# PETROLEUM AND NATURAL GAS REGULATORY BOARD

New Delhi

**PNGRB/IT/GL/001/2026**

## GUIDELINES FOR

# BASELINE IT INFRASTRUCTURE

## FOR CGD ENTITIES

Version 1.0 | 2026

## PREAMBLE

The Petroleum and Natural Gas Regulatory Board (hereinafter referred to as "the Board") was established under the Petroleum and Natural Gas Regulatory Board Act, 2006 (hereinafter referred to as "the Act") to regulate the refining, processing, storage, transportation, distribution, marketing and sale of petroleum, petroleum products and natural gas excluding production of crude oil and natural gas so as to protect the interests of consumers and entities engaged in specified activities relating to petroleum, petroleum products and natural gas and to ensure uninterrupted and adequate supply of petroleum, petroleum products and natural gas in all parts of the country and to promote competitive markets and for matters connected therewith or incidental thereto.

City Gas Distribution (CGD) networks in India are authorised and regulated by the Board under the Act. As on date, the Board has authorised CGD networks across more than 300 Geographical Areas (GAs) spanning urban clusters, semi-urban areas, and towns across the country. The CGD sector is characterised by wide variation in scale, spread, and operational maturity — from large, multi-GA entities with millions of consumers and extensive network infrastructure, to smaller single-GA entities in early stages of network development and consumer acquisition. This diversity, while a strength of the sector, also means significant variation in the degree of digital maturity and IT infrastructure capability across CGD entities. This is a central consideration in the design of these Guidelines.

As the sector progressively embraces digitisation — from smart metering and online consumer services to real-time operational monitoring — access to reliable and adequate IT infrastructure has become integral to the safe, efficient, and consumer-responsive delivery of petroleum and natural gas services.

Recognising that smaller CGD entities — particularly those in newly authorised Geographical Areas or in early stages of network development — may not have formal IT governance frameworks or minimum baseline digital infrastructure in place, and that such gaps can adversely affect consumer service quality, data integrity, regulatory reporting, and operational safety, the Board considers it necessary to issue these Guidelines to establish a baseline standard of IT infrastructure that all CGD entities should aspire to meet.

The cybersecurity landscape is also undergoing rapid transformation driven by the advancement of Artificial Intelligence (AI) technologies. AI is being leveraged by threat actors to accelerate phishing campaigns, automate vulnerability exploitation, generate adaptive malware, and conduct deepfake-based impersonation at scale. CERT-In has issued a dedicated blueprint on reducing exposure and defending against AI-assisted cyber threats. Regulated entities should be aware of this evolving threat environment and progressively strengthen their cybersecurity posture in alignment with CERT-In guidance.

These Guidelines are intended to complement and reinforce the Technical Standards and Specifications including Safety Standards (T4S) and applicable directions, guidelines, and advisories issued by CERT-In, MeitY, and MoPNG. Regulated entities are also expected to comply with the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, and the rules and regulations framed thereunder, which provide the overarching legal framework for digital systems, data protection, and cybersecurity in India.

These Guidelines are organised in four Parts. Part I sets out the short title, objectives, applicability, and definitions. Part II establishes the baseline IT infrastructure requirements across ten topic areas, covering network and connectivity, computing infrastructure, data management, consumer-facing digital services, metering and operational technology systems, business IT systems, regulatory reporting, cybersecurity, system lifecycle and technology refresh (including software management), and interoperability and API integration. Part III addresses IT governance, covering the IT governance framework (including the designation of a senior IT official and a CISO), business continuity and disaster recovery, and IT human resources. Part IV deals with implementation, reporting to the Board, the relation to other regulatory instruments and laws, and the review and update of these Guidelines. Annexure A provides an indicative self-assessment checklist, Annexure B contains the glossary of abbreviations, and Annexure C provides indicative technology baseline guidance for smaller CGD entities.

# PART I — GENERAL

## 1. Short Title and Nature

1.1 These Guidelines may be called as the PNGRB Guidelines for Baseline IT Infrastructure for CGD Entities, 2026, and may be referred to in short as the "Baseline IT Infrastructure Guidelines" or "BITIG 2026".

1.2 These Guidelines are advisory and recommendatory in character. They articulate the minimum baseline of IT infrastructure that regulated entities should establish and maintain. Regulated entities are encouraged to exceed these baseline standards where their scale of operations, risk profile, number of Geographical Areas, or consumer obligations so warrant.

1.3 These Guidelines do not prescribe specific technology products, platforms, vendors, or technical configurations except where illustrative options are provided in Annexure C for the benefit of smaller CGD entities. Regulated entities retain full discretion to select appropriate technologies, provided the functional objectives stated herein are met.

1.4 Where a regulated entity is subject to mandatory requirements under any regulatory instrument issued by the Board, or under the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, or directions issued by CERT-In, NCIIPC, MeitY, MoPNG, or any other competent authority, those statutory requirements shall prevail over and supplement these Guidelines.

## 2. Objectives

These Guidelines seek to achieve the following objectives:

2.1 To establish a minimum standard of IT infrastructure that enables regulated entities to reliably serve consumers and fulfil their regulatory obligations.

2.2 To promote uniformity and interoperability in the digital infrastructure of regulated entities, particularly smaller City Gas Distribution (CGD) entities.

2.3 To protect the interests of consumers by ensuring continuity, accuracy, and accessibility of digital services, including billing, grievance redressal, and emergency response.

2.4 To facilitate the progressive digitisation of operational and administrative functions, consistent with the Board's broader regulatory objectives.

2.5 To lay a foundation for the implementation of cybersecurity obligations under applicable national frameworks, including directions and guidelines issued by CERT-In and requirements under the Information Technology Act, 2000.

2.6 To enable effective digital reporting by regulated entities to the Board, including through API-based integration with the Board's reporting and monitoring systems, improving regulatory oversight and policy formulation.

2.7 To promote planned lifecycle management of IT and OT systems, avoiding operational risks arising from technological obsolescence.

2.8 To provide smaller CGD entities with indicative technology baseline guidance to assist them in establishing the minimum infrastructure necessary for API integration and digital operations.

## 3. Applicability

3.1 These Guidelines apply to all entities authorised by the Board to develop and operate City Gas Distribution (CGD) networks under the Petroleum and Natural Gas Regulatory Board Act, 2006.

3.2 The Board recognises that regulated entities vary significantly in size, complexity, and geographic footprint. These Guidelines are aimed at bringing regulated entities up to an acceptable baseline standard

of IT infrastructure. Annexure C of these Guidelines provides indicative minimum technology configurations specifically for the benefit of smaller CGD entities.

3.3 CGD entities that already maintain IT infrastructure significantly above the baseline described herein are encouraged to document and periodically review their existing standards against these Guidelines.

## 4. Definitions

For the purposes of these Guidelines, unless the context otherwise requires —

| Term | Meaning |
|---|---|
| Act | The Petroleum and Natural Gas Regulatory Board Act, 2006. |
| ACID | Atomicity, Consistency, Isolation, Durability — the four transactional integrity properties of a reliable database management system |
| AI (Artificial Intelligence) | Machine-based systems that can, for a given set of objectives, make predictions, recommendations, or decisions influencing real or virtual environments, including generative AI, large language models, autonomous agents, and AI-enabled automation platforms. |
| API (Application Programming Interface) | A defined set of protocols, routines, and tools that enables software applications to communicate and exchange data with each other in a structured, standardised manner. |
| Backup | A copy of data, system configurations, or software maintained separately from the primary system for recovery purposes in the event of loss, corruption, or failure. |
| Board | The Petroleum and Natural Gas Regulatory Board constituted under Section 3 of the Act. |
| Business Continuity | The capability of a regulated entity to maintain or rapidly restore essential operations and consumer services in the event of a disruption. |
| CERT-In | Indian Computer Emergency Response Team, the national nodal agency for responding to cybersecurity incidents, established under Section 70B of the Information Technology Act, 2000. |
| CGD Entity | An entity authorised by the Board to develop, operate, or maintain a City Gas Distribution network in a Geographical Area. |
| CISO (Chief Information Security Officer) | The senior official designated by a regulated entity to be responsible for overseeing and managing information security and cybersecurity, including compliance with applicable cybersecurity frameworks and directions. |
| Data Protection Board of India (DPBI) | The Data Protection Board of India (DPBI) established by the Government of India, Ministry of Electronics and Information Technology (MeitY), under Section 18 of the Digital Personal Data Protection Act, 2023 (22 of 2023). The Board has been established as a body corporate with the mandate to function as an independent adjudicatory authority for the effective enforcement of the provisions of the Act. |
| Data Protection Officer (DPO) | A senior official appointed by a regulated entity designated as a Significant Data Fiduciary under Section 10 of the Digital Personal Data Protection Act, 2023, responsible for overseeing the entity's compliance with the Act, advising on data protection obligations, conducting Data Protection Impact Assessments, and representing the entity before the Data Protection Board of India. |
| Consumer Portal | A digital interface — web-based or mobile application — through which consumers can access services, submit applications, track status, raise grievances, and make payments. |

| | |
|---|---|
| Data Centre | A physical or virtual facility used to house computing, networking, and storage infrastructure, including cloud-based equivalents. |
| Disaster Recovery | Processes, policies, and procedures to enable recovery or continuation of technology infrastructure critical to an entity following a natural or human-induced disaster. |
| DPDP Act | The Digital Personal Data Protection Act, 2023, and the rules framed thereunder, which govern the processing of digital personal data in India. |
| End-of-Life (EoL) | The status of hardware or software for which the vendor or manufacturer has ceased to provide security patches, updates, or technical support. |
| ePortal | The electronic portal of PNGRB hosting various applications for internal and external users. |
| ERP / EAS | Enterprise Resource Planning or Enterprise Application Software — integrated systems supporting financial management, human resources, procurement, asset management, and related business functions. |
| Geographical Area (GA) | An area designated by the Board for the development of a City Gas Distribution network. |
| GIS (Geographic Information System) | A system designed to capture, store, manipulate, analyse, manage, and present spatial or geographical data, used in CGD entities for network mapping, asset management, and operational planning. |
| Guidelines | These PNGRB Guidelines for Baseline IT Infrastructure for Regulated Entities, 2026. |
| Help Desk | A centralised function or system enabling consumers and internal users to raise, track, and resolve service-related queries or complaints. |
| IAM | Identity and Access Management — the policies, processes, and technology for managing digital identities and controlling access to systems and data. IAM encompasses user account management, authentication (including multi-factor authentication), authorisation through role-based access control, and the lifecycle management of access rights. |
| IT | Information Technology — encompassing hardware, software, networking, and related services used for processing, storing, and communicating information. |
| IT Act | The Information Technology Act, 2000, including all rules, regulations, and guidelines framed thereunder, including the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. |
| IT Governance | The framework of policies, accountabilities, processes, and controls through which an entity directs and oversees its IT function. |
| MeitY | Ministry of Electronics and Information Technology, Government of India. |
| Metering System | The infrastructure and associated software used for measurement, recording, and communication of gas quantity consumed by consumers. |
| MoPNG | Ministry of Petroleum and Natural Gas, Government of India. |
| NCIIPC | National Critical Information Infrastructure Protection Centre, the nodal agency for the protection of Critical Information Infrastructure in India, established under Section 70A of the Information Technology Act, 2000. |
| Network | The communications infrastructure — including wired and wireless components — that enables connectivity within and between the IT systems of a regulated entity. |

| | |
|---|---|
| NHIMS | National Hydrocarbon Infrastructure Monitoring System – a centralised national-level GIS-based planning and monitoring system for the downstream petroleum and natural gas infrastructure developed by PNGRB. |
| NTP (Network Time Protocol) | A networking protocol for clock synchronisation between computer systems, used to ensure accurate and consistent timestamps in logs and transactions. |
| OSCRF | Oil Sector Cybersecurity Reference Framework issued by MoPNG |
| OT System | Operational Technology — hardware and software used to detect or cause changes in physical processes and operational equipment, including SCADA, DCS, PLCs, and associated systems. |
| Regulated Entity | An entity registered, authorised, or licensed by the Board under the Act. |
| RPO (Recovery Point Objective) | The maximum acceptable period of data loss in the event of a system failure or disaster, measured as the time between the most recent backup or checkpoint and the point of failure. RPO defines how much data an entity can afford to lose. |
| RTO (Recovery Time Objective) | The maximum acceptable period within which a critical IT system must be restored to operational status following a failure or disaster. RTO defines how quickly an entity must recover to avoid unacceptable impact on consumer services or operational continuity. |
| SCADA | Supervisory Control and Data Acquisition — a control system used to monitor and control industrial processes. |
| SLA | Service Level Agreement — a commitment between a service provider and a regulated entity specifying the expected level of service. |
| SOC | Security Operations Centre — a dedicated function — which may be internal, shared, or outsourced — providing continuous security monitoring, threat detection, event correlation, and coordinated incident response for an entity's IT environment. |
| T4S | Technical Standards and Specifications including Safety Standards issued by the Board under the Act. |
| Technology Refresh | The planned replacement or significant upgrade of IT or OT hardware, software, or systems to maintain functional adequacy, vendor support, and security currency over time. |
| UIDAI (Unique Identification Authority of India) | The statutory authority established under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, responsible for issuing Aadhaar numbers and overseeing the Aadhaar ecosystem including authentication and KYC services. |
| VAPT (Vulnerability Assessment and Penetration Testing) | A structured process of identifying security weaknesses in IT systems (vulnerability assessment) and simulating attacks to validate exploitability (penetration testing), conducted to assess and improve an entity's security posture. |
| Zero Trust Architecture (ZTA) | A security model based on the principle of never trusting and always verifying every network request, regardless of whether it originates inside or outside the organisation's network perimeter. ZTA requires continuous verification of identity and authorisation, micro-segmentation of networks, and least-privilege access controls. |

## PART II — BASELINE IT INFRASTRUCTURE REQUIREMENTS

# 5. Network and Connectivity

### 5.1 Reliable Internet Connectivity

Regulated entities should maintain reliable, adequately provisioned internet connectivity at all principal office locations to support consumer-facing digital services, regulatory reporting, and internal business operations. Connectivity arrangements should be commensurate with the entity's operational scale and consumer base having regard to the criticality of each facility and location.

### 5.2 Redundant Communication Links

To minimise the risk of connectivity failure adversely impacting consumer services or operational monitoring, regulated entities should, based on business criticality and risk assessment, maintain more than one independent communication link for mission-critical functions. This may be achieved through multiple service providers, diverse routing, or alternative communication technologies.

### 5.3 Internal Network Segmentation and IT/OT Separation

The internal network of a regulated entity should be structured and segmented in a manner that logically separates consumer-facing systems, business IT systems, and operational/OT systems from one another. IT and OT networks should be treated as distinct security domains and should not be directly interconnected without interposing appropriate security controls — such as firewalls, data diodes, or demilitarised zones (DMZ) — to prevent threats in the IT environment from propagating to operational systems and vice versa. Segmentation should limit the potential spread of faults, failures, or security incidents across the IT environment. The segmentation and access control principles in this Guideline are consistent with the Zero Trust Architecture (ZTA) model — the security approach premised on never trusting and always verifying every network request regardless of its origin. Regulated entities, particularly those with complex or multi-site IT environments, are encouraged to adopt ZTA principles in evolving their network security architecture, with reference to guidance issued by MeitY and CERT-In.

### 5.4 Remote Connectivity

Where regulated entities permit remote access to their IT systems — for staff, vendors, or support personnel — such access should be through secure, authenticated channels. Remote access privileges should be assigned on a need-basis and periodically reviewed (at least once every year).

# 6. Computing Infrastructure

### 6.1 Adequate Computing Capacity

Regulated entities should maintain computing infrastructure — including servers, workstations, and end-user devices — of sufficient capacity and reliability to support their business operations, consumer services, and regulatory compliance obligations without sustained performance degradation. Annexure C of these Guidelines provides indicative hardware governance and functional adequacy principles for smaller CGD entities as a practical reference.

### 6.2 Server Infrastructure

Regulated entities should utilise appropriately configured server infrastructure, whether on-premise, co-located, or cloud-hosted, for hosting business applications, consumer service systems, and data storage. Critical servers should have hardware resilience provisions for high availability such as power backup and redundant components, appropriate to the criticality of the functions they support. Regulated entities should, where operationally practicable, maintain separation between application servers and database servers to improve security isolation and performance. Where co-location is unavoidable for smaller deployments, appropriate software-level isolation and access controls should be applied.

### 6.3 End-User Computing Devices

All staff whose functions are integral to consumer service, operational management, or regulatory compliance should be provided with functional, adequately maintained computing devices. End-user devices should be subject to basic configuration standards addressing software maintenance and access control.

Where regulated entities permit the use of personally-owned devices (BYOD — Bring Your Own Device) for official functions involving access to consumer data, billing systems, or internal IT infrastructure, minimum compliance requirements should be established and enforced. These should include: (a) registration of the device with the entity's IT function before access is granted; (b) installation of up-to-date operating system and security patches; (c) prohibition on storing consumer personal data locally on personal devices; (d) where technically feasible, use of Mobile Device Management (MDM) or equivalent controls enabling remote wipe of organisational data in the event of device loss or theft; and (e) revocation of access upon cessation of the individual's engagement with the entity.

### 6.4 Uninterruptible Power Supply

Critical IT infrastructure — including core servers, network equipment, and communication systems — should be supported by uninterruptible power supply or equivalent power conditioning arrangements to prevent data loss and service interruption during power fluctuations or outages.

### 6.5 Physical Environment and Environmental Controls

Critical IT infrastructure — including servers, networking equipment, and storage systems housed on the regulated entity's own premises — should be installed in a controlled physical environment that protects the equipment from environmental hazards and maintains conditions conducive to reliable operation. Regulated entities should ensure the following:

a) *Temperature and Humidity Control*: Server rooms, network rooms, and equipment spaces housing critical IT infrastructure should be maintained at appropriate temperature and humidity levels through dedicated air-conditioning or precision cooling systems, appropriate to the heat load of the equipment installed. Temperature should be monitored continuously or at regular intervals, with alerts configured to notify responsible staff of conditions outside acceptable ranges, enabling timely corrective action before equipment is damaged;

b) *Protection from Environmental Hazards*: IT infrastructure rooms should be protected from water ingress, excessive dust, and other environmental hazards. Equipment should not be placed in locations susceptible to flooding or in proximity to water supply or drainage infrastructure unless adequate protective measures are in place. Regulated entities should also take adequate measures to protect IT infrastructure rooms from pest and rodent ingress, which can cause cable and equipment damage; appropriate pest control measures should be in place for server rooms and equipment spaces; and

c) *Fire Detection and Suppression*: Appropriate fire detection equipment, including smoke detectors, should be installed in IT infrastructure rooms. Where practicable, fire suppression systems suitable for IT equipment environments — using clean agent or equivalent means rather than water-based systems — should be provided for rooms housing critical servers and network equipment.

As indicative performance benchmarks for server room physical environments, regulated entities should target: (a) temperature maintained between 18°C and 27°C, consistent with global data centre standards; (b) relative humidity maintained between 40% and 60% (non-condensing); and (c) UPS backup capacity sufficient to sustain critical IT operations for a minimum of 30 minutes, enabling either graceful system shutdown or transfer to generator power before equipment loss occurs.

For regulated entities using cloud-hosted or co-located infrastructure, physical environment controls are the responsibility of the cloud or co-location service provider. Regulated entities should satisfy themselves, through their service level agreements or provider audit reports, that appropriate physical and environmental standards are maintained at the facilities where their data and systems are hosted.

### 6.6 Physical Security

Regulated entities should implement physical security controls to protect server rooms, IT equipment rooms, network equipment rooms, and facilities housing critical IT and OT infrastructure from unauthorised physical access. Physical security measures complement the environmental controls and together form the entity's physical infrastructure protection framework.

a) *Physical Access Restriction*: Access to server rooms and network equipment rooms should be restricted to authorised personnel only, through appropriate access control mechanisms such as electronic access cards, key-controlled locks, or equivalent measures. A log of access to critical infrastructure rooms should be maintained.

b) *CCTV and Video Surveillance*: Regulated entities should install CCTV or equivalent video surveillance systems covering, at a minimum: (a) entry and exit points of server rooms, IT equipment rooms, and network equipment rooms; (b) SCADA control rooms and centralised command and control centres; and (c) principal entry and exit points of buildings or floors housing critical IT and OT infrastructure. Surveillance footage should be retained for a minimum period of 30 days. For critical facilities, identified through risk assessment, retention may be extended up to 90 days. Access to surveillance recordings should be restricted to authorised personnel designated for security oversight, and a log of such access should be maintained. Where CCTV systems capture images of identifiable individuals, regulated entities should ensure compliance with the Digital Personal Data Protection Act, 2023, including by displaying appropriate notice in monitored areas.

### 6.7 Cloud Computing

Regulated entities may utilise cloud-based computing infrastructure and services to meet their IT infrastructure requirements under these Guidelines, provided that:

a) Data residency requirements applicable under Indian law, including the Digital Personal Data Protection Act, 2023, are complied with;

b) Adequate service level agreements are in place with the cloud service provider;

c) The entity retains the ability to access, export, and migrate its data;

d) Cloud services used for critical functions are subject to appropriate cybersecurity controls consistent with guidelines issued by CERT-In, MeitY, and MoPNG;

e) Regulated entities, particularly public sector undertakings, should give preference to cloud service providers empanelled by MeitY, in accordance with the MeitY Guidelines for Cloud Selection Framework and applicable government directives on cloud procurement;

f) Identity and Access Management (IAM): Cloud deployments should have dedicated IAM controls covering strict management of cloud administrator accounts, service accounts, and API keys; adoption of least-privilege and role-based access principles; regular review of access permissions; and prompt revocation of access upon personnel change;

g) Encryption Key Management: Encryption keys protecting cloud-hosted data should be managed securely, with access to key management systems restricted and audited. Regulated entities should understand their responsibilities under the cloud provider's shared responsibility model for encryption key management; and

h) Continuous Security Monitoring: Cloud deployments should be subject to continuous security monitoring through cloud-native security tools or equivalent mechanisms, with alerts configured for anomalous activity, unauthorised access attempts, and configuration changes to critical cloud resources.

### 6.8 Infrastructure Monitoring and Observability

Regulated entities should implement monitoring and observability capabilities for their critical IT infrastructure, to enable timely detection of failures, performance degradation, and security anomalies before they affect consumer services or operational continuity. At a minimum, the following should be monitored:

a) *Infrastructure monitoring*: servers, network equipment, storage systems, and power infrastructure should be monitored for availability, resource utilisation (CPU, RAM, disk, network), and hardware health indicators, with automated alerts for conditions outside defined operational thresholds;

b) *Application monitoring*: consumer-facing applications — including the consumer portal, billing system, and grievance system — should be monitored for availability, response time, and error rates;

c) Security logging and alerting: security-relevant events should be logged, correlated, and subject to periodic or automated review; and

d) *Escalation matrix*: regulated entities should maintain a documented escalation matrix specifying who is notified, through what channel, and within what timeframe when infrastructure or application alerts are triggered.

# 7. Data Management and Storage

## 7.1 Data Identification and Classification

Regulated entities should identify and maintain an inventory of the principal categories of data they generate, process, or hold, including consumer data, operational data, financial data, and regulatory data. Data should be managed in a manner proportionate to its sensitivity and criticality. In addition, regulated entities should establish foundational data governance practices covering: (a) *data ownership* — each principal data category should have a designated owner responsible for its accuracy, accessibility, and compliance with applicable requirements; (b) *data quality* — processes should monitor and maintain the quality of critical data, particularly consumer records, metering data, and regulatory submissions, with discrepancies investigated and remediated promptly; and (c) *data lineage* — for data used in regulatory submissions or audits, regulated entities should maintain the ability to trace data from its source through any transformations to its final reported form; and (d) *data flow diagrams* — to identify data flows, associated risks, and opportunities to improve system design and data controls.

## 7.2 Data Retention

Consumer data, transaction records, metering data, and records relevant to regulatory compliance and reporting should be retained for periods consistent with applicable statutory and regulatory obligations. Regulated entities should establish documented data retention policies aligned with these requirements.

## 7.3 Data Backup and Recovery

Regulated entities should maintain regular, documented backup processes for critical business and consumer data. Key aspects of an adequate backup regime include:

a) Backups should be performed with a frequency commensurate with the criticality and rate of change of the data;
b) Regulated entities are encouraged to follow the 3-2-1-1 backup strategy or any equivalent arrangement demonstrating comparable resilience and recoverability: maintaining at least three copies of data, stored on at least two different types of storage media, with at least one copy stored at an offsite or geographically separate location, and at least one copy maintained offline or air-gapped — the last being particularly important to ensure recoverability in the event of a ransomware attack or similar cyber incident;
c) Backup restoration should be tested periodically to verify the integrity and usability of backup data; and
d) Recovery time and recovery point objectives for critical data should be defined and documented.

As indicative benchmarks for backup performance: critical data — including consumer billing, metering, and regulatory reporting data — should be backed up at a minimum daily; at least one backup copy should be stored offsite or in a cloud environment and updated at least weekly; and backup restoration should be tested and validated at least once a year, with the results and any remedial actions documented.

## 7.4 Data Integrity

Regulated entities should implement controls to maintain the accuracy, completeness, and consistency of consumer records, billing data, metering data, and regulatory reports. Data amendment and correction processes should be logged and auditable. For requirements relating to the retention of ICT security logs and system clock synchronisation, see Guideline 12.5. Database management systems used for critical transactional data — including consumer billing, metering records, and financial accounts — should provide transactional integrity guarantees ensuring that transactions are processed reliably, maintaining data consistency and preventing data corruption and partial updates.

### 7.5 Consumer Data Privacy

Regulated entities should handle consumer personal and transactional data in accordance with the Digital Personal Data Protection Act, 2023, and rules framed thereunder, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, and any other applicable data protection requirements. In particular:

a) Consumer personal data should be collected only for specified, lawful purposes and not retained beyond the period necessary for those purposes; a DPDP Act-compliant data privacy notice should be displayed wherever personal data is collected from Data Principals, informing them of the purpose of collection and their rights; consent from Data Principals should be obtained prior to the processing of their personal data, in the manner specified under the Digital Personal Data Protection Act, 2023; Data Principals should be provided with the rights available to them under the DPDP Act 2023, including the right to access information about their personal data, the right to correction and erasure, the right of grievance redressal, and the right of nomination;
b) Access to consumer data should be restricted to authorised personnel and systems on a need-to-know basis;
c) Regulated entities should implement reasonable security practices, as required under the IT Act, to protect personal data from unauthorised access, disclosure, or loss; and
d) Consumer data processed through third-party systems or cloud platforms should be subject to appropriate contractual safeguards consistent with applicable law. Regulated entities that collect or process Aadhaar-based biometric or demographic data for consumer identity verification must do so strictly in accordance with the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, and the regulations and circulars issued by the Unique Identification Authority of India (UIDAI). Aadhaar data must be handled with heightened access controls, retained only to the extent permitted by UIDAI regulations, and entities must be registered as Authentication User Agencies or KYC User Agencies, as applicable.

Regulated entities should designate a responsible individual or function within the organisation — such as a legal, compliance, or privacy officer — to oversee compliance with the broader obligations of the Digital Personal Data Protection Act, 2023, including lawful bases for processing, consent management, data principal rights (access, correction, erasure, and nomination), and liaison with the Data Protection Board of India. This privacy compliance function is distinct from the CISO's responsibility for information security safeguards under Section 25 of the Information Technology Act, 2000. Regulated entities designated as Significant Data Fiduciaries by the Central Government under Section 10 of the Digital Personal Data Protection Act, 2023 are required to appoint a Data Protection Officer (DPO) who shall report to the Board of Directors and serve as the primary interface with the Data Protection Board of India on all matters relating to the Act.

## 8. Consumer-Facing Digital Services

### 8.1 Consumer Service Portal

Regulated entities should provide a digital interface — accessible via the Internet, whether as a web portal, mobile application, or both — through which consumers can at a minimum:

a) Submit applications for new connections and track their status, redirecting to the National Unified PNG Portal (myPNG.gov.in) where necessary;
b) Access current and historical billing information;
c) Make payments through secure, digital payment channels;
d) Apply for modifications, disconnections, or reconnections; and
e) Raise and track the status of service-related grievances and complaints.

The consumer portal should be maintained with adequate availability, and outages should be minimised and communicated to consumers where they are prolonged.

As indicative performance benchmarks for consumer-facing digital services, regulated entities should strive to achieve or exceed the following: (a) consumer portal availability of at least 99.5% per month (equivalent to a maximum of approximately 3.6 hours of downtime per month), with larger entities and those with higher consumer volumes targeting 99.9%; (b) standard portal pages loading within 3 seconds, consistent with MeitY's GIGW 3.0 web performance guidelines; (c) consumer grievances submitted through digital channels acknowledged within 24 hours of receipt; and (d) emergency helpline calls answered within 30 seconds during operational hours.

### 8.2 Emergency Contact and Response

Regulated entities should maintain a continuously available emergency contact mechanism — such as a dedicated helpline number — that is operational around the clock. Emergency response contact details should be prominently displayed on the consumer portal, bills, and other consumer communications. Where feasible, digital channels for logging emergency notifications may supplement voice-based channels.

### 8.3 Grievance Redressal System

The consumer portal and internal systems of a regulated entity should support an end-to-end digital grievance redressal process, enabling consumers to register complaints, receive unique complaint reference numbers, track resolution status, and receive communication on resolution. Grievance records should be maintained in a manner that supports regulatory audit and reporting.

### 8.4 Digital Billing and Statements

Regulated entities should have the capability to generate and deliver bills, consumption statements, and payment receipts in digital form. Digital billing should, over time, become the primary mode of communication with consumers who have registered digital contact details, without prejudice to consumers' right to receive physical bills on request.

### 8.5 Accessibility and Usability

Consumer-facing digital services should be designed for ease of use by a wide range of consumers, including those with limited digital literacy. In designing and developing consumer portals and mobile applications, regulated entities should have regard to the Guidelines for Indian Government Websites and Apps (GIGW 3.0) issued by the National Informatics Centre (NIC), which provide standards on accessibility, usability, and security for digital interfaces. In particular, web portals and applications should aim to conform to the Web Content Accessibility Guidelines (WCAG 2.1) at Level AA, ensuring accessibility for persons with disabilities in accordance with the Rights of Persons with Disabilities Act, 2016. Services should be accessible on commonly used devices and browsers. Consumer-facing applications should support English and Hindi. Regional language support may be progressively implemented considering consumer demographics and operational requirements.

### 8.6 Service Availability Standards

Regulated entities should establish and endeavour to meet defined availability standards for consumer-facing digital services. Planned maintenance leading to service unavailability should be scheduled during off-peak hours and communicated to consumers in advance.

### 8.7 Multi-channel Consumer Communication

Regulated entities should develop the capability to communicate with consumers through multiple digital channels, ensuring that important service communications — including connection status updates, billing notifications, payment confirmations, emergency alerts, and grievance acknowledgements — reach consumers through their preferred and registered channel. In particular:

a) Regulated entities should support at a minimum email and SMS notifications for consumer communications;

b) Where feasible, additional channels such as mobile application push notifications may be integrated to improve consumer reach and convenience; and

c) Regulated entities must obtain explicit consent from consumers before using each communication channel, in accordance with the Digital Personal Data Protection Act, 2023, and maintain accurate and current consumer communication preferences.

# 9. Metering and Operational IT Systems

## 9.1 Metering Data Management

Regulated entities should maintain systems capable of recording, storing, and processing meter reading data accurately and in a timely manner. Where automated or remote meter reading infrastructure is deployed, the associated data management systems should ensure the integrity, completeness, and traceability of metering records. CGD entities should progressively deploy smart gas meters across industrial, commercial, and domestic consumer categories. A centralised Meter Data Management System (MDMS) should be implemented for real-time acquisition, analytics, billing integration, and operational management of smart meter data across all consumer categories.

## 9.2 Integration with Consumer Billing

Metering systems should be capable of interfacing, directly or through managed processes, with the billing system to ensure accurate and timely generation of consumer bills. Manual or semi-manual data transfer processes, where still in use, should be subject to verification and reconciliation controls.

## 9.3 Operational Monitoring Systems

Regulated entities operating CGD networks and associated pipeline infrastructure should maintain operational monitoring systems — including where applicable SCADA and distributed control systems — commensurate with the scale and complexity of their infrastructure and as required by applicable T4S standards and safety regulations. CGD entities operating multiple Geographical Areas (GAs) should establish or progressively develop a centralised Control Room or Command Centre or, where operational requirements so justify, an equivalent decentralised arrangement providing consolidated real-time operational visibility across GAs, integrated with SCADA and, where applicable, with ERP platforms for automated metering data acquisition, gas reconciliation, and billing.

## 9.4 IT/OT Interface Management

Where operational technology systems are connected to or interface with business IT systems, regulated entities should manage such interfaces in a controlled manner. The primacy of operational safety — as governed by the applicable T4S framework — should be preserved at all times. In any conflict between IT and OT system requirements, operational safety shall take precedence. The IT/OT security architecture described in this Section (9.4) together with Sections 5.3 and 9.5 of these Guidelines is broadly consistent with the Defence-in-Depth approach of the IEC 62443 series of standards for industrial control system security, which provides the internationally recognised technical framework for OT security and which regulated entities operating pipeline, SCADA, or process control systems are encouraged to refer to.

> **Note:** Cybersecurity obligations applicable to operational systems, including SCADA and control systems, are addressed in the guidelines and directions issued by CERT-In, MeitY, NCIIPC, and MoPNG from time to time. Regulated entities should comply with applicable directions as they are issued by those authorities.

## 9.5 Legacy OT Hardware and Software Management

Operational technology systems — including SCADA, DCS, PLCs, RTUs, and HMIs — are characterised by long deployment lifecycles, often extending fifteen to twenty-five years. During this period, the hardware and software components of an OT system may reach or pass vendor end-of-life status, yet continued operation may be necessary due to the cost, safety assessment requirements, and operational disruption involved in replacement. Regulated entities should manage this inherent lifecycle tension through a structured approach to legacy OT asset management, distinct from the approach applied to general IT infrastructure.

### 9.6 OT Asset Register

Regulated entities should maintain a comprehensive register of OT assets at the component level, recording for each system and major component: the hardware model, part number, and firmware version; the operating system and application software versions installed; the total installed quantity and physical location; the current vendor support status (active, extended, or end-of-life); the OEM or vendor contact details for technical support and patching; and the OEM or vendor SLA arrangements in place for maintenance, patching, and spare parts supply. This register should be reviewed and updated at least annually and maintained as part of the entity's overall IT asset inventory.

### 9.7 Managing Legacy OT Systems Awaiting Modernisation

Where an OT system is running hardware or software that is at or beyond vendor end-of-life and immediate replacement is not operationally or financially feasible, regulated entities should implement a documented risk mitigation regime covering the following compensating controls as applicable:

a) *Network isolation*: the legacy system should be isolated within a dedicated, more secure sub-network segment, separated from other OT zones and from the corporate IT network by additional firewalls or, where feasible, unidirectional security gateways (data diodes);

b) *Air-gap maintenance*: where the operational function of the legacy system permits, it should be maintained in an air-gapped configuration with no direct network connectivity to IT systems or the Internet;

c) *Application whitelisting*: only OEM-authorised and approved applications should be permitted to execute on legacy OT workstations and servers, using application control or whitelisting solutions validated by the OEM;

d) *Workstation hardening*: local administrator accounts should be disabled and replaced with custom restricted accounts; USB and removable media ports should be disabled where not operationally required; auto-run of media should be disabled; and screen auto-lockout should be configured for operator stations where operationally safe;

e) *Endpoint protection*: OEM-validated antivirus or endpoint protection should be deployed and kept current with OEM-approved signatures, with regular scans conducted; and

f) *Continuous monitoring*: network traffic at the boundary of the legacy system segment should be monitored for anomalies, and any suspicious activity should be escalated promptly.

The risk associated with each legacy OT system managed under these compensating controls should be formally documented, reviewed by the CISO or equivalent official, and reported to senior management at least annually. A target timeline for modernisation or replacement should be established and tracked as part of the entity's capital planning process, acknowledging that OT replacement timelines are driven by safety assessment requirements, planned maintenance windows, and OEM support, and may extend over multiple years.

### 9.8 OT Spare Parts and Hardware Continuity

OT hardware components — particularly PLCs, DCS controllers, RTUs, and HMIs — may be proprietary and become unavailable from the market as the platform ages. Regulated entities should identify the critical hardware components of their OT systems for which supply continuity is essential, and establish arrangements to ensure availability in the event of hardware failure. This may include maintaining an in-house inventory of critical spare components, obtaining long-term supply agreements with the OEM or authorised spares suppliers, or exploring certified refurbished component sources. Failure to plan for spare parts continuity can result in extended outages of critical operational infrastructure where replacement components are no longer readily available.

## 10. Business IT Systems

### 10.1 Financial and Accounting Systems

Regulated entities should maintain digital systems for financial accounting, billing, and revenue management. These systems should support accurate record-keeping, audit trails, and the generation of financial statements and regulatory submissions. Regulated entities incorporated as companies under the Companies Act, 2013 that use accounting software for maintaining their books of account must ensure that such software complies with

the Companies (Accounts) Amendment Rules, 2014, as amended with effect from 1 April 2023. Specifically, the accounting software must: (a) record an audit trail of each and every transaction; (b) create an edit log of each change made in the books of account along with the date on which such change was made; and (c) ensure that the audit trail feature cannot be disabled.

### 10.2 Human Resources and Workforce Management

Regulated entities should maintain digital records of their workforce, including staff responsible for consumer service, field operations, and IT functions, in a manner that supports regulatory reporting on human resources where required.

### 10.3 Asset and Maintenance Management

Regulated entities should maintain a digital inventory (including GIS data where applicable) of their principal infrastructure assets, including pipeline networks, equipment, and consumer installations. Asset management systems should, over time, support planned maintenance scheduling, inspection records, and lifecycle tracking, consistent with the applicable T4S framework requirements.

### 10.4 Document Management

Regulated entities should maintain critical documents — including authorisation documents, statutory compliance records, consumer agreements, and regulatory submissions — in secure digital form, with appropriate version control and access management.

## 11. Regulatory Reporting and Data Submission

### 11.1 Digital Reporting Capability

Regulated entities should maintain IT systems capable of generating, compiling, and submitting regulatory reports and data to the Board in the formats and through the channels prescribed or adopted by the Board from time to time.

### 11.2 API-Based Reporting Integration

Where the Board operates or introduces a digital reporting or monitoring portal, data submission portal, or regulatory information system, e.g., the National Hydrocarbon Infrastructure Monitoring System (NHIMS) or PNGRB's ePortal, the regulated entities should ensure that their IT systems are capable of integrating with such systems through API-based data exchange, where so required by the Board. Regulated entities should:

a) Design or procure IT systems — particularly ERP, billing, and metering systems — with the capability to expose or consume APIs for structured data exchange;
b) Maintain API documentation and integration credentials securely; and
c) Test and validate API integrations periodically to ensure data accuracy and continuity of reporting.

As indicative benchmarks for regulatory reporting systems: (a) API response times for regulatory data submissions to the Board's systems (including NHIMS and the PNGRB ePortal) should not exceed 5 seconds for standard transactions; and (b) the availability of regulatory reporting interfaces should be at least 99.5% per month.

### 11.3 Data Accuracy and Audit Trail

Data submitted to the Board should be generated by regulated entities' own IT systems with appropriate controls to ensure accuracy and consistency. Regulated entities should maintain audit trails enabling them to trace submitted data back to source records.

### 11.4 Confidentiality of Regulatory Submissions

Regulated entities should manage regulatory data and submissions in a manner that preserves their confidentiality and integrity, including during transmission. Submissions made through digital channels should use secure transmission methods, including encrypted channels.

# 12. Cybersecurity Baseline

Regulated entities handle sensitive consumer data, manage critical energy infrastructure, and are subject to a growing and increasingly AI-assisted landscape of cyber threats. While detailed cybersecurity requirements are addressed through applicable national frameworks, regulated entities should maintain a baseline level of cybersecurity commensurate with the nature of their operations. This Section sets out ten guidelines covering the principal cybersecurity baseline obligations: compliance with national cybersecurity frameworks (12.1); information security under the IT Act (12.2); basic security controls including access management, MFA, RBAC, endpoint protection, and network security (12.3); encryption of data at rest and in transit (12.4); log retention and system clock synchronisation (12.5); vulnerability assessment and penetration testing (12.6); cyber incident reporting, response, and drills (12.7); security awareness and training (12.8); third-party and supply chain security (12.9); and governance of artificial intelligence systems (12.10).

## 12.1 Compliance with National Cybersecurity Frameworks

Regulated entities should comply with all applicable directions, guidelines, and advisories issued by CERT-In under Section 70B of the Information Technology Act, 2000, including mandatory requirements relating to cyber incident reporting, security practices, and information security management. Entities whose systems are designated as Critical Information Infrastructure (CII) by the Central Government under Section 70A of the Act should additionally comply with the applicable mandatory guidelines issued by the National Critical Information Infrastructure Protection Centre (NCIIPC). Other entities may refer to NCIIPC's guidance as a voluntary best practice reference.

Regulated entities should also have regard to any sector-specific cybersecurity guidelines and directions issued by the Ministry of Petroleum and Natural Gas from time to time, such as the Oil Sector Cybersecurity Reference Framework (OSCRF), which provide additional requirements applicable to oil and gas entities. Regulated entities should further refer CERT-In's Blueprint for Reducing Exposure and Defending against AI-Assisted Vulnerabilities Exploitation in Digital Infrastructure, which provides national-level guidance on cybersecurity governance and defensive measures in the context of AI-enabled threats.

## 12.2 Information Security under the IT Act

Regulated entities should implement reasonable security practices and procedures as required under Section 43A of the Information Technology Act, 2000, and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. This includes maintaining a documented information security programme, or adopting a recognised information security standard, appropriate to the scale and sensitivity of the entity's IT operations.

## 12.3 Basic Security Controls

Regulated entities should implement and maintain, as a minimum, the following categories of security controls:

a) *Access Management*: Access to IT systems and data should be restricted to authorised users on a need-to-know and least-privilege basis, implemented through a Role-Based Access Control (RBAC) model that assigns permissions according to each user's designated function rather than on an ad hoc basis. Multi-Factor Authentication (MFA) should be enforced for all remote access sessions and for all privileged or administrative accounts. User accounts should be reviewed periodically, and access of departing or role-changing staff should be promptly revoked or adjusted.

b) *Endpoint Protection*: Deploy and maintain appropriate endpoint security measures — including malware protection and device management — on servers, workstations, and other IT assets. Regulated entities should implement advanced endpoint security capabilities beyond signature-based antivirus protection, including behavioural detection and response capabilities on servers, workstations, and laptops, to detect and respond to sophisticated threats including fileless malware and AI-assisted attacks. In hardening operating systems, web servers, database platforms, and network devices, regulated entities are encouraged to refer to the Center for Internet Security (CIS) Benchmarks, which provide widely-adopted hardening guidance for commonly deployed technology platforms.

c) *Network Security*: Implement appropriate perimeter security controls, such as firewalls, to protect the entity's IT environment from unauthorised access. Network traffic should be monitored for anomalies on critical systems. Regulated entities operating consumer-facing web portals or external APIs should

deploy Web Application Firewall (WAF) capabilities to protect against application layer vulnerabilities including those identified in the OWASP Top 10, such as injection attacks, broken access control, and cross-site scripting. Network-level intrusion detection or prevention capabilities should be considered for critical network segments. Application whitelisting or allowlisting controls should be implemented to prevent execution of unauthorised software on critical IT systems, consistent with the approach required for OT systems.

d) *Email and Communication Security*: Apply controls to reduce the risk of phishing, malware distribution, and other email-borne threats targeting entity staff, including AI-generated and deepfake-based social engineering.

e) *Privileged Access Management*: Regardless of whether privileged access is initiated remotely or from within the corporate network, regulated entities should implement heightened controls over privileged and administrative sessions, including session monitoring, logging of actions undertaken during the session, and time-limited access grants. Periodic review (at least once a year) of Privileged Access should be done consistent with good practice.

f) *Security Operations Centre (SOC)*: Regulated entities operating large-scale infrastructure should consider establishing or obtaining access to Security Operations Centre (SOC) capabilities — providing continuous security monitoring, threat detection, and coordinated incident response — consistent with guidance issued by CERT-In.

As indicative benchmarks for access management: (a) Multi-Factor Authentication (MFA) should be enforced for 100% of privileged accounts and all remote access connections without exception; (b) credentials for privileged accounts should be rotated at least every 90 days; and (c) access rights for privileged users should be formally reviewed at least once annually to confirm that access remains necessary, appropriate, and consistent with current role responsibilities.

### 12.4 Encryption of Data

Regulated entities should protect sensitive data through encryption, commensurate with the sensitivity and criticality of the data. In particular:

a) Sensitive consumer data, financial records, and regulatory submissions should be encrypted at rest using industry-standard encryption algorithms;

b) Data in transit — including API communications, regulatory data submissions, remote access sessions, and transfers over public networks — should be protected using strong transport layer security (TLS) or equivalent encrypted channels;

c) Backup media containing sensitive data should be encrypted to prevent unauthorised access in the event of physical loss or theft; and

d) Regulated entities should align their encryption practices with the guidance issued by CERT-In, MeitY, and MoPNG from time to time.

### 12.5 Log Retention and System Clock Synchronisation

Regulated entities should maintain logs of ICT infrastructure activity to support security monitoring, incident investigation, and regulatory compliance. This guideline addresses ICT security logs; for requirements relating to audit trails on business and consumer data records, see Guideline 7.4. In accordance with directions issued by CERT-In:

a) ICT infrastructure logs should be retained for a minimum of 180 days or the period prescribed in the applicable CERT-In directions in force from time to time whichever is higher, stored securely and within Indian jurisdiction unless otherwise permitted by applicable law;

b) Log files should be protected against tampering and unauthorised modification — regulated entities should use write-protected or equivalent mechanisms for log storage on critical systems;

c) All critical IT systems — including servers, network equipment, and application platforms — should be configured to synchronise their system clocks with an authoritative and accurate time source using the Network Time Protocol (NTP) or equivalent, to ensure consistency and forensic reliability of log timestamps; and

d) Log monitoring should be performed periodically, with anomalies investigated and escalated in accordance with the entity's incident response procedures.

### 12.6 Vulnerability Assessment and Penetration Testing

Regulated entities should assess the security posture of their IT systems through periodic Vulnerability Assessment and Penetration Testing (VAPT). In particular:

a) Critical internal systems and infrastructure should be subject to VAPT at least once annually, conducted by or under the supervision of auditors empanelled by CERT-In;

b) Internet-facing systems — including consumer portals, APIs, web applications, and cloud deployments — should undergo security assessment, including external VAPT, at least once annually. VAPT of consumer-facing web applications and APIs should specifically assess against the OWASP Top 10 vulnerability categories, which represent the most critical and commonly exploited web application security risks;

c) OT and SCADA systems should be assessed for cybersecurity vulnerabilities periodically, in a manner consistent with operational safety requirements and applicable T4S standards;

d) Critical findings and vulnerabilities identified through VAPT should be remediated within defined and documented timelines, prioritised according to severity; and

e) VAPT results and remediation actions should be reviewed by the CISO and reported to senior management.

### 12.7 Cyber Incident Reporting, Response, and Drills

Regulated entities should maintain documented procedures for responding to cybersecurity incidents. In the event of a cyber incident:

a) The incident should be reported to CERT-In within the timelines prescribed under applicable CERT-In directions — currently within six hours of detection or notification — in accordance with the Information Technology Act, 2000;

b) The incident should also be reported to NCIIPC where the entity's systems have been designated as Critical Information Infrastructure or Protected Systems;

c) Threat intelligence related to cyber incidents should be shared with CERT-In and MoPNG as appropriate, to support sector-wide situational awareness;

d) The entity's designated CISO should lead the response effort and coordinate with relevant authorities; and

e) Any incident reported to CERT-In under the foregoing obligation should also be communicated to the Board within the same reporting cycle. In addition, any cyber incident that affects or has the potential to affect consumer services, operational safety, or regulatory reporting — whether or not it falls within CERT-In reporting categories — should be brought to the Board’s notice promptly.

Regulated entities should also conduct periodic cybersecurity exercises to test their incident response readiness. This should include tabletop exercises simulating realistic attack scenarios, backup restoration validation, and, where feasible, participation in cyber drills and simulations conducted by CERT-In from time to time.

As indicative benchmarks for cyber incident response performance, aligned with the Oil Sector Cybersecurity Reference Framework (OSCRF): (a) the Mean Time to Detect (MTTD) for high and critical severity security alerts should be under 30 minutes from the time the alert is generated; (b) the Mean Time to Respond (MTTR) — from detection to initial containment action — should be under 4 hours for high and critical incidents; and (c) the Mean Time to Resolution should be under 120 hours where no external procurement is required. These benchmarks should be tracked, reviewed periodically, and progressively improved as monitoring capabilities mature.

### 12.8 Security and Privacy Awareness and Training

Regulated entities should conduct periodic cybersecurity and data privacy awareness and training programmes for all staff. Data privacy awareness should cover consumer data handling obligations under the DPDP Act 2023, including consent requirements, Data Principal rights, personal data breach notification, and restrictions on sharing consumer data with third parties. In the context of the evolving AI-assisted threat landscape, awareness programmes should specifically address:

a) AI-generated phishing and spear phishing campaigns, which may closely mimic legitimate communications;
b) Deepfake voice and video impersonation, including fraudulent executive communications;
c) Business email compromise and credential theft techniques using AI-assisted social engineering; and
d) Safe handling of sensitive data when using AI tools, including restrictions on uploading consumer or operational data to publicly accessible AI platforms.

Staff with administrative or privileged access to IT systems should receive more targeted security training appropriate to their roles. Regulated entities should aim to provide cybersecurity awareness training to all employees at least once every three years, with the CISO team refreshing their knowledge through relevant certifications or structured learning at least once every two years, consistent with good industry practice in the petroleum sector and the training standards specified in the OSCRF.

### 12.9 Third-Party and Supply Chain Security

Regulated entities should assess the cybersecurity posture of key IT vendors and service providers, particularly those with access to sensitive systems or consumer data. Contractual arrangements with such vendors should include appropriate security obligations, confidentiality requirements, and incident notification provisions. Regulated entities should also assess AI service providers and third-party AI platforms used in their operations as part of their vendor security review.

Regulated entities that engage third-party staff or contractors to perform functions involving access to consumer data, billing systems, internal networks, or OT infrastructure should: (a) require the vendor organisation to execute a Non-Disclosure Agreement (NDA) covering the confidentiality of consumer information and internal IT data before access is granted; and (b) where practicable, require background verification of third-party personnel granted access to critical systems or sensitive consumer data, commensurate with the sensitivity of the access being provided. Access credentials for third-party personnel should be time-bound, reviewed upon contract renewal or termination, and promptly revoked when the engagement ends.

### 12.10 Governance of Artificial Intelligence Systems

As regulated entities increasingly adopt AI technologies — including in operational analytics, predictive maintenance, consumer service automation, and decision-support systems — they should ensure that AI adoption is governed in a structured, risk-aware manner proportionate to the entity's current and planned use of AI technology and consistent with CERT-In's guidance. The following baseline measures should be established:

a) *AI Usage Policy*: Regulated entities should define and implement an AI usage policy covering acceptable and prohibited uses of AI tools by staff, including a clear prohibition on uploading sensitive consumer data, operational data, or regulatory information to publicly accessible AI platforms or large language models without appropriate authorisation and safeguards.
b) *AI Asset Inventory*: Regulated entities should maintain visibility over AI systems deployed or in active use within the organisation, including AI-powered applications, third-party AI services, AI APIs, and AI-integrated workflows, as part of their broader IT asset inventory.
c) *Risk Assessment*: Before deploying AI in contexts that affect consumer services, operational safety, metering, or regulatory reporting, regulated entities should conduct a risk assessment covering data exposure risks, third-party dependency, integration security, and potential impact on operational continuity.
d) *Human Oversight*: AI-assisted outputs that affect safety-critical decisions, consumer rights, billing accuracy, or regulatory submissions should remain subject to human review and accountability. Fully autonomous AI decision-making in these domains should be avoided without appropriate validation and oversight mechanisms in place.
e) *AI-Aware Security Controls*: Security controls protecting AI systems, APIs, and integrated workflows should be maintained, including access controls on AI platforms and monitoring of AI usage for anomalous behaviour.
f) *AI Transparency and Explainability*: Where AI systems are used in contexts that affect consumer services, billing accuracy, metering, or regulatory submissions, regulated entities should maintain the

ability to explain or audit the basis for AI-generated outputs or decisions. Fully opaque AI decisions affecting individual consumers or regulatory compliance should be avoided; human review mechanisms should be in place for AI-generated outputs in these high-stakes contexts.

g) *Continuous Monitoring of AI Systems*: AI systems in production should be monitored for performance degradation, model drift, anomalous output patterns, and potential misuse. Monitoring logs should be maintained and reviewed periodically, and material deviations from expected behaviour should trigger human investigation and, where warranted, suspension of the AI system pending review.

## 13. System Lifecycle and Technology Refresh

Technology obsolescence is a significant operational and security risk for regulated entities. IT and OT systems that are no longer supported by their vendors expose entities to heightened cybersecurity risk, operational failures, and regulatory non-compliance. Regulated entities should manage the lifecycle of their technology assets in a planned and systematic manner.

### 13.1 Technology Lifecycle Policy

Regulated entities should establish and maintain a documented technology lifecycle policy covering their principal IT and OT assets. The policy should define:

a) Expected useful life and planned refresh cycles for major hardware categories (servers, networking equipment, end-user devices, OT hardware);
b) Criteria for identifying end-of-life and end-of-support status for hardware and software; and
c) Processes for planning and budgeting technology refresh in advance of end-of-life dates.

### 13.2 Hardware Refresh

Regulated entities should plan for the timely replacement of hardware assets before they reach end-of-life or fail to meet operational requirements. Servers and core networking equipment critical to consumer services or operational monitoring should be prioritised for refresh. Hardware procurement should take into account the expected support lifecycle offered by the vendor at the time of acquisition.

### 13.3 Software Currency and End-of-Life Management

Regulated entities should avoid deploying software — including operating systems, middleware, and business applications — that has reached end-of-life and no longer receives security updates from the vendor, particularly on systems connected to the internet, processing consumer personal data, or interfacing with operational systems. Where immediate migration is not operationally feasible, regulated entities should implement compensating controls, document the risk formally, and establish a binding timeline for migration.

### 13.4 OT and SCADA System Modernisation

Regulated entities should maintain visibility over the lifecycle status of their OT assets, including vendor support timelines, and plan for modernisation or replacement of OT systems through a structured, multi-year capital programme. Unlike general IT infrastructure, OT system replacement cannot be administratively time-bound — timelines must be determined in consultation with operations, safety, and OEM teams, and must reflect planned maintenance windows, safety re-certification requirements, and OEM support availability. The following principles should govern OT modernisation planning:

a) *Risk-prioritised sequencing*: OT systems that are directly connected to corporate IT networks, have internet-facing interfaces, or are running substantially end-of-life software carry the highest cybersecurity exposure and should be prioritised for isolation or early modernisation. Systems that are fully air-gapped and adequately compensated may be scheduled for later phases subject to documented annual risk review;
b) *OEM support arrangements*: regulated entities should maintain active OEM support contracts or extended support agreements for all critical OT systems in operation. Where a system has passed the vendor's standard support lifecycle, entities should seek to formalise extended support arrangements with the OEM — including patch provision, remote support, and spare parts availability — and document the terms of such arrangements;

c) *Safety assessment before any change*: any hardware or software replacement in an OT environment must be assessed for safety impact before implementation, consistent with applicable T4S requirements. OEM involvement should be obtained for any modification to a control system that could affect its certified safety function;

d) *Greenfield vs brownfield considerations*: entities commissioning new OT systems or expanding existing infrastructure ('greenfield') should apply current security standards — including network segmentation, encrypted communications where operationally feasible, and audit logging — from the outset. Brownfield modernisation of existing systems should progressively migrate toward current standards as components are replaced;

e) *Cybersecurity in procurement*: hardware and software procured for OT systems should be assessed for cybersecurity adequacy — including vendor support lifecycle, patch availability, and security architecture — as part of the procurement evaluation, alongside operational and functional criteria. Entities should prefer OT platforms for which the OEM provides a documented, active cybersecurity support and patching programme.

### 13.5 Budgetary Provision for Technology Refresh

Regulated entities should make adequate budgetary provision for planned technology refresh as part of their annual capital and operational expenditure planning. Technology refresh should not be deferred indefinitely on grounds of cost alone where doing so creates material risk to consumer services, operational safety, or information security.

### 13.6 Software Licensing and Supported Software

Regulated entities should use software that is properly licensed and maintained under vendor support arrangements. The use of software versions that have reached end-of-life and no longer receive security updates should be avoided. Earlier sub-sections of this Guideline address related software lifecycle topics including end-of-life management (13.3) and OT system modernisation (13.4).

### 13.7 Software Patch and Update Management

Regulated entities should maintain a regular process for applying security patches and software updates to operating systems and applications. For IT systems, patches should be applied within timelines proportionate to severity. As indicative benchmarks which may be varied based on documented risk assessment, OEM recommendations and implementation constraints, subject to suitable mitigating controls: critical severity patches (CVSS score 9.0 and above, or as categorised in CERT-In advisories) should be deployed within 30 days of vendor release; high-severity patches (CVSS score 7.0 to 8.9) should be deployed within 60 days. Patch management for OT systems is governed by fundamentally different constraints and must follow the approach described below.

**OT Patch Management**: Patches for OT systems — including operating system patches, application patches, antivirus signatures, and firmware updates — must be applied only after validation and explicit approval by the OEM of the OT system. Regulated entities should align their OT patch management practices with those specified in the OSCRF. An unapproved patch applied to a control system may cause process upsets, equipment damage, or safety failures, and OEM approval is therefore a mandatory prerequisite, not an optional step. The following specific requirements apply:

a) Only OEM-approved and validated patches and antivirus signatures should be installed on OT systems. Patches sourced from any party other than the OEM or an OEM-authorised channel should not be deployed;

b) OEM-approved security patches and antivirus or endpoint protection signatures should be deployed within 90 days of the OEM issuing its approval and validation of the patch for the specific OT platform;

c) All patches should be tested in a staging or test environment equivalent to the production OT system before deployment to the live operational environment, where such a test environment is available;

d) Patches should be pushed to OT systems through a dedicated patch management server or jump server located in the DMZ between the IT and OT networks, to avoid direct connectivity between the patch source and the OT control network; and

e) Firewall software and security signatures for firewalls placed at the IT/OT boundary should be updated promptly upon release of approved updates, while updates for internal OT network firewalls should be deployed within 30 days of release, consistent with OEM guidance.

### 13.8 Application Development and Acquisition

Where regulated entities develop, procure, or commission bespoke software applications — including consumer portals or billing platforms — they should ensure that appropriate quality assurance, testing, and acceptance procedures are followed before deployment. Software should be evaluated for functional adequacy, security, accessibility, and API capability. Where AI-assisted development tools are used, the generated code should be reviewed and tested before deployment.

## 14. Interoperability and API Integration

Regulated entities operate within an interconnected digital ecosystem involving consumers, payment service providers, government portals, smart metering networks, and the Board's own regulatory systems. Regulated entities should design and procure IT systems with interoperability in mind.

### 14.1 Interoperability by Design

When procuring, developing, or significantly upgrading IT systems — particularly consumer service platforms, billing systems, metering systems, and ERP solutions — regulated entities should favour systems that support open, standard-based interfaces and avoid proprietary data formats that create vendor lock-in or impede data portability. CGD entities managing gas distribution network data should maintain their GIS data in standard geospatial interchange formats — such as GeoJSON, Shapefile, GeoPackage, or equivalent — to facilitate regulatory reporting and API-based data exchange with the Board's systems. Refer to Annexure C for indicative GIS software options suitable for CGD entities.

### 14.2 API Capability for Core Systems

The core IT systems of regulated entities — including billing, metering, consumer management, and financial systems — should, to the extent practicable, be capable of exposing or consuming APIs to enable:

a) Data exchange with the Board's regulatory reporting and monitoring systems;
b) Integration with national payment gateways and digital payment platforms;
c) Integration with smart metering infrastructure and data concentrators;
d) Interoperability with national consumer service and government platforms; and
e) Sharing of relevant operational data with emergency response agencies where operationally required.

### 14.3 API Security

APIs exposed by regulated entities to external parties should be appropriately secured. Minimum API security measures should include:

a) Authentication and authorisation controls to ensure only permitted parties access the API;
b) Encryption of data in transit using TLS or equivalent;
c) Rate limiting and anomaly monitoring to detect and limit misuse; and
d) Maintenance of API access logs for audit and incident investigation purposes.

### 14.4 Third-Party Integration Governance

Regulated entities should maintain a register of significant third-party integrations — including payment gateways, cloud services, metering data platforms, AI service providers, and government portals — with which their IT systems interface. Each integration should be covered by appropriate contractual arrangements addressing security, data handling, and service levels. Integrations should be reviewed periodically for continued necessity and security adequacy.

### 14.5 Data Portability

Regulated entities should ensure that consumer data and operational records held in their IT systems can be exported in a structured, machine-readable format. This is important to enable migration to new systems, regulatory data submissions, and, where applicable, the exercise of consumer data rights under the Digital Personal Data Protection Act, 2023.

# PART III — IT GOVERNANCE

## 15. IT Governance Framework

### 15.1 Senior IT Official and Designated CISO

Every regulated entity should designate a senior official responsible for overseeing its IT function. The level of seniority and the scope of this role should be commensurate with the scale and complexity of the entity's IT environment.

In addition, every regulated entity should designate a Chief Information Security Officer (CISO) or an official performing equivalent functions, who shall be responsible for:

a) Overseeing the entity's information security and cybersecurity posture, including compliance with applicable CERT-In directions, the IT Act, and any cybersecurity guidelines issued by MeitY and MoPNG such as the Oil Sector Cybersecurity Reference Framework (OSCRF);
b) Developing, implementing, and reviewing the entity's information security policies and procedures;
c) Reporting significant cybersecurity risks and incidents to senior management and, where required, to the Board and CERT-In;
d) Serving as the primary interface with CERT-In and other competent authorities on cybersecurity matters; and
e) Overseeing compliance with applicable provisions of the Digital Personal Data Protection Act, 2023, in so far as they relate to information security.

Regulated entities operating SCADA, DCS, PLCs, or other OT systems should ensure that the CISO, or the designated individual responsible for OT cybersecurity, possesses or has access to adequate expertise in industrial control system security, including familiarity with the IEC 62443 series and the OSCRF issued by MoPNG. Given the fundamental difference between IT and OT security — particularly the primacy of operational safety in OT environments, the constraints on patch deployment, and the specialised threat landscape — regulated entities should avoid applying generic IT security controls to OT systems without adequate assessment of operational impact.

The seniority and organisational positioning of the CISO should be commensurate with the scale and risk profile of the entity's IT operations. For smaller regulated entities where a full-time CISO is not feasible, the function may be combined with another senior role, discharged through a group-level arrangement, or supported through a qualified outsourced cybersecurity specialist, provided accountability remains clearly assigned and adequately discharged.

### 15.2 IT Policies and Procedures

Regulated entities should develop and maintain documented IT policies and procedures covering, at a minimum:

a) Acceptable use of IT systems and devices;
b) User access management, including provisioning, review, and revocation;
c) Data backup and recovery;
d) Software update and maintenance;
e) Vendor and third-party IT service management;
f) API integration governance;
g) Incident reporting and response;
h) Artificial Intelligence usage — covering acceptable and prohibited uses of AI tools, data handling obligations when using AI platforms, and human oversight requirements for AI-assisted decisions.

i) BYOD policy — where regulated entities permit staff or third parties to access organisational systems, consumer data, or internal applications from personally-owned devices, a documented BYOD policy should be in place specifying the minimum compliance requirements for such devices; and

j) Enterprise architecture documentation — regulated entities should maintain documented architecture covering their principal IT domains, including application, infrastructure, integration and API, data, and security architecture, to support IT governance, change management, and vendor management decisions.

Policies should be reviewed and updated periodically, and where applicable, in response to significant changes in the entity's IT environment or applicable regulatory requirements.

### 15.3 IT Asset Management

Regulated entities should maintain an inventory of their principal IT assets — including hardware, software licenses, cloud subscriptions, API integrations, and AI systems in active use — to enable effective management, maintenance, and governance of their IT environment.

### 15.4 Change Management

Significant changes to IT systems supporting critical consumer services or operational functions should be subject to a change management process that assesses risks, obtains appropriate approvals, and ensures adequate testing before deployment. Changes to OT or operational safety systems should additionally comply with the applicable T4S requirements.

### 15.5 Vendor and Third-Party Management

Where regulated entities rely on third-party vendors or service providers for critical IT functions — including managed IT services, cloud services, metering system support, AI platforms, or software platforms — they should:

a) Maintain documented service level agreements with key IT service providers;

b) Retain adequate oversight over vendor-delivered services;

c) Ensure that vendor access to regulated entity systems is subject to appropriate controls; and

d) Have a contingency plan for the event of material vendor failure or exit.

## 16. Business Continuity and Disaster Recovery

### 16.1 Business Continuity Planning

Regulated entities should develop and maintain a Business Continuity Plan (BCP) that addresses the continuation of critical IT-dependent functions — including consumer services, billing, emergency response, and operational monitoring — in the event of significant IT disruptions, including those arising from AI-assisted cyberattacks and ransomware. The BCP should be tested and updated periodically (at least once annually), including through tabletop exercises and simulated attack scenarios.

### 16.2 Disaster Recovery

Regulated entities should establish and maintain a Disaster Recovery plan for critical IT systems. The plan should define, for each critical IT system, quantified Recovery Point Objectives (RPO — the maximum acceptable period of data loss in the event of a failure) and Recovery Time Objectives (RTO — the maximum acceptable period within which a system must be restored to operational status). RPO and RTO should be proportionate to the criticality of each system and the impact of its unavailability on consumer services and operational continuity. As indicative benchmarks: the RPO for critical consumer-facing systems — including billing, consumer portal, and metering data — should not exceed 4 hours; the RTO for such systems should not exceed 24 hours; and the RTO for regulatory reporting systems should not exceed 48 hours. These targets should be reviewed and progressively tightened as infrastructure and resilience capabilities mature. The plan should additionally define recovery procedures, recovery site arrangements where applicable, and roles and responsibilities. Disaster recovery capabilities should be tested periodically, including through backup restoration validation, to verify their effectiveness.

### 16.3 Manual Fallback Procedures

Regulated entities should maintain documented manual or alternative procedures for critical consumer-facing and operational functions in the event of IT system unavailability. Staff responsible for critical functions should be familiar with these fallback procedures, which should be subject to periodic review.

### 16.4 Incident Response and Communication

In the event of a significant IT disruption affecting consumer services, regulated entities should communicate proactively with affected consumers through available channels. All cyber incidents falling under CERT-In Cybersecurity directions should be reported to CERT-In, and to NCIIPC where applicable, within the prescribed timelines. Any incident reported to CERT-In under the foregoing obligation should also be communicated to the Board within the same reporting cycle. In addition, any cyber incident that affects or has the potential to affect consumer services, operational safety, or regulatory reporting — whether or not it falls within CERT-In reporting categories — should be brought to the Board's notice promptly.

## 17. IT Human Resources and Capacity

### 17.1 Dedicated IT Function

Regulated entities should maintain an internal IT function or, where full in-house capability is not feasible, ensure access to dedicated IT support through managed service arrangements. Responsibility for IT governance and cybersecurity, as described in Guideline 15.1, should be clearly assigned through a designated CISO or equivalent official.

### 17.2 IT and Data Privacy Competency of Staff

Staff performing IT and data privacy related functions should possess the necessary skills and knowledge for their respective roles. Regulated entities should provide or facilitate appropriate training and capacity-building for IT staff, commensurate with the entity's scale of operations and IT complexity.

### 17.3 Digital Literacy for Operational Staff

Staff engaged in consumer service and field operations should receive basic digital literacy training to enable effective use of the entity's IT systems. Regulated entities should plan for periodic refresher training as systems are updated or upgraded. Data privacy awareness training should be conducted for field executives who collect or process consumer personal data in the course of their operational activities, covering data handling obligations, consent requirements, and the prohibition on unauthorised sharing of consumer information.

# PART IV — IMPLEMENTATION AND COMPLIANCE

## 18. Implementation Approach

### 18.1 Self-Assessment

Regulated entities should undertake a self-assessment of their current IT infrastructure against the baseline standards described in these Guidelines. The self-assessment should identify gaps, prioritise remediation actions, and form the basis of a time-bound improvement plan where gaps are identified. Annexure A provides an indicative self-assessment checklist.

### 18.2 Phased Improvement

The Board recognises that smaller regulated entities may require a phased approach to achieving full baseline compliance. Regulated entities should aim to address gaps in consumer-facing digital services, emergency systems, cybersecurity baseline, encryption, and data backup as priority areas before progressively addressing governance, lifecycle management, and internal business systems. Regulated entities with limited in-house IT capacity are encouraged to leverage managed IT service providers, outsourced IT support, or shared service arrangements to supplement their internal capability in meeting these baseline requirements. Smaller CGD entities are encouraged to refer to Annexure C of these Guidelines, which provides indicative minimum technology configurations — including hardware governance principles, operating system, database, GIS software, and API integration stack — to assist them in establishing the foundational IT infrastructure needed for digital operations and regulatory integration.

### 18.3 New Entities and Authorisations

Entities seeking new authorisations from the Board, or commencing operations under an existing authorisation, should ensure that baseline IT infrastructure consistent with these Guidelines is in place from the commencement of commercial operations, or within such period as the Board may specify.

### 18.4 Scalability

As a regulated entity's operations grow — whether through expansion of its geographical area, increase in consumer base, or addition of new infrastructure — its IT systems should be scaled accordingly to continue meeting the baseline standards set out in these Guidelines.

## 19. Reporting to the Board

### 19.1 Annual IT Infrastructure Status Report

Regulated entities are encouraged to include a summary statement on the status of their IT infrastructure — covering any significant gaps, improvements made during the year, planned technology refresh activities, cybersecurity posture, AI governance developments, and significant API or system integration developments — in their annual submissions to the Board, or through such reporting mechanism as the Board may prescribe.

### 19.2 Information on Request

Regulated entities should be in a position to provide the Board with information on their IT infrastructure status, consumer-facing digital service availability, cybersecurity posture, and IT governance arrangements upon request, including in the context of regulatory inspections or reviews.

## 20. Relation to Other Regulatory Instruments and Laws

These Guidelines complement and should be read together with:

a) Guidelines, circulars, and directions issued by the Ministry of Petroleum and Natural Gas (MoPNG) relating to digital infrastructure, IT governance, cybersecurity, and consumer services in the petroleum and natural gas sector, as issued from time to time;

b) Applicable Technical Standards and Specifications including Safety Standards (T4S) issued by the Board, which govern operational and safety requirements for infrastructure and equipment;

c) Directions, advisories, and guidelines issued from time to time by CERT-In and MeitY;

d) The Guidelines for Indian Government Websites and Apps (GIGW 3.0) issued by the National Informatics Centre, applicable to the design and development of consumer-facing web portals and mobile applications;

e) The MeitY Guidelines for Cloud Selection Framework applicable to cloud procurement by government and public sector entities;

f) The Information Technology Act, 2000, and rules and regulations framed thereunder, including the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011;

g) The Digital Personal Data Protection Act, 2023, and rules framed thereunder, governing the processing and protection of digital personal data;

h) The IEC 62443 series of standards for industrial automation and control system security, which provides the internationally recognised security architecture and lifecycle framework for operational technology environments including SCADA, DCS, and PLCs. The IT/OT security provisions in these Guidelines — including network segmentation, IT/OT separation, DMZ architecture, and OT patch management — are broadly consistent with the Defence-in-Depth approach of IEC 62443; and

i) The NIST Cybersecurity Framework (CSF) 2.0, which organises cybersecurity activities under six functions: Govern, Identify, Protect, Detect, Respond, and Recover. The cybersecurity and governance provisions of these Guidelines implicitly address all six functions, and regulated entities using NIST CSF for their internal security governance may use that framework as an organising lens for implementing these Guidelines.

## 21. Review and Update

21.1 The Board shall review these Guidelines periodically, at least once every three years, to assess their continued relevance and adequacy in light of technological developments, changes in the sector, and evolving regulatory requirements. The Board may also initiate an earlier review if significant developments in the cybersecurity or AI landscape — including material updates to CERT-In directions, NCIIPC guidance, or sector-specific cybersecurity guidelines issued by MoPNG — warrant an earlier revision of these Guidelines.

21.2 The Board may, based on experience with implementation, issue supplementary guidance, clarifications, or indicative good practice notes to assist regulated entities in meeting the baseline standards described herein.

21.3 Regulated entities, industry associations, and other stakeholders are encouraged to provide feedback on the implementation experience to the Board, which shall be considered in the course of periodic reviews.

# ANNEXURE A

## Indicative Self-Assessment Checklist

The following checklist is provided to assist regulated entities in conducting a self-assessment of their IT infrastructure against the baseline standards set out in these Guidelines. This checklist is indicative and not exhaustive.

| # | Baseline Requirement | Status (Met / Partial / Not Met) | Action / Remarks |
|---|---|---|---|
| **A** | **NETWORK AND CONNECTIVITY** | | |
| A1 | Reliable internet connectivity at all principal offices | | |
| A2 | Redundant communication links for mission-critical functions | | |
| A3 | IT/OT network separation with appropriate controls (firewall / DMZ / data diode) | | |
| A4 | Secure remote access arrangements in place | | |
| **B** | **COMPUTING INFRASTRUCTURE** | | |
| B1 | Adequate server and computing capacity for operations | | |
| B2 | UPS/power backup for critical IT infrastructure | | |
| B3 | Cloud usage governed by SLAs, data residency compliance, MeitY empanelment (PSUs) | | |
| B4 | Server rooms and equipment spaces cooled and temperature-monitored; physical access restricted to authorised personnel; fire detection in place | | |
| B5 | Cloud IAM controls in place; encryption key management documented; continuous cloud security monitoring active | | |
| B6 | Infrastructure and application monitoring in place; escalation matrix documented | | |
| **C** | **DATA MANAGEMENT** | | |
| C1 | Data retention policy documented and in effect | | |
| C2 | 3-2-1-1 backup strategy (or equivalent) adopted for critical data | | |
| C3 | Backup restoration tested periodically | | |
| C4 | Data integrity controls on consumer and billing records | | |
| C5 | Consumer data handled per DPDP Act 2023 and IT Act Rules | | |
| C6 | Data governance framework in place: data ownership defined, data quality monitored, data lineage maintained for regulatory data | | |
| C7 | Aadhaar-based KYC handled per UIDAI regulations; entity registered as AUA/KYC User Agency where applicable | | |
| **D** | **CONSUMER-FACING DIGITAL SERVICES** | | |
| D1 | Consumer portal / mobile app operational | | |
| D2 | Online new connection application and tracking available | | |
| D3 | Digital billing and payment capability available | | |
| D4 | Digital grievance registration and tracking available | | |
| D5 | 24×7 emergency helpline operational | | |
| D6 | Portal aligned with GIGW 3.0 / WCAG 2.1 accessibility standards | | |

| # | Baseline Requirement | Status (Met / Partial / Not Met) | Action / Remarks |
|---|---|---|---|
| D7 | Multi-channel consumer communication capability in place (minimum email + SMS); consumer consent recorded per DPDP Act | | |
| **E** | **METERING AND OPERATIONAL SYSTEMS** | | |
| E1 | Metering data managed digitally with adequate traceability | | |
| E2 | Metering data integrated with billing system | | |
| E3 | Operational monitoring system (SCADA/DCS) in place as required by T4S | | |
| **F** | **REGULATORY REPORTING** | | |
| F1 | IT systems capable of generating required regulatory reports | | |
| F2 | API-based integration capability for PNGRB reporting systems | | |
| F3 | Audit trails maintained for regulatory data submissions | | |
| F4 | Accounting software has audit trail feature per Companies (Accounts) Amendment Rules 2014 (for company entities) | | |
| **G** | **CYBERSECURITY BASELINE** | | |
| G1 | Compliant with applicable CERT-In directions | | |
| G2 | MoPNG sector-specific cybersecurity guidelines assessed and being implemented | | |
| G3 | Designated CISO (or equivalent) in place with documented responsibilities | | |
| G4 | CERT-In incident reporting process documented (6-hour reporting) | | |
| G5 | Information security programme in place (per IT Act Rules) | | |
| G6 | RBAC implemented; MFA enforced for remote and privileged access | | |
| G7 | Endpoint protection deployed on IT assets | | |
| G8 | Network perimeter security (firewalls, monitoring) in place | | |
| G9 | Sensitive data encrypted at rest and in transit (TLS for APIs and submissions) | | |
| G10 | ICT logs retained for prescribed period; NTP synchronisation configured | | |
| G11 | Annual VAPT by CERT-In empanelled auditors; findings remediated | | |
| G12 | Cybersecurity awareness training (incl. AI threats, deepfakes) conducted | | |
| G13 | Tabletop exercises / cyber drills conducted periodically | | |
| G14 | Third-party/vendor cybersecurity obligations documented | | |
| G15 | SOC capability established or access obtained (esp. for large/CII entities); security events monitored continuously | | |
| **H** | **AI GOVERNANCE** | | |
| H1 | AI usage policy defined and communicated to staff | | |
| H2 | AI asset inventory maintained | | |
| H3 | Risk assessment conducted before AI deployment in sensitive contexts | | |

| # | Baseline Requirement | Status (Met / Partial / Not Met) | Action / Remarks |
|---|---|---|---|
| H4 | Human oversight in place for AI-assisted critical decisions | | |
| H5 | Restrictions on uploading sensitive data to public AI platforms | | |
| H6 | AI transparency and explainability mechanisms in place for high-stakes AI outputs affecting consumers or regulatory submissions | | |
| H7 | Continuous monitoring of AI systems operational; model drift and anomalous outputs tracked and reviewed | | |
| **I** | **SYSTEM LIFECYCLE AND TECHNOLOGY REFRESH** | | |
| I1 | Technology lifecycle policy documented | | |
| I2 | IT hardware refresh plan in place for critical systems | | |
| I3 | End-of-life software identified and migration planned | | |
| I4 | OT/SCADA lifecycle and modernisation plan maintained | | |
| I5 | Budgetary provision made for technology refresh | | |
| **J** | **INTEROPERABILITY AND API INTEGRATION** | | |
| J1 | Core systems (billing, metering, ERP) have API capability | | |
| J2 | GIS data maintained in standard interchange formats | | |
| J3 | API security controls in place (auth, TLS encryption, logging) | | |
| J4 | Third-party integration register maintained | | |
| J5 | Consumer data exportable in structured format | | |
| **K** | **IT GOVERNANCE** | | |
| K1 | Senior IT official designated with clear responsibilities | | |
| K2 | Designated CISO (or equivalent) in place with documented responsibilities | | |
| K3 | Documented IT policies (incl. AI usage, access, backup, vendor, incident) | | |
| K4 | IT and API asset inventory maintained | | |
| K5 | Vendor/third-party IT SLAs in place | | |
| K6 | Change management process in place for critical systems | | |
| K7 | Enterprise architecture documentation maintained (application, infrastructure, data, security architecture) — esp. for larger entities | | |
| **L** | **BUSINESS CONTINUITY AND DISASTER RECOVERY** | | |
| L1 | Business Continuity Plan (BCP) documented and tested | | |
| L2 | Disaster Recovery plan documented and tested (incl. backup restoration) | | |
| L3 | Manual fallback procedures documented for critical functions | | |
| L4 | RPO and RTO defined for critical systems | | |
| **M** | **SOFTWARE MANAGEMENT** | | |
| M1 | All software licensed and under vendor support | | |
| M2 | Security patch/update process in place | | |
| **N** | **IT HUMAN RESOURCES** | | |

| # | Baseline Requirement | Status (Met / Partial / Not Met) | Action / Remarks |
|---|---|---|---|
| N1 | Dedicated IT function or managed IT support in place | | |
| N2 | IT staff trained for their roles | | |
| N3 | Basic digital literacy training provided to operational staff | | |

Regulated entities are advised to retain completed self-assessment records for internal governance and for submission to the Board if requested.

# ANNEXURE B

## Glossary of Abbreviations

| Abbreviation | Full Form |
|---|---|
| | |
| AUA | Authentication User Agency (registered with UIDAI under the Aadhaar framework) |
| BCP | Business Continuity Plan |
| BITIG | Baseline IT Infrastructure Guidelines |
| CGD | City Gas Distribution |
| CIGU | CERT-In Guideline/Advisory (document series prefix) |
| CPU | Central Processing Unit |
| DCS | Distributed Control System |
| DMZ | Demilitarised Zone |
| GIGW | Guidelines for Indian Government Websites and Apps |
| ICT | Information and Communications Technology |
| KYC | Know Your Customer |
| LLM | Large Language Model |
| LNG | Liquefied Natural Gas |
| MFA | Multi-Factor Authentication |
| NGPL | Natural Gas Pipeline |
| NIC | National Informatics Centre |
| OEM | Original Equipment Manufacturer |
| OT | Operational Technology |
| OWASP | Open Web Application Security Project |
| PLC | Programmable Logic Controller |
| PostGIS | A spatial database extender for PostgreSQL |
| QGIS | Quantum GIS — an open-source Geographic Information System |
| RAM | Random Access Memory |
| RBAC | Role-Based Access Control |
| SOC | Security Operations Centre |
| SPDI Rules | Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 |
| T4S | Technical Standards and Specifications including Safety Standards |
| TLS | Transport Layer Security |
| UIDAI | Unique Identification Authority of India |
| UPS | Uninterruptible Power Supply |
| VAPT | Vulnerability Assessment and Penetration Testing |
| WCAG | Web Content Accessibility Guidelines |

# ANNEXURE C

## Indicative Minimum Technology Baseline for Smaller CGD Entities

This Annexure is provided as a practical reference to assist smaller City Gas Distribution (CGD) entities — particularly those newly authorised or operating in developing Geographical Areas — in establishing the minimum technology infrastructure necessary to carry out digital operations, API integration with PNGRB systems, and compliance with applicable regulatory requirements.

This Annexure is indicative and illustrative in character. It does not impose any mandatory product or vendor requirements. Regulated entities retain full discretion to select any technology that meets the functional objectives described. Open-source options are highlighted wherever they provide a cost-effective and technically adequate alternative, which is particularly relevant for smaller entities with limited IT budgets.

> **Note:** The configurations described in this Annexure represent a suggested starting point. Entities should assess their actual consumer base, operational footprint, and regulatory obligations when dimensioning their infrastructure, and should scale up as operations grow consistent with Guideline 18.4.

### C.1 Purpose and Scope

This Annexure covers the following areas of the technology baseline for smaller CGD entities:

1. Minimum hardware configuration
2. Operating system selection
3. Database management system
4. Geographic Information System (GIS) software
5. API integration stack
6. Consumer portal and business application software

### C.2 Hardware Infrastructure — Functional Adequacy and Governance Principles

Hardware configurations depend on the specific consumer base, transaction volumes, and operational complexity of each entity, and any prescribed figure would quickly become technically outdated. No regulatory framework or government body in India specifies minimum hardware configurations in terms of processor cores, RAM, or storage capacity, and BITIG follows the same practice. Instead, regulated entities should dimension their computing infrastructure according to the following functional adequacy and hardware governance principles, which are consistent with the approach taken by CERT-In, NIC, and comparable regulatory frameworks:

i. Capacity proportionate to operational scale: servers, workstations, networking equipment, and storage should be of sufficient capacity to support peak consumer portal sessions, concurrent API transactions, metering data ingestion, and database operations without sustained performance degradation. Regulated entities should assess their capacity requirements against their current and projected consumer base and plan accordingly, scaling up as operations grow consistent with Guideline 18.4;

ii. Resource utilisation monitoring and capacity planning: regulated entities should monitor the utilisation of critical hardware resources — including CPU, RAM, disk space, and network throughput on servers — on an ongoing basis, and maintain projections for upgrade requirements to ensure adequate processing power and storage are available before constraints affect service delivery;

iii. Hardware hardening before commissioning: all hardware — including servers, networking equipment, firewalls, switches, and end-user devices — should be hardened before being commissioned for use in the production environment. Hardening includes: changing all default usernames and passwords immediately upon commissioning; disabling or removing unused services, ports, and protocols; disabling unused physical ports (USB, network) where not operationally required; and configuring the

device in accordance with the OEM's security recommendations. These requirements are consistent with CERT-In and NIC guidance on secure configuration of IT infrastructure;

iv. Active vendor support lifecycle: hardware deployed on critical functions should be from vendors providing an active maintenance and support lifecycle. End-of-life hardware — for which the OEM has ceased to provide firmware updates, security patches, or technical support — should not be used on critical workloads, consistent with Guideline 13.2; and

v. NTP synchronisation: all servers and networked IT systems should be configured to synchronise their system clocks with an authoritative time source. Regulated entities are directed to use the NIC-designated NTP servers — samay1.nic.in and samay2.nic.in — as their primary and secondary NTP sources, consistent with the guidelines issued by NIC and CERT-In for government and regulated entities. Accurate time synchronisation is essential for the forensic integrity of ICT logs and for the correct timestamping of transactions and regulatory submissions. As an indicative benchmark, system clocks should be synchronised to within 1 second of the NIC reference time, and synchronisation status should be monitored with alerts configured for drift exceeding this threshold.

**Note:** *For entities using cloud infrastructure, hardware sizing is managed by the cloud service provider. Regulated entities using cloud services should select instance types appropriate to their workload requirements, monitor resource utilisation through cloud provider dashboards, and ensure that auto-scaling or instance upgrade provisions are in place for consumer-facing systems.*

### C.3 Operating System

The operating system (OS) forms the foundation of all server and workstation infrastructure. Regulated entities should select an OS that:

i. Has an active Long-Term Support (LTS) or equivalent lifecycle from the vendor, ensuring continued security patch availability;

ii. Is supported by the business applications (ERP, billing, GIS, database) that the entity intends to deploy; and

iii. Is within the technical competence of the entity's IT staff or managed service provider.

Indicative options:

| Option | Notes |
|---|---|
| Ubuntu LTS (Linux) | Recommended open-source option for server infrastructure. Well-supported, widely used for enterprise applications, and free to use. Current LTS versions have five-year support cycles. Suitable for hosting PostgreSQL, web servers, and API middleware. |
| RHEL / Rocky Linux / AlmaLinux | Enterprise Linux distributions. Rocky Linux and AlmaLinux are free, binary-compatible alternatives to RHEL, suitable for entities preferring a RHEL-compatible environment without licence cost. |
| Windows Server | Widely used commercial option, appropriate where the entity's business applications (billing, ERP) require a Windows environment or where staff skillsets favour it. Licencing cost should be factored into the infrastructure budget. |

*End-of-Life OS*: Entities should not run end-of-life OS versions (e.g. Windows Server 2008 and 2008 R2, Windows Server 2012 and 2012 R2, Ubuntu 21.x or older, Red Hat Enterprise Linux (RHEL) 7, CentOS Linux, etc.) on internet-connected or consumer-facing systems. Migration to supported versions is required consistent with Guideline 13.3.

### C.4 Database Management System

A reliable, well-supported database management system (DBMS) is essential for storing consumer records, metering data, billing transactions, and regulatory reporting data. The DBMS must support API-based data exchange and should be capable of handling the entity's transaction volumes with appropriate performance and data integrity.

PostgreSQL is the recommended open-source database for smaller CGD entities, for the following reasons:

i. It is free and open-source, removing licence barriers for smaller entities;
ii. It is enterprise-grade, ACID-compliant, and actively maintained with a long-established support community;
iii. The PostGIS extension to PostgreSQL is the leading open-source geospatial database engine, enabling CGD entities to store and query pipeline network coordinates, consumer location data, and infrastructure asset positions directly within the database;
iv. It natively supports JSON and JSONB data types, making it well-suited for REST API integration and data exchange with PNGRB regulatory systems; and
v. It runs on all major operating systems including Linux and Windows.

Commercial database alternatives — including, for example, MySQL Community Edition / MariaDB (open-source), Microsoft SQL Server, and Oracle Database — are equally acceptable where they meet the entity's functional requirements and the entity has the appropriate licencing and support arrangements in place.

> **Note:** For CGD entities maintaining gas network GIS data, the PostGIS extension to PostgreSQL is strongly recommended as the geospatial database backend. PostGIS adds support for geographic objects including pipeline routes, valve locations, pressure monitoring points, and consumer connection points, and is compatible with both QGIS and ESRI ArcGIS as front-end GIS tools.

### C.5 Geographic Information System (GIS) Software

GIS capability is essential for CGD entities. Gas distribution networks must be spatially mapped for operational management, emergency response, regulatory compliance, and submission of network data to the Board. A functional GIS enables entities to:

i. Map and manage gas pipeline routes, valve locations, pressure regulation stations, and consumer connection points;
ii. Conduct spatial analysis for network expansion planning and fault isolation;
iii. Maintain network data in standard formats for regulatory reporting and API-based data exchange with PNGRB systems; and
iv. Support field operations using mobile GIS applications for on-site asset inspection and data collection.

Indicative GIS software options:

| Option | Notes |
|---|---|
| QGIS (open-source) | QGIS is a free, open-source desktop GIS application that is fully capable for CGD network management. It supports all standard geospatial data formats (Shapefile, GeoJSON, GeoPackage, PostGIS), integrates directly with PostgreSQL/PostGIS, and has an active developer community. QGIS is recommended as the primary GIS option for smaller CGD entities given zero licence cost and functional adequacy for the required tasks. |

| | |
|---|---|
| ESRI ArcGIS | ArcGIS is the industry-leading commercial GIS platform, providing advanced spatial analysis, 3D modelling, enterprise web GIS, and mobile field data collection capabilities. It is appropriate for larger regulated entities or those requiring advanced spatial analytics beyond basic network management. The licence cost is significant and should be factored into the IT budget accordingly. |

Irrespective of the GIS software selected, regulated entities should maintain their network GIS data in standard open interchange formats — GeoJSON, Shapefile, GeoPackage (GPKG), or equivalent — to ensure portability, interoperability with PNGRB systems, and compatibility with future platform changes, consistent with Guideline 14.1.

### C.6 API Integration Stack

API integration capability is necessary for regulated entities to exchange data with PNGRB's regulatory reporting systems, payment gateways, government platforms, and smart metering infrastructure. The following components constitute an adequate API integration stack for a smaller CGD entity:

| Component | Description and Indicative Options |
|---|---|
| Web / Application Server | A web server to host the entity's consumer portal, APIs, and application services. Apache HTTP Server and Nginx are widely-used, free, open-source options. Both are suitable for hosting REST API endpoints and web portals on Linux servers. |
| Transport Layer Security (TLS) | All API communications and consumer portal traffic must be transmitted over HTTPS using TLS 1.2 or higher. A valid SSL/TLS certificate from a recognised Certificate Authority must be installed and kept current. Free certificates are available through services such as Let's Encrypt. |
| API Framework / Middleware | A lightweight API framework to develop and expose REST APIs. Options include Spring Boot (Java), Django REST Framework (Python), or Express.js (Node.js), all of which are open-source and widely used for building government and utility APIs. |
| Data Exchange Format | JSON (JavaScript Object Notation) is the standard data exchange format for REST APIs and is recommended for all API integrations with PNGRB systems. GeoJSON should be used for spatial / GIS data exchange. |
| API Gateway (Optional but recommended) | An API gateway manages authentication, rate-limiting, logging, and routing for multiple API endpoints. Open-source options include Kong and WSO2 API Manager. For smaller entities, a basic reverse proxy (Nginx) with authentication can serve this function initially. |
| API Documentation | APIs exposed by the entity should be documented using the OpenAPI / Swagger specification standard. |
| Authentication | API access should be secured using OAuth 2.0, API keys, or equivalent token-based authentication. Credentials and tokens should be stored securely and rotated periodically. |

### C.7 Consumer Portal and Business Application Software

Smaller CGD entities should, as a minimum, have the following application software in place to support consumer services and operational management:

| Application Area | Indicative Options |
|---|---|
| Consumer Billing and Management | Commercial CGD billing software packages are available from several vendors with sector-specific functionality. Entities should ensure the selected package supports API connectivity, data export in standard formats, and integration with payment gateways. |
| ERP / Financial Accounting | Open-source ERP options such as Odoo (Community Edition) and ERPNext provide financial accounting, procurement, HR, and asset management capabilities at no software licence cost, and are suitable for smaller CGD entities. Commercial alternatives (SAP, Oracle, Zoho, Tally) are equally acceptable. |
| Consumer Portal (Web) | The consumer portal may be developed on widely-used open-source content management or web application frameworks. It should comply with GIGW 3.0 guidelines and WCAG 2.1 accessibility standards as noted in Guideline 8.5. |
| Mobile Application | A mobile application for consumer self-service may be developed natively (Android / iOS) or as a Progressive Web App (PWA). PWA is a cost-effective option for smaller entities as it does not require separate native app development. |
| Grievance Management | Grievance management functionality may be integrated into the consumer portal or provided through a standalone helpdesk system. Open-source options include Zammad and Request Tracker. |
| GIS / Network Management | As described in C.5 above. |

Regulated entities are encouraged to consult NIC, STQC, or CERT-In empanelled technology advisors when establishing their initial IT infrastructure, to ensure that the selected technology stack meets applicable security, interoperability, and data residency requirements.

**Issued by the Petroleum and Natural Gas Regulatory Board**
New Delhi | 2026