B-Ready FAQs
Utility Services- Internet

1.1 REGULATORY OVERSIGHT OF TARIFF SETTING AND SERVICE QUALITY

B-Ready assessment area	Relevant Provisions	Link
Regulatory authority- Initiate investigations for Anticompetitive Practices	Chapter II of TRAI Prohibition of Discriminatory Tariffs for Data Services Regulations, 2016 takes measure to facilitate competition and promote efficiency in telecom sector.	https://trai.gov.in/sites/default/files/2024-09/Regulation_08022016_0.pdf
Regulatory authority- Impose fines for Monitoring of Anticompetitive Practices	As per Chapter III of TRAI Prohibition of Discriminatory Tariffs for Data Services Regulations, 2016, there is a provision of fine/ penalty for anti-competitive practices.	https://trai.gov.in/sites/default/files/2024-09/Regulation_08022016_0.pdf
Service Quality Assurance- Adherence to Performance Standards	Regulation 4, The Quality of Service of Broadband Service Regulations 2006. TRAI has mandated that service providers shall submit performance monitoring reports on Quarterly basis and the same reports are published on TRAI's website. The service providers shall submit Report on QoS benchmarks for all the parameters in the format to be prescribed by the Authority on Quarterly basis, ending 31st March, 30th June, 30th September and 31st December, but not later than 6 weeks from the end of the Quarter. The Authority may review from time to time the periodicity and the format of such report.	-
Service Quality Assurance- Penalties for Breaches of Reliability Obligations	As per Regulation 3A(1) of Quality of Service of Broadband Service Regulations 2006, If service provider providing broadband service fails to meet benchmark of QoS parameter in S.No.i to viii of regulation (3), it shall, without prejudice to T&C of its licence/Act/rules/regulations/orders/direction, be liable to pay amount, by way of financial disincentive, upto Rs.50,000/parameter & for second/subsequent contravention, upto Rs. 1,00000/parameter for each contravention, as Authority may, by order direct. Provided that no order for payment shall be made by Authority unless service provider providing broadband service has been given reasonable opportunity of representing against contravention of regulation observed by Authority.	-

1.2 REQUIREMENTS ON COORDINATION IN INTERNET CONNECTIONS AND INFRASTRUCTURE DEVELOPMENT

B-Ready assessment area	Relevant Provisions	Link
Joint Planning and Construction- Provisions on adherence to common excavation plans or "dig once" policies	Regulation 3, Indian Telegraph Infrastructure Safety Rule, 2023. CBuD App is available and the website. Indian Telegraph Infrastructure Safety Rule, 2023 were notified on 03.01.2023. Regulation 3 deals with joint Planning and coordination- The licensee shall, on submission of notice by the person under sub-rule (1), as expeditiously as possible provide through the common portal, the details of telegraph infrastructure owned or control or managed by such licensee, falling under or over or along the property with which the person intends to deal in legal exercise of the right, along with precautionary measures for coordination in avoiding damages to the telegraph infrastructure.	https://cbud.gov.in https://www.dot.gov.in/static/uploads/2025/07/a003a544173b6fb436eef06b238a1871.pdf
Joint Planning and Construction- Timelines for approval processes	Table 1, Citizen Charter of DoT, 2024 Timelines are defined for issuance of various licenses on joint construction of infrastructure through Saral Sanchar Portal. Time Limit for approval of Infrastructure Provider (IP-I) License which is obtained for construction of Infrastructure is 1 month, as given in Point 2 of Citizen Charter issued by DoT (Page 5 of 14). Issue of Letter of Intent (LOI) after compliance of all objections / shortcomings in the application (subject to submission of complete details for clearance from security angle and actual clearance by IMC for GMPCS authorization) is issued within 60 days. All other timelines of different authorization and clearances are defined on the website of DOT.	https://www.dot.gov.in/static/uploads/2025/07/efa24d7f27b3a82547cad588e0280414.pdf
Rights of Way Regulations on equal access to government-owned infrastructure	Section 13 of the Telecommunication Act, 2023 have the provisions of non-exclusive and non-discriminatory provisions. Any person providing right of way under section 11 or section 12, shall ensure grant of right of way to the facility providers in a non-discriminatory manner and, as far as practicable, on a non-exclusive basis.	https://egazette.gov.in/WriteReadData/2023/250880.pdf
Rights of Way Regulations on rights of way for digital infrastructure service providers	Section 2(h) & (o), RoW Rules, 2024 are meant for overground and underground telecom network which includes Mobile Tower, Optical Fiber, Posts, Poles etc. As per section 2(h) and 2(o) of DoT Nitification dated 17th September 2024. All these are also meant for Digital Infrastructure Providers.	https://eservices.dot.gov.in/sites/default/files/circular-notifications/Telecommunications%20Right%20of%20Way%20Rules%202024.pdf
Open Infrastructure Passive or active infrastructure	Clause 33, License Agreement for Unified License Agreement, 2024 There are enabling provisions in Unified License (UL) Agreement to deal with subject of passive and active (up to a limited extent) infrastructure sharing. However, infrastructure sharing is not obligatory for operators. Related clauses of UL- 33.1	https://www.dot.gov.in/static/uploads/2025/08/d3bc8ffcf20cef4d9a0fd7d47e6ec7da.pdf

B-Ready assessment area	Relevant Provisions	Link
sharing between broadband operators	Sharing of active/passive infrastructure shall be governed by terms and conditions of respective service authorization and guidelines to be issued by Licensor from time to time; 33.3. Licensee may share its own passive infrastructure for providing other services authorized to it under any other telecom license issued by Licensor; 4. Authorized Gateway hub operated by satellite provider itself is permitted to be shared with satellite bandwidth seeker.	
Open Infrastructure Local loop unbundling and line access	Clause 33, License Agreement for Unified License Agreement, 2024 In India, local loop unbundling (LLU) as part of passive infrastructure sharing is permitted as per extant licensing regime on mutual agreement basis between TSPs and there is no restrictions on LLU. However, it is not mandatory. It depends upon various TSPs operating in Indian Telecom sector to share each other's access network as per their requirement. Govt. has provided enabling conditions in licensing regime however it neither mandates nor restrict. Clause 33 of Unified License allows sharing of RAN, transmission systems, and Wi-Fi equipment. Clause 38 prohibits exclusive contracts for public networks. Proposed amendments to Model Building Bye-Laws ensure fair, non-exclusive access to telecom infrastructure in buildings.	https://www.dot.gov.in/static/uploads/2025/08/d3bc8ffcf20cef4d9a0fd7d47e6ec7da.pdf
Asymmetric regulations for dominant carriers	Clause 11(a)(iv), TRAI Act, 1997 As per the Clause 11(a)(iv) of Chapter –III of the TRAI Act, TRAI takes measure to facilitate the competition and promote efficiency in telecom sector. And there is no monopoly, as such sufficient players are active in Data services.	https://www.trai.gov.in/sites/default/files/2024-10/The_TRAI_Act_1997.pdf

1.3 CYBERSECURITY REGULATIONS

B-Ready assessment area	Relevant Provisions	Link
Liability Regimes-Liability and a legal right to pursue compensation for personal data protection breaches	There are provisions for Penalty, Punishment regarding Data Protection. The Telecommunications Act, 2023 (Chapter IX, Section 42) stipulates liability for personal data breaches. It includes penalties up to ₹2 crore and imprisonment up to 3 years for unauthorized access, data interception, or personation. Clause 42(5) also provides for compensation for damage to telecom networks. Additionally, Clause 37.1 of the Unified License Agreement mandates licensees to protect subscriber data and comply with legal provisions, reinforcing the regulatory framework for personal data protection.	https://www.dot.gov.in/static/uploads/2025/07/f9cded65465151e5743f10ec386f3ad9.pdf https://www.dot.gov.in/static/uploads/2025/08/d3bc8ffcf20cef4d9a0fd7d47e6ec7da.pdf
Liability Regimes-Provisions on data breach incident reporting	Section 7, Telecommunications (Telecom Cyber Security) Rules, 2024. CERT-In is designated nodal agency & has issued directions to report any Cyber security incident within 6 hours to CERT-In. Telecommunications (Telecom Cyber Security) Rules, 2024 defines Reporting of security incidents in section 7- (1) On occurrence of any security incident affecting telecom entity, such entity shall report same to CG within 6 hours of such occurrence in form & manner specified, incl furnishing of info: (a) number of users affected (b) duration (c) geographical area affected(d) extent to which functioning of telecom network/service is affected (e) extent of impact on economic & societal activities (f) remedial measures taken or proposed to be taken.	https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf; https://www.cert-in.org.in/PDF/FAQs_on_CyberSecurityDirections_May2022.pdf ; https://www.cert-in.org.in/PDF/CERT-In_directions_extension_MSMEs_and_validation_27.06.2022.pdf ; https://www.dot.gov.in/static/uploads/2025/07/7922e64b2a1ea70363e1b66970df52f5.pdf
Cybersecurity Coordination-Carrying out risk-assessment strategies	Para 2, IT Amendment Act, 2008; Section 8 & 9, Information Technology (The Indian Computer emergency response team and manner of performing function and duties) Rules, 2013 Yes. Indian Computer Emergency Response Team (CERT-In) is national agency for cyber security in India. In the Roles and function section of the website, it has been defined that CERT-iN undertakes risk analysis.	https://www.cert-in.org.in/PDF/G.S.R_20(E).pdf ; https://www.cert-in.org.in/PDF/act301009.pdf ; https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_1517807324077&type=rule&filename=the_indian_computer_emergency_response_team_rule_2013.pdf ;

B-Ready assessment area	Relevant Provisions	Link
		https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf ; https://dotws.cdot.in/sites/default/files/20230628_T-CSIRT_%20DoT.pdf
Cybersecurity Coordination - Carrying out cybersecurity audits, drills, exercises, or trainings	Para 2, IT Amendment Act, 2008; Section 8 & 9, Information Technology (The Indian Computer emergency response team and manner of performing function and duties) Rules, 2013. Central Government in terms of the provisions of sub-section (1) of section 70B of Information Technology (IT) Act, 2000 (IT Act, 2000) has appointed "Indian Computer Emergency Response Team (CERT-In)" vide notification dated 27th October 2009 published in the official Gazette and as per provisions of sub-section (4) of section 70B of IT Act, 2000 The Indian Computer Emergency Response Team shall serve as the national agency for performing the functions in the area of cyber security.	https://www.cert-in.org.in/PDF/G.S.R_20(E).pdf ; https://www.cert-in.org.in/PDF/act301009.pdf ; https://www.cert-in.org.in/PDF/Comprehensive_Cyber_Security_Audit_Policy_Guidelines.pdf ; https://www.cert-in.org.in/
Cybersecurity Coordination- Leading collective efforts against cyber threats	Clause 11, Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 Clause 11 of Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 specifies involvement of both public and private stakeholders in handling cybersecurity incidents.	https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_1517807324077&type=rule&filename=the_indian_computer_emergency_response_team_rule_2013.pdf
Cybersecurity Coordination - Enforcing cybersecurity laws and regulations	Section 8 & 9, Information Technology (The Indian Computer emergency response team and manner of performing function and duties) Rules, 2013 Central Government in terms of the provisions of sub-section (1) of section 70B of Information Technology (IT) Act, 2000 (IT Act, 2000) has appointed "Indian Computer Emergency Response Team (CERT-In)" vide notification dated 27th October 2009 published in the official Gazette and as per provisions of sub-section (4) of section 70B of IT Act, 2000 The Indian Computer Emergency Response Team shall serve as the national agency for performing the functions in the area of cyber security.	https://www.cert-in.org.in/PDF/G.S.R_20(E).pdf ; https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf
Cybersecurity protection or	Section 70B(6), Information Technology Act, 2000 Yes , regulatory framework establish mandatory cybersecurity standards and	https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf

B-Ready assessment area	Relevant Provisions	Link
minimum standards and safeguards	cybersecurity safeguards. As per directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents, cyber incidents are required to be reported to CERT-In which can be seen at https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf	
Computer Security Incident Response Teams	Section 70B(6), Information Technology Act, 2000 Yes, As per directions under section 70B (6) of Information Technology Act, 2000 relating to information security practices, procedure, prevention, response & reporting of cyber incidents, required to be reported to CERT-In. Rule 12(1) of Information Technology (Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rule, 2013 defines how to report incidence. CERT-In, MeitY formulated Cyber Crisis Management Plan (CCMP) for countering cyber-attacks and cyber terrorism for implementation by all Ministries/Departments of Government and organizations under their administrative control. Also, CERT-In developed "Guidance Framework for CCMP" may be used as template to prepare & implement their own CCMP	https://cert-in.org.in/s2cMainServlet?pageid=CCMP) https://pib.gov.in/PressReleasePage.aspx?PRID=1565959#:~:text=The%20Cyber%20Crisis%20Management%20Plan%20%28CCMP%29%20for%20Countering,states%20and%20critical%20organizations%20operating%20in%20Indian%20cyberspace ; https://rbi.org.in/Scripts/NotificationUser.aspx?ID=10435 ;

1.4 ENVIRONMENTAL SUSTAINABILITY

B-Ready assessment area	Relevant Provisions	Link
Environmental Reporting or Disclosure Standards for Digital Connectivity Infrastructure	Para 2(iii), DoT directions 16-06/2011-CS-III, 2019 In order to achieve the objectives of Green Telecom and reduce the carbon footprint, Telecom Regulatory Authority of lndia (TRAI) had issued recommendations on" Approach towards Sustainable Telecommunications". Government of lndia has considered the TRAI recommendations and decided for setting up of procedures for measurement of carbon footprint and implement carbon emission reduction targets. Accordingly, DoT issued to the licensees for implementation with immediate effect. The Service providers shall submit the Carbon Footprint report to DGT Wing on self certification basis	https://dot.gov.in/sites/default/files/Sustainable%20Tekecommunications_0.pdf?download=1
Emissions and Energy Efficiency of Digital Connectivity Infrastructure	Para-2(xiii), DoT Order No.16-06/2011-CS-III on the subject “Approach towards Sustainable Telecommunications dated 7th January, 2019 DoT has released order reg “Approach towards Sustainable Telecommunications” : - “Target for reduction in ‘Average Carbon Emission (tonnes of CO2e per unit Petabyte as per v above)’ shall be 30% by year 2019-20 and 40% by year 2022-23, taking base year as 2011-12. Targets shall be reviewed in year 2022-23.” Target for reduction in average carbon emission is given up to year 2022-23 in above order and now, targets are under review. 2. Draft "National telecom Policy-2025" under "Mission 6:Sustainable Development" has following goals: a. Reduce carbon footprint from telecom service sector by 30%; b. Achieve renewable energy adoption for 30% of telecom towers.	https://dms.dot.gov.in/sites/default/files/Sustainable%20Tekecommunications_0.pdf?download=1
Emissions and Energy Efficiency of Digital Connectivity Infrastructure	Chapter 7-9, Energy Conservation Building Code (ECBC), 2017	-

2.1 DIGITAL SERVICES AND INTEROPERABILITY

B-Ready assessment area	Relevant Provisions	Link
Electronic Application	Yes, a customer apply for a new commercial internet connection through a fully online process.	https://enterprise.jio.com/Enterprise/myjio-ent/SMB/plans/?type=jbb
Electronic Payments	Yes, it is possible to pay the connection fee for a new fixed broadband connection through electronic payment methods	https://enterprise.jio.com/Enterprise/myjio-ent/SMB/plans/?type=jbb
Information on Existing Infrastructure	GIS Data showing the existing internet network, including the coverage of Jio is available at https://www.jio.com/selfcare/coverage-map/ The similar coverage map is available for other wireless service provider. To find the wireline Internet service provider in areas all over India, the Searchable Service platform- "Know your ISP" is available at https://www.sancharsaathi.gov.in/KnowYourIsp/display-isps.jsp.	-
Information on Planned Works	https://cbud.gov.in/login CBuD mobile app and website are available. App: https://apps.mgov.gov.in/details;jsessionid=6B7F7920EAF6889276881525C11D49D5?apid=1852	-
Obtaining Permits Related to Network Expansion	TSP and ISP apply and obtain Right of Way (RoW) Permission from local authority for installation of conduits and cables on behalf of the customer without customer involvement on the Portal - https://eservices.dot.gov.in/right-of-way-permissions This is mandated by Government of India, as per section 11 and 12 of The Telecommunication Act, 2023 - Any facility provider may submit an application to a public entity / person under whose ownership, control or management, the public property is vested, to seek permissions for right of way for telecommunication network under, over, along, across, in or upon such public property.	-

2.2 MONITORING OF SERVICE SUPPLY IN PRACTICE

B-Ready assessment area	Relevant Provisions	Link
Monitoring of Reliability and Quality of Internet Supply in Practice	TRAI releases data on Key Performance Indicators regarding Quality of Internet services. The TSPs including Jio have to submit the Quarterly report on the established parameters.	https://trai.gov.in/release-publication/reports/wireless-data-reports
Publication of Monitoring of Reliability and Quality of Internet Supply in Practice	https://trai.gov.in/release-publication/reports/wireless-data-reports TRAI releases data on Key Performance Indicators regarding Quality of Internet services.	-

2.3 AVAILABILITY OF INFORMATION AND CUSTOMER NOTIFICATION

B-Ready assessment area	Relevant Provisions	Link
Connection Requirements	The details of steps to get a new commercial internet connection (for example, application submission, payment of fees, site inspection, etc. are provided FAQ part of the website of Jio.	https://www.jio.com/business/services/connectivity/business-internet-line/
Connection time estimates	https://www.jio.com/help/faq/jiofiber/onboarding-installation/installation/how-long-will-it-take-to-activate-my-jiofiber-connection/ The details Connection time estimates are provided FAQ part of the website.	-
Tariff Changes	As per TTO (52nd amendment) issued by TRAI- No service provider shall terminate/change any existing tariff plan without giving a notice of not less than thirty days to the subscriber of its intention to terminate the tariff plan. As per the Screenshot attached, Jio follows the practice of communicating changes in tariff to customers.	Link for TTO amendment is https://www.trai.gov.in/sites/default/files/2024-09/52Fifty_Second_Amendment_19_Sep_2012.pdf
Planned Outages	Jio directly communicates planned internet outages to its customers in advance, through SMS and on My Jio App.	
Complaint Mechanisms	https://www.jio.com/help/contact-us Complaints can be reported to through call or by email as mentioned on the website of Jio.	-
Complaint resolution within a published timeframe	https://myjiostatic.cdn.jio.com/jio/regulatory/rjil-telecom-charter-2025.pdf?downloadPdf=true&pdfname=rjil-telecom-charter-2025.pdf	-
Complaint mechanism independent from the utility to escalate complaints.	The consumer can lodge their complaints at CPGRAMS portal. It is an online platform available to the citizens 24x7 to lodge their grievances to the public authorities on any subject related to service delivery. The status of the grievance filed in CPGRAMS can be tracked with the unique registration ID provided at the time of registration of the complainant. -	https://pgportal.gov.in/

2.4 ENFORCEMENT OF CYBERSECURITY REGULATIONS IN PRACTICE

B-Ready assessment area	Relevant Provisions	Link
In Practice- Carrying out risk-assessment strategies	Chapter 3- Activities and operations of CERT-In Annual Report 2024 states that the Cert-In conducted risk assessment in practice.	https://dgtelecom.gov.in/dgt-hq/; Cert-In - AnnualReport https://www.cert-in.org.in/s2cMainServlet?pageid=PUBANULREPRT
In Practice- Carrying out cybersecurity audits, drills, exercises, or trainings	Chapter 3- Activities and operations of CERT-In Annual Report 2024 states that the Cert-In conducted cybersecurity Audit in practice.	https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf https://www.cert-in.org.in/s2cMainServlet?pageid=PUBANULREPRT
In Practice - Leading collective efforts against cyber threats	Chapter 3- Activities and operations of CERT-In Annual Report 2024 states that the Cert-In works in close coordination to handle cybersecurity incidents.	https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf
In Practice - Enforcing cybersecurity laws and regulations	CERT-IN is the national nodal agency to enforce cybersecurity laws and regulations.	https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf
Operational computer security incident response team	CERT-In is operational and responsible for handling cybersecurity incidents. As per Chapter 3- Activities and operations of CERT-In Annual Report 2024, 2041360 were handled in 2024. -	https://www.cert-in.org.in/s2cMainServlet?pageid=PUBANULREPRT