under the National Data Governance Ordinance, 2025, shall exercise its statutory functions in relation to government data in cloud environments. NDGA responsibilities relevant to this Policy include establishing and maintaining the Bangladesh National Data Governance and Interoperability Architecture (BNDIA); defining data classification standards and ensuring consistent application across government; coordinating the National Responsible Data Exchange (NRDEX) platform and associated API standards; and overseeing Chief Data Officers at institutional levels to ensure data governance compliance.

4.3 Institutional Roles at Agency Level

4.3.1 System Owner

Each government system deployed to cloud shall have a designated System Owner who is accountable for all aspects of the system's governance, security, and operational performance. The System Owner shall ensure that the system is classified according to data sensitivity (D0-D4) and service criticality (C0-C4) frameworks; approve workload placement decisions and ensure alignment with residency requirements; ensure that appropriate security controls are implemented and maintained; authorize access to the system and ensure periodic access reviews are conducted; ensure that the system meets its Service Level Objectives and operational requirements; and maintain accountability for compliance with this Policy and associated legal requirements.

4.3.2 Chief Data Officer

As mandated by the National Data Governance Ordinance, 2025, each significant government entity shall designate a Chief Data Officer (CDO) responsible for data governance within the organization. In relation to cloud deployments, the CDO shall ensure that data classification is applied consistently across cloud workloads; oversee data sharing arrangements and ensure compliance with NRDEX protocols; ensure that personal data processing in cloud environments complies with PDPO requirements; maintain data inventories and lineage documentation for cloud-hosted data assets; and coordinate with NDC on data-related aspects of cloud migration and operation.

4.3.3 Chief Information Security Officer

Each significant government entity shall designate a Chief Information Security Officer (CISO) or equivalent role responsible for information security. In relation to cloud deployments, the CISO shall ensure that security baselines are implemented across all cloud workloads; coordinate with NCSA on security assessments, vulnerability management, and incident response; ensure that security monitoring and logging requirements are met; oversee security aspects of cloud procurement and vendor management; and maintain the agency's security posture documentation and risk register for cloud systems.

4.4 RACI Model for Government Cloud

The following Responsible, Accountable, Consulted, Informed (RACI) matrix summarizes the distribution of responsibilities across key governance functions. R indicates the party responsible for performing the work, A indicates the party accountable for the outcome, C indicates parties that must be consulted, and I indicates parties that must be informed.

Table 4.1: Government Cloud RACI Matrix

Function	NDC	NDC	Agency	BDCCL/NDC	NCSA	PDPO/NDGO
Workload Classification	A	R	R	C	C	C
Landing Zone Build	C	R	C	R	C	C
IAM Federation and PAM	C	R	R	R	C	C
Security Monitoring (SIEM/SOC)	C	C	C	R	A/R	C
Privacy Impact Assessment	C	C	A/R	C	C	A/R
Incident Response Coordination	C	C	R	R	A/R	C
Supplier Due Diligence	A	R	R	C	C	C
Audit and Compliance Reporting	A	R	R	R	C	C

4.5 Accreditation and Conformance Framework

Any Cloud Service Provider (CSP) or operator supporting Government workloads shall be accredited against the Government Cloud Control Baseline. Accreditation ensures that providers meet minimum security, privacy, and operational standards before being permitted to process government data. The accreditation framework operates at multiple tiers corresponding to the sensitivity and criticality of workloads the provider may support.

4.5.1 National Cloud Provider Registry

A National Cloud Provider Registry (NCPR) shall be maintained under the national cloud governance structure, containing accredited sovereign providers including NDC service scope, BDCCL Government Cloud scope, and accredited Meghna Cloud scope where applicable; accredited private and public cloud providers approved for specific workload classes; approved service catalogues, regions and locations, and sub-processor lists for each provider; accredited service tiers and supported security capabilities including KMS/HSM, BYOK/HYOK, logging export, and private connectivity; and validity periods, renewal dates, and audit evidence references demonstrating ongoing compliance.

4.5.2 Accreditation Tiers

Accreditation shall be tiered to match risk profiles of different workload categories. Accreditation Tier A (Baseline) qualifies providers for D0-D2 and C0-C2 workloads, requiring demonstration of baseline security controls, standard audit compliance, and operational maturity. Accreditation Tier B (High) qualifies providers for D3 and C3 workloads, subject to sovereignty and key control requirements including domestic hosting, customer-controlled encryption keys, and enhanced incident reporting. Accreditation Tier C (CII) qualifies providers for D4 and C4 workloads, requiring the strongest controls, tested disaster recovery exercises, heightened audit rights, and integration with National Security Operations Center.

Accreditation shall be conditional on submission of comprehensive evidence packages documenting control implementation; independent audits and/or government-led assessments

validating control effectiveness; demonstrated ability to enforce residency and key custody controls through technical and contractual means; and verified incident response integration demonstrating timely reporting and coordination capabilities.

4.6 Multi-Tenant Shared Platforms and Separation of Duty

Where shared platforms are used across multiple agencies through multi-tenancy arrangements, the operator shall implement strict tenant isolation ensuring that one tenant cannot access another tenant's data or resources; separation of duty preventing any single administrator from having unrestricted access across tenants; and auditable administrative boundaries with comprehensive logging of all cross-tenant administrative actions. NDC shall approve tenancy models for platforms that process D3/D4 data or support C3/C4 critical services, ensuring that isolation mechanisms are appropriate for the risk level.

Specific requirements for multi-tenant platforms include separate identity boundaries and administrative roles per tenant with prohibition of shared administrator accounts; isolated network segments with micro-segmentation for east-west traffic control between tenant workloads; tenant-specific encryption keys managed through separate key hierarchies where feasible; and comprehensive audit logging capturing all administrative actions with tenant attribution.

4.7 Compliance Layers and Accountability

Compliance with this Policy shall be implemented through four mutually reinforcing layers. Policy compliance encompasses adherence to this Policy and associated technical baselines, mandatory for all ministries, agencies, and their suppliers. Legal compliance ensures adherence to PDPO, NDGO, CSO, and sectoral legal instruments which apply as higher-order requirements and take precedence where conflicts arise. Technical compliance demonstrates adherence to mandatory baselines including the Government Cloud Control Framework (G-CCF) and Government Cloud Technical Baseline (GCTB). Operational compliance provides evidence through logs, attestations, reports, scans, disaster recovery test outputs, audit artifacts, and service health metrics.

Accountability shall follow the shared responsibility model appropriate to cloud computing. Government entities remain accountable for governance decisions, risk acceptance, and lawful processing decisions regardless of where workloads are hosted. Providers are accountable for the controls within their service boundary and for producing evidence demonstrating compliance. Joint accountability exists for incident coordination, audit support, and exit execution where both parties must cooperate to achieve required outcomes.

CHAPTER 5: DATA CLASSIFICATION, SOVEREIGNTY, AND RESIDENCY

5.1 Data Classification Framework

Data classification provides the foundation for all governance decisions regarding workload placement, security controls, access management, and cross-border processing. Consistent application of data classification enables proportionate controls that protect sensitive data while avoiding unnecessary restrictions on lower-risk information. All Government systems shall classify data at creation and at ingestion into platforms using the framework established in this section. NDC may issue supplemental guidance and sector-specific examples to support consistent classification across government.

5.2 Data Classification Categories

Table 5.1: Data Classification Framework

Class	Description	Examples	Minimum Controls	Residency
D0 Open	Public data; no personal data	Statistics, public notices	Integrity; provenance	Any location
D1 Internal	Operational, not public	Internal memos, metrics	IAM; TLS; logging	Prefer BD
D2 Confidential	Sensitive govt/personal data	Citizen accounts, cases	Strong IAM; encryption; DPIA	BD only
D3 Restricted	Highly sensitive, regulated	Health, tax, biometric	HSM/KMS; PAM; SIEM	Sovereign only
D4 National Critical	CII, national security	National registries, CII	HYOK; 24/7 SOC; isolation	NDC mandatory

D0 Open Data comprises information explicitly approved for public release containing no personal or confidential content, including published statistics, public notices, and open datasets. D1 Internal Data comprises operational information not intended for public release but with limited sensitivity, including internal memoranda and routine administrative records. D2 Confidential Data comprises sensitive government information and ordinary personal data requiring controlled access, including service delivery records and citizen accounts. D3 Restricted Data comprises highly sensitive personal data, regulated sector data, and information affecting public safety, including health records, tax records, and biometric-linked identity data. D4 National Critical Data comprises Critical Information Infrastructure data and national security adjacent information, including national registries, payments switching systems, and emergency services coordination data. Data designated as Critical Information Infrastructure (CII) under Section 15 of the Cyber Safety Ordinance, 2025, or classified as 'Restricted' under PDPO but designated as 'Critical' by the National Security Operations Center (NSOC). For the purposes of PDPO compliance, both D3 (Restricted) and D4 (National Critical) shall be treated as 'Restricted Personal Data' under Section 29 of the Personal Data Protection Ordinance, 2025. The distinction between D3 and D4 in this policy is solely for determining hosting location (Sovereign Cloud vs. National Data Center).

5.3 Workload Placement Rules

Placement rules determine where government workloads may be hosted based on their data classification. These rules apply to production environments and non-production environments containing real data including backups, logs, and telemetry.

Table 5.2: Workload Placement Matrix

Category	Sovereign G-Cloud	Accredited Cloud	Public Cloud	On-Premises
D0 Open	Permitted	Permitted	Permitted	Permitted
D1 Internal	Permitted	Permitted	With controls	Permitted
D2 Confidential	Preferred	Permitted only if Hold Your Own Key (HYOK) encryption is implemented where the provider has no access to decryption keys.	Exception only	With controls
D3 Restricted	Mandatory default	If sovereign equivalent	Prohibited	With equivalent
D4 Critical	Mandatory	Not permitted	Prohibited	Air-gapped only

D3 and D4 workloads shall be hosted in Sovereign Cloud Zones unless written exemption is granted. D2 workloads may be hosted in accredited public cloud only if data residency, access controls, and auditability are contractually and technically enforced. Encryption in transit using TLS 1.2 or higher shall be mandatory for all workloads. Encryption at rest using AES-256 or equivalent shall be mandatory for D2 and above. Customer-controlled keys through BYOK or HYOK shall be required for D3 and D4 data with KMS/HSM services under Bangladesh jurisdiction.

5.4 Residency Scope and Requirements

Residency requirements apply to all derivative artifacts including database replicas and read replicas, object storage replication and versioning copies, backups and snapshots, log aggregation stores including SIEM data and APM datasets, support dumps and diagnostic artifacts, and CDN edge caching. For D2 through D4 data, all such artifacts shall be kept within Bangladesh jurisdiction unless explicitly authorized.

5.5 Encryption Key Sovereignty

For D2 through D4 data, encryption keys shall be managed in Bangladesh-resident KMS or HSM. For D3 and D4 data, BYOK or HYOK arrangements shall be used where feasible so providers cannot decrypt data without Government authorization. Key management practices shall include defined rotation schedules, revocation mechanisms, separation of duties between key administrators and data users, and comprehensive audit logging of all key operations.

5.6 Cross-Border Processing Exceptions

Cross-border processing for D1 and D2 may be permitted only via explicit exception approved by NDC and relevant authorities. D3 and D4 cross-border processing is prohibited without exception. Exception requests shall identify all data flows including sub-processors and support access locations, require strong encryption with Bangladesh-controlled keys, define time-bound exception periods with migration plans, and document risk assessments covering legal risk, foreign lawful access risk, and supplier controls.

5.7 Data Retention and Secure Deletion

Retention periods shall be defined by law, operational needs, and service requirements. Providers shall support secure deletion and media sanitization consistent with documented standards. For object storage and backups, deletion must include versioned copies and immutable vault retention logic. For D3 (Restricted) and D4 (National Critical) data subject to

statutory retention periods, storage systems must utilize Write Once, Read Many (WORM) technology to prevent modification or deletion before the retention period expires. Deletion events shall be logged as auditable records demonstrating compliance.

5.8 Data Mapping and Lineage

Agencies shall maintain data maps identifying where personal and sensitive data flows, how it is transformed, and which parties access it. For C2 and higher criticality services, lineage and provenance records shall be maintained including ingestion sources, transformations, and exchange events. Metadata management shall include dataset identifiers, versions, quality signals, and lineage graphs. For NRDEX exchanges, records shall capture purpose, recipient, API contract version, and re-sharing permissions.

CHAPTER 6: CLOUD SECURITY BASELINE AND ASSURANCE REQUIREMENTS

6.1 Security Baseline Objectives

The Government Cloud Security Baseline establishes the minimum mandatory security controls that all government cloud deployments must implement regardless of hosting location or provider. The baseline implements defense-in-depth principles where multiple overlapping controls protect against different threat vectors, and Zero Trust Architecture principles where no user, device, or network segment is implicitly trusted. Security requirements are embedded from initial design through operations, ensuring that protection is not an afterthought but a foundational element of all cloud deployments.

The security baseline aligns with international standards including ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, and NIST Cybersecurity Framework while incorporating Bangladesh-specific requirements from the Cyber Safety Ordinance, 2025, and associated regulations. The baseline provides a common foundation that enables consistent security posture assessment, comparable audit evidence, and coordinated incident response across government cloud environments.

6.2 Zero Trust Architecture Requirements

Government cloud environments shall implement Zero Trust Architecture (ZTA) principles requiring explicit verification of every access request regardless of network location or previous authentication status. Trust is never implicit and must be continuously earned through demonstrated compliance with security policies. Key ZTA requirements include authenticating and authorizing every request for both user-to-application and service-to-service interactions; enforcing mutual TLS (mTLS) for internal service communications for C2 and higher criticality workloads; applying continuous policy evaluation including context-aware access and risk-based conditional access controls; and adopting micro-segmentation with deny-by-default network policies that limit lateral movement.

6.3 Identity and Access Management

Identity and Access Management (IAM) controls shall be implemented consistently across sovereign and accredited cloud environments. Requirements include federated identity using SAML 2.0 or OpenID Connect (OIDC) standards with central directory integration and lifecycle management for joiner, mover, and leaver processes. Multi-Factor Authentication (MFA) shall be required for all administrative actions and for access to D2 and higher classified data. Phishing-resistant MFA using FIDO2 or WebAuthn shall be required for privileged users and C3/C4 criticality workloads where feasible.

Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) shall be implemented for fine-grained authorization with periodic access reviews at least quarterly for privileged access and annually for standard access. Privileged Access Management (PAM) shall be implemented with just-in-time elevation, session recording for high-risk actions, and break-glass accounts with strict controls including dual authorization and comprehensive audit logging. Service accounts and machine identities shall use short-lived credentials, workload identity federation where available, and secrets shall never be stored in source code or configuration files.

6.4 Network Security

Network security controls shall implement defense-in-depth from the perimeter to individual workloads. Ingress controls shall include Web Application Firewall (WAF) for all public endpoints, DDoS protection services, rate limiting to prevent abuse, bot mitigation, and API gateway enforcement for all external APIs with authentication, authorization, and schema validation. Egress controls shall include outbound allow-listing for C2 and higher criticality workloads, DNS filtering to prevent command and control communications, egress proxying where appropriate, and continuous monitoring for data exfiltration patterns.

Network segmentation shall separate management plane, data plane, and application plane networks with appropriate access controls between segments. Tenant networks shall be isolated for shared platforms to prevent cross-tenant access. Secure remote administration shall require bastion hosts or equivalent jump servers with no direct exposure of management interfaces to the Internet. All management access shall be logged and subject to PAM controls. For all government usage of external SaaS applications, a Cloud Access Security Broker (CASB) solution must be deployed to enforce DLP policies, detect Shadow IT usage, and ensure consistent access controls across unmanaged devices.

6.5 Compute, Virtualization, and Container Security

Compute security requirements apply to virtual machines, containers, and serverless workloads. Hardened images shall be used as the foundation for all deployments, with golden images maintained using CIS-aligned baselines and subject to continuous patching. Image provenance and signing shall be enforced to ensure that only authorized images are deployed. Secure boot and attestation shall be implemented for sensitive workloads, with hardware-backed root of trust where available.

Container security shall include runtime hardening, least privilege containers running as non-root where feasible, admission controls that prevent deployment of non-compliant containers, and scanning of images for vulnerabilities before deployment. Isolation requirements shall separate production and non-production environments, restrict administrative access to hypervisors and hosts, and implement controls to defend against container escape and hypervisor attack classes. Confidential computing using trusted execution environments shall be considered for D3 and D4 workloads where feasible to reduce insider and hypervisor risk.

6.6 DevSecOps and Secure Software Supply Chain

All Government software deployed to cloud, including platform configurations expressed as code, shall follow DevSecOps practices. CI/CD pipelines shall be protected with least privilege runners, signed artifacts, protected branches, mandatory code reviews, and immutable build logs. Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), and Software Composition Analysis (SCA) shall be integrated into pipelines for C1 and higher criticality services.

Software Bill of Materials (SBOM) shall be generated for C2 and higher criticality services, maintaining component inventories and tracking vulnerability exposure. Artifact signing and verification shall be implemented for containers, packages, and Infrastructure as Code modules. Secrets scanning shall prevent accidental exposure of credentials in source code. Build environments shall be isolated with restricted access to build secrets and comprehensive logging of build provenance.

6.7 Baseline Cloud Controls Catalogue

Table 6.1: Baseline Cloud Control Domains

Domain	Control Requirements	Evidence Examples
Governance and ISMS	Risk management, control implementation, ISO 27001 alignment	SoA, risk register, audit reports
IAM and PAM	MFA, RBAC/ABAC, JIT access, federation	Access reviews, PAM logs, policies
Network Security	Segmentation, WAF, ingress/egress controls	WAF configs, flow logs, firewall rules
Cryptography and Keys	TLS 1.2+, AES-256, HSM/KMS, BYOK/HYOK	KMS logs, HSM attestations, rotation records
Logging and Audit	Tamper-evident logs, centralized SIEM	SIEM exports, retention proof, integrity hashes
Resilience and DR	Tested DR, immutable backups, RTO/RPO	DR drill reports, restore tests, availability metrics
Supply Chain	SBOM, signed builds, SAST/DAST/SCA	SBOMs, signing attestations, scan results

6.8 Security Monitoring and Incident Response

Security monitoring shall provide continuous visibility into cloud environments through centralized logging aggregating identity, network, compute, storage, and application layer events. Security Information and Event Management (SIEM) integration shall enable correlation, alerting, and threat detection. For CII-designated systems, integration with the National Security Operations Center (NSOC) shall be mandatory as specified under the Cyber Safety Ordinance.

Incident response capabilities shall include documented runbooks for common incident types, defined escalation paths, and forensic readiness with preserved evidence chain of custody. Incident classification shall follow P1 through P4 severity levels with defined response timelines. P1 incidents involving active exploitation, widespread outage, or confirmed breach require immediate escalation and joint incident response. P2 incidents involving major degradation or contained security incidents require acknowledgement within one hour and mitigation plan within eight hours. P3 (Minor) incidents involving localized degradation, non-critical bugs, or near-miss security events require acknowledgement within four business hours and resolution within three business days. P4 (Low) incidents involving cosmetic issues, information requests, or minor non-blocking errors require acknowledgement within 24 hours and resolution in accordance with the next scheduled maintenance window or release cycle.

6.9 Vulnerability Management

Vulnerability management shall implement continuous scanning, risk-based prioritization, and timely remediation. Critical vulnerabilities (CVSS 9.0+) in internet-facing systems shall be remediated within 7 days. High vulnerabilities (CVSS 7.0-8.9) shall be remediated within 30 days. Medium and low vulnerabilities shall be remediated according to documented schedules based on exposure and exploitability. Penetration testing shall be conducted annually for C2 and higher criticality services and after significant architectural changes.

6.10 Privacy Engineering Controls

Privacy engineering controls shall implement PDPO requirements through technical mechanisms. Data Protection Impact Assessments (DPIAs) shall be conducted for processing activities presenting high risks including profiling, biometric processing, cross-agency data linkage, and D3/D4 data processing. Data minimization shall be enforced in schemas, logging configurations, and backup procedures. Consent management shall capture, store, and enforce consent preferences with full audit trails.

Technical mechanisms shall enable data subject rights including automated access request responses, data export in portable formats, correction propagation across systems per PDPO Section 14, and erasure verification. Pseudonymization and anonymization techniques shall be applied where feasible. Personal data shall be prohibited from storage on blockchain or other immutable ledgers; only hashes or access-controlled references shall be stored where transaction capability is required.

6.11 Assurance and Audit Requirements

Providers supporting government workloads shall provide assurance artifacts including independent audit reports with clear scope coverage, architecture and threat model documentation showing trust boundaries and data flows, penetration test summaries with remediation evidence, vulnerability management metrics and patch compliance reporting, software supply chain evidence including SBOMs and signed artifacts, disaster recovery testing evidence with corrective action tracking, and operational runbooks and incident response playbooks.

Continuous compliance mechanisms shall include Cloud Security Posture Management (CSPM) for configuration drift detection, policy enforcement for identity, network, encryption, logging, and backups, automated evidence collection including configuration snapshots and scan outputs, periodic access reviews, and Service Level Objective dashboards for C3/C4 services with monthly reporting to NDC.

6.12 Minimum Technical Specifications

The following minimum technical specifications shall be included in procurement requirements for cloud services.

- For IAM and PAM: MFA for privileged and remote access with phishing-resistant MFA for C3/C4 where feasible; OIDC/SAML federation with conditional access policies and session lifetime controls; PAM with approval workflows and session recording for high-risk actions.
- For Network: public ingress only via approved gateways with WAF for internet-facing applications; controlled egress gateway with DNS controls and flow logging; separation of production and non-production with tenant isolation for shared platforms.
- For Observability: centralized logs, metrics, and traces with correlation identifiers; immutable audit logs for C2 and higher with retention baselines per criticality tier.
- For Backup and DR: encrypted and immutable backups for C2 and higher; restore tests and failover drills as specified in service tier requirements.
- For DevSecOps: SAST/DAST/SCA in CI/CD pipelines; secrets scanning; SBOM generation and signed artifacts for critical services.

CHAPTER 7: PRIVACY ENGINEERING AND PDPO COMPLIANCE IN CLOUD

7.1 Privacy Engineering Objectives

Privacy engineering ensures that personal data protection requirements established by the Personal Data Protection Ordinance, 2025 are implemented through technical controls embedded in cloud systems from design through operations. Rather than treating privacy as an afterthought or compliance checkbox, privacy engineering integrates data protection into the architecture, development practices, and operational procedures of cloud-hosted government services. This approach reduces the risk of data breaches, supports citizen trust, and ensures that government cloud deployments meet their legal obligations under PDPO.

The privacy engineering framework established by this Policy recognizes that cloud computing introduces both opportunities and challenges for personal data protection. Cloud platforms offer advanced security controls, encryption capabilities, and access management features that can enhance privacy protection when properly configured. However, cloud deployments also create risks from multi-tenancy, cross-border data flows, automated data processing, and complex supply chains that must be carefully managed.

7.2 Roles and Responsibilities Under PDPO

7.2.1 Data Fiduciary

Government agencies are typically the Data Fiduciaries (data controllers) for citizen-facing digital services. As Data Fiduciaries, agencies determine the purposes and means of processing personal data and bear primary accountability for ensuring that processing complies with PDPO requirements. This accountability is not transferred when personal data is processed in cloud environments; the agency remains responsible for ensuring that cloud deployments meet all applicable privacy requirements.

7.2.2 Data Processor

Cloud providers and managed service providers generally act as Data Processors when processing personal data on documented instructions from the Data Fiduciary. The relationship between Data Fiduciary and Data Processor shall be governed by contracts specifying processing purposes and scope, security measures required, sub-processing restrictions and approval requirements, breach notification obligations and timelines, data retention and deletion requirements, and audit rights and evidence provision obligations.

7.2.3 Significant Data Fiduciary

For systems meeting PDPO thresholds for Significant Data Fiduciary status based on volume of data processed, sensitivity of data categories, or risk to data subjects, enhanced governance and accountability measures shall apply. Significant Data Fiduciaries must appoint a Chief Data Officer as required under PDPO Section 23, conduct mandatory Data Protection Impact Assessments for high-risk processing, implement enhanced security measures proportionate to risk, and maintain comprehensive records of processing activities.

7.3 Privacy by Design Requirements

All government cloud deployments processing personal data shall implement Privacy by Design principles as mandatory controls, not optional enhancements. Privacy by Design ensures that privacy protection is embedded into systems from the earliest design stages rather than retrofitted after deployment.

7.3.1 Data Minimization

Data minimization requires collecting and processing only the minimum personal data necessary for the defined service outcome. Implementation requirements include designing schemas that capture only necessary fields, avoiding over-collection in forms and user interfaces; configuring logging and telemetry to exclude unnecessary personal identifiers or to pseudonymize identifiers where operationally feasible; implementing retention controls that delete or anonymize personal data when no longer required for the processing purpose; and minimizing personal data in backups and replicas through selective backup strategies or automated data lifecycle management.

7.3.2 Purpose Limitation

Purpose limitation requires that personal data is processed only for the specific purposes communicated to data subjects and authorized under law. Technical enforcement shall include attribute-based access controls (ABAC) that restrict data access based on purpose attributes, API scope policies that limit data fields returned based on the requesting application's authorized purposes, audit logging that captures the stated purpose for each data access to enable compliance verification, and technical barriers preventing repurposing of personal data without appropriate authorization.

7.3.3 Privacy by Default

Privacy by Default requires that systems default to the most privacy-protective settings without requiring user action. Implementation requirements include disabling unnecessary telemetry collection by default, masking or hashing personal identifiers in logs unless explicit justification exists for full capture, avoiding storage of sensitive content in Application Performance Monitoring (APM) traces, and implementing the principle of least privilege for all data access with explicit authorization required for expanded access.

7.3.4 Pseudonymization and Anonymization

Pseudonymization replaces direct identifiers with pseudonyms to reduce re-identification risk while maintaining data utility. Anonymization removes the ability to identify individuals from datasets. Requirements include pseudonymization for analytics and testing environments with strict segregation from production personal data, anonymization or aggregation for public release of datasets with verification that re-identification is not feasible, and documented assessment of re-identification risk for any pseudonymized or anonymized datasets.

7.4 Data Subject Rights Enablement

Systems processing personal data shall implement operational workflows and technical mechanisms to support data subject rights under PDPO. Rights requests shall be processed within the timelines specified by PDPO and shall be logged for audit and accountability purposes.

Table 7.1: Data Subject Rights Technical Implementation

Right	PDPO Section	Technical Implementation
Right to Access	Section 10	Secure self-service portal; identity verification; audit logging of access requests
Right to Data Portability	Section 11	Export in structured formats (JSON, CSV); machine-readable; NRDEX integration
Right to Correction	Section 12	Correction workflows; system-wide propagation; audit trail maintenance
Right to Erasure	Section 12	Secure deletion; backup purging; deletion verification certificates
Right to Withdraw Consent	Section 13	Consent revocation mechanisms; processing cessation; downstream notification
System-wide Propagation	Section 14	Event-driven sync; API notifications; verification across replicas and backups

7.4.1 System-Wide Propagation

PDPO Section 14 requires that updates, corrections, or erasures of personal data must be propagated across all systems where the data is stored. This requirement has significant technical implications for cloud deployments where data may be replicated across multiple databases, cached in various locations, and backed up to archive storage. Implementation shall include event-driven architectures that propagate changes to all downstream systems, synchronization mechanisms that ensure consistency across replicas and caches, deletion verification procedures that confirm erasure across all storage locations including backups and archives, and audit trails documenting propagation completion with timestamps and affected systems. Implementation shall utilize Change Data Capture (CDC) mechanisms to detect row-level changes in primary registries and stream update events to dependent systems in near-real-time, ensuring consistency without heavy batch processing.

7.5 Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) shall be conducted for any new or materially changed system that presents high risks to the rights and freedoms of data subjects. DPIA triggers include processing of D3 or D4 classified data, use of profiling or automated decision-making affecting individuals, processing of biometric identifiers for identification purposes, integration of multiple datasets through NRDEX creating comprehensive profiles, large-scale processing of sensitive personal data as defined in PDPO Section 6, and systematic monitoring of publicly accessible areas.

DPIA outputs shall include documented assessment of necessity and proportionality, identification of risks to data subject rights, specification of mitigations and residual risk acceptance with appropriate sign-off authority, and ongoing monitoring plans to verify that controls remain effective.

7.6 Consent Management

Where consent is the lawful basis for processing, systems shall implement consent management capabilities that capture consent with clear documentation of what was consented to and when, store consent records with auditability and tamper-evidence, enforce consent by technical means preventing processing where valid consent is not recorded, enable withdrawal by providing accessible mechanisms for data subjects to withdraw consent, and provide notices in Bangla and accessible formats appropriate for the service population.

7.7 Privacy Controls for NRDEX and Blockchain Integration

Where the National Responsible Data Exchange (NRDEX) is used for data sharing between agencies, privacy controls shall ensure that sharing occurs via documented API contracts with minimized payloads containing only data elements necessary for the specified purpose, explicit purpose constraints enforced through API scopes and access controls, and audit logging capturing purpose, recipient, API contract version, and re-sharing permissions. Where blockchain or distributed ledger capabilities are used for transaction integrity or audit trails, personally identifiable information shall not be stored on-chain unless explicitly authorized. Instead, only hashes, cryptographic commitments, or references to off-chain records with controlled access shall be stored on immutable ledgers.

7.8 Breach Handling and Notification

Personal data breaches shall be handled in coordination with both PDPO breach notification requirements and Cyber Safety Ordinance incident reporting obligations. Requirements include rapid detection and classification of incidents using SIEM/SOAR capabilities with defined runbooks, evidence preservation maintaining chain of custody for investigation and potential legal proceedings, notification to the competent authority within the timelines specified by PDPO for confirmed personal data breaches, notification to affected data subjects where required providing clear guidance on protective measures, remediation planning addressing root causes and preventing recurrence, and post-incident review documenting lessons learned and control improvements.

7.9 Privacy-Enhancing Technologies

Government cloud deployments should consider and implement Privacy-Enhancing Technologies (PETs) where appropriate to minimize privacy risks while maintaining data utility. Applicable technologies include tokenization or format-preserving encryption for identifiers where operational access to actual values is not required, differential privacy or aggregation thresholds for public releases of statistical datasets, secure multi-party computation or federated analytics for cross-agency analytics where raw data sharing is not necessary, and homomorphic encryption for specific use cases where processing of encrypted data is feasible. Encryption and access isolation shall be implemented as the default baseline for all personal data processing in cloud environments.

CHAPTER 8: IMPLEMENTATION ROADMAP AND MIGRATION FRAMEWORK

8.1 Implementation Objectives

The implementation roadmap establishes a phased approach to achieving the vision and objectives of this Policy over a five-year period from 2026 to 2030. The roadmap is designed to stand up a secure, compliant, and interoperable Government Cloud capability using sovereign assets including the National Data Center and sovereign cloud operators such as BDCCL Government Cloud and accredited domestic providers; deliver repeatable onboarding, migration, and assurance processes through a cloud factory model that reduces time-to-live and variability across ministries; operationalize Digital Public Infrastructure enablement through BNDA/NSB integration, NRDEX-ready data exchange patterns, and national trust and transaction capabilities; embed security, privacy, and resilience controls as default guardrails with policy-as-code where feasible and continuous compliance reporting; and implement FinOps and Green ICT practices to ensure affordability, predictability, and measurable sustainability outcomes.

8.2 Implementation Workstreams

Implementation shall be organized across seven workstreams that operate in parallel, with defined dependencies and coordination mechanisms. Workstream 1 (Governance and Assurance) encompasses provider accreditation, audit and compliance reporting, and exception handling. Workstream 2 (Platform Foundations) covers landing zones, network segmentation, IAM/PAM, KMS/HSM, observability stack, and CMDB. Workstream 3 (Interoperability and DPI Enablement) addresses BNDA/NSB integration, API governance, NRDEX patterns, TPS Exchange, and Blockchain RPC services. Workstream 4 (Migration Factory) handles inventory, categorization, 6R playbooks, cutover patterns, and disaster recovery drills. Workstream 5 (Security Operations) covers SOC integration, SIEM/SOAR deployment, vulnerability management, and incident response exercises. Workstream 6 (People and Change) encompasses role-based training, certification programmes, change management, and adoption support. Workstream 7 (FinOps and Green ICT) addresses tagging standards, chargeback mechanisms, cost controls, capacity planning, and sustainability metrics. The NDC shall establish a dedicated FinOps Unit responsible for centralized cloud billing, reserved instance planning, and detecting cost anomalies across all government tenants.

8.3 Phased National Roadmap

Table 8.1: Implementation Phase Overview

Phase	Timeline	Primary Outcomes
Phase 0: Mobilize	0-3 months	Establish governance, inventory baseline, immediate guardrails
Phase 1: Foundation	3-9 months	Landing zones, identity federation, logging, accreditation v1, first pilots
Phase 2: Scale	9-24 months	Migration waves, shared services, NRDEX-ready exchange patterns
Phase 3: Optimize	24-48 months	Reliability/SRE maturity, automation, cost and sustainability optimization
Phase 4: Mature and Innovate	48-60 months	Advanced trust services, confidential computing, PQC readiness

8.3.1 Phase 0: Mobilize (Months 0-3)

The Mobilize phase establishes the governance foundation and immediate guardrails necessary for controlled cloud adoption. Key deliverables include publication of initial accreditation requirements and waiver registry, completion of baseline workload inventory across priority ministries, and deployment of immediate security guardrails for any existing cloud deployments.

8.3.2 Phase 1: Foundation (Months 3-9)

The Foundation phase builds the technical platform capabilities and validates approaches through initial pilots. Key deliverables include operational landing zones for NDC and BDCCL with IAM federation, KMS/HSM integration, WAF/DDoS protection, and observability stack; completion of Accreditation v1 with controls evidence reviewed and audit rights contractually secured; first pilot workloads live with agreed SLOs, tested RPO/RTO, completed DPIAs where required, and operational monitoring dashboards; and initial BNDA/NSB integration blueprint and API gateway standards.

8.3.3 Phase 2: Scale (Months 9-24)

The Scale phase executes migration waves across ministries and operationalizes shared services. Key deliverables include migration waves across priority sectors following the sequencing logic; NRDEX-ready data exchange patterns with schema governance and event-driven architecture; continuous compliance dashboards and sector-specific playbooks; standard PaaS offerings and multi-region disaster recovery patterns; and chargeback mechanisms for shared services with energy reporting.

8.3.4 Phase 3: Optimize (Months 24-48)

The Optimize phase focuses on reliability engineering, automation, and efficiency improvements. Key deliverables include mature Site Reliability Engineering practices with auto-remediation capabilities; capacity optimization and reserved capacity strategies; advanced detection capabilities including User and Entity Behavior Analytics; mature compliance automation with continuous evidence pipelines; and carbon accounting maturity with tightened sustainability targets.

8.3.5 Phase 4: Mature and Innovate (Months 48-60)

The Mature and Innovate phase positions Bangladesh for emerging capabilities and regional leadership. Key deliverables include advanced trust and transaction services including TPS Exchange and Blockchain RPC capabilities; confidential computing for high-sensitivity workloads; Post-Quantum Cryptography readiness and crypto agility; international equivalence mapping for cloud security standards; and frontier skills development in confidential computing, PQC, and sovereign AI.

8.4 Sector Adoption Sequencing

Table 8.2: Sector Adoption Waves

Wave	Candidate Sectors	Typical Workloads	Rationale
Wave A	Citizen portals, collaboration, public information	Web portals, static content, CRM, analytics	Low risk, high visibility, quick wins
Wave B	Social protection, education, agriculture	Case management, learning platforms, extension apps	Moderate risk, scalability benefits

Wave C	Health, land, local government	Registries, telemedicine, land services	High sensitivity, requires mature controls
Wave D	Finance, customs, justice, CII-adjacent	Payment services, enforcement workflows	Highest assurance and audit requirements

8.5 Migration and Modernization Factory

The Migration Factory establishes repeatable processes for transitioning workloads to Government Cloud. The standard lifecycle includes Discover phase for application inventory, dependencies, data mapping, and technical debt assessment; Classify phase for data classification, criticality tiering, and regulatory constraint identification; Plan phase for migration strategy selection, target architecture design, SLO/RPO/RTO definition, and security/privacy assessment including DPIA triggers; Build phase for landing zone provisioning, CI/CD setup, configuration-as-code, secrets management, and baseline observability; Migrate phase for data migration execution, application cutover, and validation; Operate phase for SRE handover, runbooks, incident drills, and continuous compliance reporting; and Optimize phase for cost, performance, resiliency, and sustainability improvements and legacy decommissioning.

8.5.1 Migration Strategies

Table 8.3: Migration Strategy Framework (6R)

Strategy	Typical Triggers	Policy Constraints
Rehost	Legacy VMs with minimal change; urgent DC exit	Must implement baseline controls, logging, encryption, segmentation
Replatform	DB migration to managed service; containerize	Ensure portability; avoid proprietary lock-in without exit plan
Refactor	Need elasticity, resilience, API-first; DPI integration	Mandatory DevSecOps, threat modeling, SLO/error budgets
Replace	SaaS adoption; commodity functions	Cross-border, support access, telemetry risks must be assessed
Retire	Duplicate systems; unsupported technology	Must preserve records retention obligations
Retain	Regulatory blockers; OT/ICS environments	Time-bound decision with mitigation and modernization roadmap

8.6 Prioritization Rules

Workload migration shall be prioritized according to the following rules. Priority shall be given to workloads that unblock Digital Public Infrastructure including identity and access, payments integration, registry modernization, and interoperability enabling services. Priority shall also be given to workloads with high demand elasticity and citizen-facing performance requirements. Workloads requiring specialized OT/ICS environments shall be deferred until segmentation, monitoring, and supplier controls are validated. For D3/D4 data classes and C3/C4 criticality, sovereign placement in NDC or accredited domestic sovereign cloud shall be required unless a time-bound exception is granted. Priority shall be given to migrations that reduce systemic risk by removing unsupported systems, consolidating duplicative platforms, and eliminating unmanaged server sprawl.

8.7 Capacity Building and Change Management

Successful implementation requires comprehensive capacity building across government. Training tracks shall include cloud architecture and operations for technical staff, DevSecOps and Site Reliability Engineering for development and operations teams, security and compliance for CISOs and audit personnel, data governance and privacy engineering for CDOs and privacy officers, and executive awareness for senior leadership. A Centre of Excellence may be established to provide ongoing support, maintain best practices documentation, and facilitate communities of practice across agencies.

CHAPTER 9: MONITORING, EVALUATION, AND REVIEW

9.1 Monitoring Framework Objectives

The monitoring framework ensures accountability for implementation progress, enables evidence-based decision making, and supports continuous improvement of government cloud initiatives. Effective monitoring tracks implementation progress against planned milestones, identifies deviations early enabling timely corrective action, provides data for resource allocation and prioritization decisions, ensures accountability of implementing agencies, and supports transparency through regular public reporting.

9.2 National Cloud Assurance Dashboard

A National Cloud Assurance Dashboard (NCAD) shall be implemented to provide a consolidated view of government cloud operations. The dashboard shall display service inventory showing what runs where across NDC, BDCCL, Meghna Cloud, and accredited providers; workload classification by data class and criticality tier; service availability and SLO compliance status; vulnerability posture and patch compliance metrics; incident counts and response performance indicators; disaster recovery readiness including RPO/RTO achievement and test outcomes; audit findings and remediation status; data residency compliance and cross-border exception tracking; cost governance signals including egress patterns and anomaly trends; and sustainability indicators where measurable.

9.3 Key Performance Indicators

Table 9.1: National Cloud KPI Dashboard

KPI	Definition	Target (Phase 2)
Onboarding Lead Time	Median days from request to landing zone provisioned	≤ 30 days
Migration Throughput	Number of workloads migrated per quarter	Increasing trend; per-sector targets
Security Posture	Percentage of critical findings closed within SLA	≥ 90%
Incident Response	Median time to contain P1 cloud incident	Improving trend; agreed thresholds
Availability	Percentage of priority digital services meeting SLO	≥ 95%
Data Exchange Readiness	Number of priority registries integrated via NRDEX patterns	≥ 5 priority registries
Cost Control	Percentage of systems with anomaly detection enabled	100% for top 20 systems

9.4 Mandatory Reporting Requirements

9.4.1 Tier 4 and CII Services (Monthly)

The highest criticality services shall report monthly on uptime and SLO compliance, security event summary with counts and severity distribution, critical CVE remediation status, privileged access review summary, and backup and restore verification summary.

9.4.2 Tier 3 Services (Quarterly)

High criticality services shall report quarterly on service inventory and hosting locations including backups, logs, and telemetry; data classification and criticality tier summary; SLO and availability report with monthly breakdown; incidents and response metrics including

MTTD/MTTR and severity distribution; vulnerability posture and remediation SLA compliance; access review and PAM summary; DR and restore test evidence with corrective actions; residency and cross-border attestations with exception register; audit findings and remediation status; and FinOps indicators including cost anomalies and egress trends.

9.5 Review Cadence

Table 9.2: Review and Reporting Cadence

Frequency	Scope	Responsible Party
Monthly	NDC delivery review; FinOps and risk dashboards	NDC
Quarterly	NDC performance review; migration wave plan update; compliance summary	NDC
Annual	Independent assurance summary; technical baseline updates; provider re-accreditation	BCC
Every 3-4 Years	Major policy review and amendment cycle	ICTD/NDC

9.6 Compliance Maturity Model

A four-level maturity model shall be used to phase requirements and guide audit assessments. Services shall progress through maturity levels based on their data classification and criticality tier, with higher tiers requiring higher maturity levels within defined transition windows.

Table 9.3: Compliance Maturity Levels

Level	Characteristics	Target Workloads
Level 1	Baseline controls implemented; manual evidence collection	D0/D1, C0/C1
Level 2	Centralized logging; periodic scans; documented DR tests	D2, C2
Level 3	Continuous posture monitoring; policy-as-code; SIEM integration	D3, C3 (minimum)
Level 4	Continuous control validation; automated evidence pipelines; resilience engineering	D4, C4 (target)

Tier 3 and Tier 4 services shall target Level 3 or higher within defined transition windows established by NDC. Failure to achieve required maturity levels shall trigger remediation plans with escalation to the National Data Center if not resolved within agreed timelines.

9.7 Continuous Compliance Approach

Government cloud environments and accredited providers shall implement continuous compliance through control evidence automation preferred for Tier 3/4 and C2+ workloads, including Cloud Security Posture Management (CSPM) for configuration drift detection, automated evidence capture of configuration snapshots, policy evaluation results, and scan outputs, and continuous audit log export with integrity controls.

Periodic attestations shall be required monthly for Tier 4 and CII environments, quarterly for Tier 3 environments, and semi-annually for Tier 1/2 environments unless risk assessment indicates more frequent reporting is necessary. Independent assurance shall include annual independent assessment for Tier 3/4 services with additional ad-hoc audits following major incidents, material changes, or risk flags.

9.8 Policy Review Mechanisms

9.8.1 Technical Baseline Updates

Technical baselines including the Government Cloud Control Framework (G-CCF) and Government Cloud Technical Baseline (GCTB) shall be updated annually to reflect security developments, emerging threats, and technology changes. Updates shall include transition windows for providers to comply, compatibility rules for ongoing contracts, and migration guidance for legacy systems.

9.8.2 Major Policy Reviews

This Policy shall be subject to comprehensive review every three to four years to assess continued relevance, update provisions based on implementation experience, and incorporate legal, regulatory, and technological developments. Major reviews shall examine policy outcomes and institutional effectiveness, market developments and competitive dynamics, legal framework changes including amendments to PDPO, NDGO, and CSO, and international best practice evolution.

9.8.3 Emergency Updates

Emergency updates may be issued for critical vulnerabilities, emerging threats, or urgent legal requirements. Emergency updates shall specify immediate applicability, communicate through established channels to all affected parties, and be incorporated into subsequent baseline updates.

9.9 Stakeholder Consultation

For major changes affecting implementation requirements or compliance obligations, NDC shall conduct stakeholder consultations with ministries and agencies, BDCCL operations, accredited providers, relevant regulators, and key sector representatives. Consultations shall include publication of proposed changes, comment periods for feedback, documented responses to substantive comments, and implementation toolkits and templates to support transition.

9.10 Enforcement and Remediation

9.10.1 Non-Compliance Classification

Non-compliance shall be classified to drive proportional enforcement. NC-1 (Minor) covers documentation gaps and minor control deviations without material risk impact. NC-2 (Moderate) covers control deviations increasing risk such as incomplete logging or delayed patching beyond SLA. NC-3 (Major) covers material risk exposure including residency breaches, privileged access weaknesses, or repeated SLO violations. NC-4 (Critical) covers confirmed breaches of sensitive data, repeated severe failures, or violations affecting CII, sovereignty, or legal compliance.

9.10.2 Remediation Timelines

Minimum remediation timelines shall apply based on classification. NC-1 findings shall be remediated within 30 days. NC-2 findings shall be remediated within 15-30 days depending on risk assessment. NC-3 findings shall require immediate risk mitigation within 72 hours, full remediation plan within 7 days, and closure within 30 days unless justified extension is

approved. NC-4 findings shall require immediate containment and national escalation, remediation plan within 72 hours, and continuous oversight until closure.

9.10.3 Enforcement Actions

Depending on severity and repeated failure, enforcement actions may include mandatory corrective action plans with increased audit frequency, restrictions on onboarding new workloads until closure, mandatory architectural changes such as migration to sovereign environment, suspension of specific services or interfaces, provider de-accreditation for specific tiers or full removal from registry, procurement suspension or contract termination in accordance with contract clauses, and referral under applicable legal instruments where offences are suspected.

CHAPTER 10: CONCLUSION AND FUTURE OUTLOOK

10.1 Policy Summary

The National Cloud Policy of Bangladesh 2026 establishes a comprehensive framework for cloud adoption across the Government of Bangladesh. This Policy provides the governance structures, technical standards, security baselines, and implementation mechanisms necessary to realize the benefits of cloud computing while protecting national interests, citizen data, and critical government functions.

The Policy establishes a sovereign-by-design approach ensuring that sensitive government data and critical infrastructure remain under Bangladesh legal control and jurisdiction. It implements risk-based workload placement rules that balance innovation and efficiency with appropriate protection based on data classification and service criticality. The Policy mandates baseline security, privacy, and resilience controls aligned with PDPO, NDGO, and CSO requirements. It creates institutional mechanisms through the National Data Center to coordinate implementation, resolve disputes, and ensure consistent application across government. The Policy specifies procurement and accreditation frameworks that promote competition, prevent vendor lock-in, and ensure that all providers serving government meet required standards.

10.2 Alignment with National Objectives

This Policy directly supports the objectives of the National Digital Transformation Strategy. Cloud computing is foundational to Digital Public Infrastructure, enabling the scalable, resilient, and interoperable platforms necessary for identity services, payments infrastructure, data exchange, and citizen service delivery. The Policy ensures that cloud adoption accelerates digital transformation while maintaining the sovereignty, security, and trust that citizens expect from government services.

The Policy aligns with and operationalizes the requirements of the legal framework including the National Data Governance Ordinance, 2025, which establishes data governance, interoperability, and institutional mandates; the Personal Data Protection Ordinance, 2025, which protects personal data and establishes data subject rights; and the Cyber Safety Ordinance, 2025, which mandates cybersecurity measures and Critical Information Infrastructure protection. By translating legal requirements into technical controls and operational procedures, this Policy ensures that cloud adoption occurs within a coherent legal and regulatory environment.

10.3 Critical Success Factors

Successful implementation of this Policy depends on several interdependent factors. Sustained political commitment and inter-ministerial coordination are essential to navigate institutional resistance and ensure continuity across government cycles. The ICT Division must maintain leadership in coordinating cross-agency initiatives, with the National Data Center providing strategic oversight and dispute resolution.

Adequate financing through blended approaches combining national budget allocations, development assistance, and public-private partnerships is necessary to build the required infrastructure and capabilities. Capacity building across government must develop the skills needed for cloud architecture, security operations, privacy engineering, and service

management. Change management programmes must address organizational resistance and build adoption momentum.

Technical execution quality is critical, including rigorous implementation of security baselines, continuous compliance monitoring, and effective incident response. NDC must maintain delivery discipline while remaining responsive to emerging challenges and opportunities.

10.4 Future Directions and Emerging Technologies

10.4.1 Sovereign AI and GPU Services

The National Digital Transformation Strategy identifies GPU-powered AI engine capability as a strategic national asset. The Government Cloud programme should establish a phased GPU service offering within sovereign environments at NDC and BDCCL with strict data handling and model governance. Service tiers should include training environments for model development, inference services for production deployment, and secure enclaves for sensitive analytics. MLOps baselines should address model registry, lineage tracking, evaluation frameworks, and monitoring of drift and bias. Data controls must ensure de-identification, privacy-enhancing technologies, and access approvals for sensitive datasets used in AI training and inference.

10.4.2 Trust and Transaction Services

The Digital Transformation Strategy identifies high-throughput transaction processing through TPS Exchange and Blockchain RPC capabilities for immutable record-keeping in critical government transactions. These should be delivered as shared services with API governance, auditability, and privacy constraints integrated with BNDA/NSB patterns and NRDEX exchange. Use cases include land registration with tamper-evident records, credential verification for educational and professional qualifications, licensing and permit systems with auditable decision trails, and high-integrity audit trails for financial and regulatory transactions.

10.4.3 Post-Quantum Cryptography Readiness

Quantum computing poses long-term risks to current cryptographic algorithms. The Policy anticipates the need for crypto agility enabling transition to post-quantum cryptographic algorithms as standards mature. NDC should monitor NIST post-quantum cryptography standardization and develop migration plans. Hybrid schemes combining classical and post-quantum algorithms may be piloted for high-assurance applications. Key management systems should be designed with algorithm agility to facilitate future transitions.

10.4.4 Confidential Computing

Confidential computing using hardware-based Trusted Execution Environments provides additional protection for sensitive workloads by protecting data during processing, not just at rest and in transit. This technology should be evaluated and piloted for D3 and D4 workloads where the threat model includes protection against privileged insiders and infrastructure compromise. As confidential computing matures, it may enable new deployment patterns that maintain sovereignty assurances while leveraging broader cloud capabilities.

10.5 Regional and International Context

Bangladesh's cloud policy positions the country alongside regional and international peers in developing sovereign cloud capabilities. The policy draws on international standards including ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, and the NIST Cybersecurity Framework while incorporating Bangladesh-specific requirements. International cooperation on cloud security, incident response, and emerging technology governance will remain important as the threat landscape evolves and new technologies emerge.

10.6 Call to Action

The successful realization of this Policy requires commitment and action from all stakeholders. The ICT Division and National Data Center must provide strategic leadership and coordination. Bangladesh Computer Council, BDCCL, and NDC must deliver technical capabilities and services meeting required standards. All Ministries, Divisions, and Agencies must engage constructively with the migration process, appointing accountable officers and executing their responsibilities under the governance framework.

Private sector providers must meet accreditation requirements and operate transparently within the policy framework. Development partners must align support with policy objectives and contribute to capacity building. Citizens must be informed about how their data is protected and their rights are enabled in government cloud environments.

Together, these stakeholders can realize the vision of a secure, sovereign, and innovative Government Cloud that accelerates Bangladesh's digital transformation while maintaining the trust and protection that citizens deserve.

DOCUMENT CONTROL

Document Title	National Cloud Policy of Bangladesh
Issuing Authority	ICT Division, Government of Bangladesh
Status	Draft for Inter-Ministerial Consultation
Version	1.0
Date	January 2026

Note: *This Policy is designed to replace and supersede earlier drafting approaches and to align comprehensively with Bangladesh's emerging legal and institutional framework for data governance, personal data protection, cyber safety, and national digital transformation. The Policy recognizes the concurrent enactment of the National Data Governance Ordinance, 2025 (NDGO), the Personal Data Protection Ordinance, 2025 (PDPO), and the Cyber Safety Ordinance, 2025 (CSO), which together create a comprehensive legal architecture for digital governance in Bangladesh.*