Annexure-I

Job Descriptions / Nature of experience required for posts

S.No.	Name of the post	Job Descriptions/ Nature of Experience required for posts
1.1	**Deputy Manager (Database Administration)**	1.Installation and configuration of Database. 2.Working in relational database administration like oracle ,PostgreSQL, MySQL, MSSQL. 3. DB optimization, backup ,replication and DR setup. 4. RDB Restoration and data recovery. 5. Performance tuning of database systems 6. Automation of repeating DB tasks 7. Diagnose data base errors 8. Knowledge of NoSQL databases 9 .Excellent verbal, analytical and written communication skills.
1.2	**Manager (Database Administration)**	
1.3	**Senior Manager (Database Administration)**	
1.4	**Deputy Manager (System Administration)**	1. Installation, maintenance & troubleshooting of Linux server based OS and its flavours like RHEL, Ubuntu, SUSE,CentOS etc. AND/OR Installation, maintenance & troubleshooting of Windows server based OS, and Hyper V server administration, including AD,NTP, WINS, DHCP, DNS applications. 2. Strong knowledge of Server Virtualisation, Storage Virtualisation, Cloud Orchestration and experience of VMware Cloud OR Openstack Cloud 3. Provide technical support for server systems. 4. Maintain and review security standards, back-up & replication strategies 5.Performing Vulnerability assessment on a regular basis 6.Perform analysis and investigation on detected malware. 7.Identify potential malicious activity from memory dumps, logs, and packet captures 8.Basic knowledge of scripting language is preferred– Python/ Perl/shell/PHP 9.Excellent verbal, analytical and written communication skills.
1.5	**Manager (System Administration)**	
1.6	**Senior Manager (System Administration)**	
1.7	**Deputy Manager (Security)**	1. Experience in a network administrator and security administrator roles. 2. Hands on experience in networking. 3. Experience with firewalls, UTM,VPN technologies. implementation troubleshooting, and problem resolution is desired 4. Experience in working ondeeep security and end point protection solutions 5.Up-to-date knowledge of cybersecurity threats, current best practices and latest software. 6.Experience in cloud security and full lifecycles implementations 7.Implementing security features and monitoring tools, performing periodic security assessments 8. Managing the development, refresh and implementation of security policies, standards, guidelines and procedures 9. Monitoring and reporting incidents to customers and prepare detail report for that incident. 10. Knowledge on WAF , DLP , IPS , IPS, IDS , SIEM etc 11. Basic Knowledge of SOAR (Security Orchestration, Automation, and Response), programming and scripting will be added advantage. 12. Excellent verbal, analytical and written communication skills.
1.8	**Manager (Security)**	
1.9	**Senior Manager (Security)**	
1.10	**Sr. Manager (IT)**	1. Expert knowledge of professional java frameworks like Spring, hibernate etc. 2. Expert Knowledge in build automation tools like maven. 3. Experience in Async job scheduling platforms like Kafaka/RabbitMQ

		4. Experience in SQL and NoSQL database systems like MySQL, elasticsearch, redis etc. 5. Good hands-on knowledge of Configuration Management and Deployment tools like – Jenkins, Ansible, chef etc 6. Proficient in scripting, Git and Git workflows. 7. Knowledge of web development in node.js,javascript,HTML 8. Expert knowledge in RestAPIs. 9. System admin knowledge (Windows/Linux) is preferred. 10. Knowledge of scripting language– Python/ Perl/shell/PHP.

Note: Job description / nature of experience mentioned above are indicative. The duties and responsibilities of candidates appointed on posts shall not be limiting to these only.

******

Annexure-II

SYLLABUS FOR ALL POSTS/ LEVELS FOR EXAMINATION (if skill test/ written exam is held)

S.No.	Name of Post & Level	Syllabus
1.1	**Deputy Manager (Database Administration)/ E-1 Level**	Core Database concepts, Introduction to Databases and Transactions, Basics of SQL, DDL, DML, DCL, Mandatory Access Control, Data Encryption, Database objects, data storage, data Backup, Data security, Data Model, Database System Concepts and Architecture, Data Modelling Using the Entity-Relationship Model, The Relational Data Model, Relational Constraints, Entity-Relationship and object Modelling, The Relational Database Standard, Query Processing & Query Optimization Database Design, ER-Diagram and Unified Modelling Language, Transaction management and Concurrency control, Relational Algebra and Calculus, Constraints, Views and SQL, SQL Joins, Normalization, Primary Key v/s Foreign Key.
1.2	**Manager (Database Administration)/ E-2 Level**	
1.3	**Senior Manager (Database Administration)/ E-3 Level**	
1.4	**Deputy Manager (System Administration)/ E-1 Level**	Server Planning, Installation, Migration, Configuration, Mail servers, Database servers, Collaboration servers, Monitoring servers, Threat management, Different Type of Operating System Management, Cloud Administration, Understanding of Web services- IIS, WWW, and FTP, installing from Server Manager, separate worker processes, adding components, sites, ports, SSL, certificates. Understanding of file, print services, accounts, groups, Active Directory infrastructure, different storage topologies, local storage, network storage, Fibre Channel, iSCSI hardware, RAID redundancy- RAID 0, RAID 1, RAID 5, RAID 10 and combinations, hardware and software RAID, Solid State Drive (SSD) and Hard Disk Drive (HDD), ATA basic disk, dynamic disk, mount points, file systems, mounting a virtual hard disk, distributed file systems, performance monitoring, logs and alerts, Event Viewer, BIOS, UEFI, TPM, boot sector, bootloader, MBR, boot.ini, POST, Safe Mode, Backup and restore, disaster recovery planning, clustering, AD restore, folder redirection, data redundancy, Software, driver, operating systems, applications, Windows Update, Windows Server Update Service (WSUS), Introduction to Linux, Open Source Development, Linux Security Fundamentals, File System Management, Run levels, Network file system (NFS), XINETD, Domain naming service, Logical volume manager, Package Manager (RPM), Automation of jobs, Fundamentals of APACHE, SQUID, SAMBA.
1.5	**Manager (System Administration)/ E-2 Level**	
1.6	**Senior Manager (System Administration)/ E-3 Level**	

1.7	**Deputy Manager (Security)/ E-1 Level**	• **Physical Security:**
		  • Perimeter Security
		  • Building security
		  • BMS
		  • IOT Security
		• **Hacking**
		  • Types – Script kiddies, Cyber terrorists, White, Grey and Black Hat hackers, Spy hackers, State sponsored hackers, hacktivist
		  • Motives of Hackers: Financial gain, political, causing damage, vendetta by ex-employees, curiosity etc
		  • Vulnerabilities, Exploits, Payloads, backdoors, shells
		  • CVE – Common Vulnerabilities and exposures
		  • CWE – Common Weakness enumeration

1.8	**Manager (Security)/ E-2 Level**	
1.9	**Senior Manager (Security)/ E-3 Level**	

		• Phases of hack – Reconnaissance, Scanning, Enumeration, Gaining access, Maintaining access, Clearing tracks • OSINT Framework • **Network Security** • OSI Model • Topologies • Threat sources – Internal (Employees, accidents, policies), External (Hackers, script kiddies etc) • Types of attacks – DoS, Buffer overflows, Malwares, Social engineering, brute force • Steps in a network attack – Information gathering, Port scanning, Network enumeration, Gaining and keeping admin access, Using the access/information, leaving a backdoor, covering tracks • Security Policy • Audits – Risk assessment, physical security audit, network configuration audit, pen-testing, Backup audit, employee awareness audit • Firewalls, Types of firewalls – packet filtering, application proxy firewalls, Stateful firewall • VPNs • IPS/IDS • Spoofing – TCP, DNS, email • Denial of Service attacks – SYN floods, UDP floods DDoS, Smurf attacks, • Virus Scanners – Host based, Network based • Wireless security • **Introduction and Overview of Cyber security** • Layers of Security – Physical, Personal, Operations, Communications, Computer, Network and Information Security • Vulnerabilities, threats and controls • CIA – Confidentiality, Integrity and Authentication • Software Vulnerabilities – Logic Bomb, Trojan Horse, Virus, Trapdoor, Worm etc • Risk Mitigation techniques • Controls– Encryption, Software, Hardware, Policies, and Physical securities. Types of Controls – preventive, detective, corrective, recovery, deterrent, compensating. • Cyber defense – Network Security Gateway, Firewalls, IDS/IPS, Honeypots, Hardening of Systems with EDR • Password policies • Cryptography – Hashing, Digital Signatures, Digital Certificates • Social Engineering and its types like Phishing, Vishing, Impersonation • **Cryptography** • Need for cryptography – CIA, Non repudiation and Key exchange • Types of cryptography – Symmetric, Asymmetric • Ciphers, Traditional Ciphers – Substitution Ciphers & transposition ciphers • DES – Data encryption standard • AES – Advanced encryption standard • One time pad (OTP)

		• RSA • DIFFIE-HELLMAN Key exchange • Hash, Digital Signature, • Public Key Infrastructure - Certification authority, Registration Authority, Certificate Database, Certificate store • Steganography • IPSec, SSL/TLS, PGP • **IT and Cyber Laws** • IT Act 2008 – background, Civil and Criminal IT offences, Adjudication process, Law of evidence, Cases • IT Act 2000 and further amendment in 2008 • Scope of IT Act – application & legal recognition of electronic documents, Licensed certifying authorities, Jurisdictions, Cyber Appellate Tribunal, Digital Contracts, • Civil Liabilities under Chapter IX – Sec 43 – damages to Computer Systems, Sec 43 A – Compensation, Sec 44 & 45 that deal with penalties • Nature of Cybercrimes – Section 66, Section 66A (now scrapped), Section 66B(stolen computer, Section 66C(Identity theft), Section 66 D(impersonation), 66F(Cyber terrorism), Section 66E(Video voyeurism) Section 67(obscenity) • Digital Signature related – Section 71 – penalty for misrepresentation, Section 73, Section 74 • Preserving Evidence - Sec 65 (tampering with computer source documents), Section 67C • Privacy Related - Sec 72 • Provisions related to Empowering central agencies – Sec 69, 69A, 69B, 70B • Power of Police officers – Sec 80 • Cognizability, Bailability, Compundability • Offences by Companies – Sec 85 • Personal Data Protection Bill 2019 – Data fiduciary, rights of individual, restrictions on data transfer outside India • **Cloud Security** • Cloud computing and its types • Cloud Infra – computing, network and storage • Data Security in cloud • CIA in Cloud • Cloud OWASP Top 10 ▪ R1 – Accountability and data risk ▪ R2 – User identity Federation ▪ R3 – Legal and regulatory compliance ▪ R4 – Business Continuity & Resiliency ▪ R5 – User Privacy & Secondary Usage of Data ▪ R6 – Service and Data integration ▪ R7 – Multi tenancy & Physical Security ▪ R8 – Incidence Analysis & Forensics ▪ R9 – Infrastructure Security ▪ R10 – Non production environment exposure

- **Risk Management**
  - Steps – Identify, Analyse, Evaluate, Treat, Monitor & Review risk
  - Considerations regarding Risk Management – Culture, Information Sharing, Priorities, Resilience, Speed, Threat Environment, Cyber Hygiene
  - Risk Calculation – Hazard * Vulnerability * Elements at risk
  - Risk matrix
  - Risk rating = likelihood*Severity.

- **Application Security**
  - Types – Data center, Desktop, Cloud, Mobile, Web applications
  - Data Centre applications – Custom apps or third party apps
  - Third party application security & risks
  - Application Security Testing – DevOps, Soruce code security
  - Cloud application security
    - Threats – misconfigurations, unauthorized access, insecure APIs, account hijacking
    - Tools for cloud application management
    - NGFW
    - SAAS Security
    - Encryption in cloud
  - Web Application Security
    - WAF
    - API Security
    - SQL Injections, Cross site Scripting, Cross site Request forgery
    - Packet sniffing, Man in the middle attacks, DNS attacks
    - Denial of Service, Phishing, Key-logging
    - Steps to secure – Authentication, Access control, Confidentiality, Integrity, Non-repudiation
    - Session management – implementing timeouts, session id management, cookie management

- **NIST Cybersecurity Framework**
  - Risk Management
    - Identify: Asset Management, Business environment, Governance, Risk assessment, Risk management strategy
    - Protect: Access Control, Awareness and Training, Data Security, Information protection and procedures, Maintenance, Protective technology.
    - Detect: Anomalies and Events, Continuous monitoring, Detection process
    - Respond: Response planning, communications, analysis, mitigation, improvements
    - Recover: recover planning, improvements, communications

  - Establishing and Improving Organization's Cybersecurity Program
    - Step 1: Prioritize and Scope. Align with organization's objectives and priorities.
    - Step 2: Orient. Identify related systems and assets, regulatory requirements and overall risk approach.
    - Step 3: Create a current profile. It should give the current compliance and baseline for further actions

		▪ Step 4: Conduct a risk assessment. ▪ Step 5: Create a target profile. ▪ Step 6: Determine, Analyze and Prioritize Gaps. ▪ Step 7: Implement Action plan to fill gaps. • **Cybersecurity Best practices** • Breaches and their impacts • Cyber resilience: Identify, Prevent, Detect and respond • SOC – Security Operations centre • Incident response plan • Practicing Cyber hygiene • Data security – full disk encryption, backups, data masking, data erasure • Governance Framework, Involvement of senior management • Personnel screening and insider threats • Physical security of assets • Cybersecurity awareness and training • Network security • Information system protection • Account management and access controls • Asset management • Endpoint Detection & Response • **Security Operations Centre and SIEM:** • SIEM comprises of gathering, analysing, presenting information from wide range of network and security devices, identify and access management applications, vulnerability management, policy compliance tools, operating systems, database and application logs, external threat data. • SIEM is used to identify, document and respond to security events • SIEM consists of Log management, IT regulatory compliance, Event correlation, active response and endpoint security • Structure of SIEM: Source device -> Log collection -> Parsing -> Rule Engine/Correlation – Monitoring and Storage of logs • SOC is a team of security analysts to detect, analyse, respond to, report on and to prevent cyber security incidents. • SOC team must perform advanced forensic analysis, packet captures, malware reverse engineering on artefacts collected during an incident. • Basic Attacks can be mitigated using IDS/HIPS/NIPS but manual intervention is required to resolve major incidents • Security Orchestration Automation and Response (SOAR): SOAR refers to technologies that enable organizations to collect inputs monitored by the security operations team. For example, alerts from the SIEM system and other security technologies — where incident analysis and triage can be performed by leveraging a combination of human and machine power — help define, prioritize and drive standardized incident response activities. SOAR tools allow an organization to define incident analysis and response procedures in a digital workflow format. • **Cyber Security Incident Management:** • Incident types can be Denial of Service, Malicious code executions, Unauthorized access, Phishing, Man in middle etc

		• Incident response team • Elements of Incident response plan - Mission, Strategies and goals, Senior management approval, organizational approach, incident communication, metrics for measuring response effectiveness, roadmap for maturing the plan etc. • Incident response lifecycle: Preparation, Decision and analysis, Containment, Eradication, Recovery, Post incident activity • Tracking and reporting all incidents • **Malwares** • Types: adwares, spyware, virus, Trojan, worm, rootkit • Analysis: Static and dynamic • Debugger • **Digital Forensics** • Network Forensics ▪ Steps in network forensics ▪ Digital forensic methods for network layers – Data link & physical layers, TCP/IP, Internet, Wireless, ▪ Tools – tcpdump, wireshark, xplico, netsnif etc • Motivations – Blackmailing, fake profiles, Intellectual Property thefts • Uses – Criminal and Civil investigations, Administrative requirements, • Computer forensics – Intellectual Property theft, espionage, Regulatory compliance etc. • Roles of Forensic Investigators – Collection and Preservation of data, reporting • Forensic Toolkit • Autopsy tool
1.10	**Sr. Manager (IT)/ E-3 Level**	1. **Expert knowledge of professional java frameworks like Spring, hibernate etc.** Spring-Architecture, environment, IoC containers, bean scope, bean lifecycle, bean post processors, dependency injection, beans auto wiring, event handling, JDBC framework, transaction management, web MVC framework, Log4j, etc. Hibernate-Architecture, environment, configuration, sessions, persistent class, mapping files, O/R Mappings, Query language, Native SQL, caching, batch processing, interceptors, etc. **2. Expert knowledge in build automation tools like maven.** Maven- Environment, POM, build life cycle, build profiles, repositories, plug-ins, creating project, snapshots, build automation, deployment automation, etc. **3. Experience in Async job scheduling platforms like Kafka/RabbitMQ** Kafka-fundamentals, cluster architecture, workflow, simple producer, consumer group, tools, etc. RabbitMQ- overview, messaging model, producer, consumer, exchanges, queues, bindings, connections, channels, etc. **4. Experience in SQL, NoSQL databases systems like MySQL, elasticsearch, redis, etc.** SQL- RDBMS concepts, syntax, operators, expressions, create/drop/select/insert commands, result sorting, contraints, joins, unions, indexes, alias syntax, alter command, truncate table, views, transactions, wildcards, date functions, temporary tables, clone tables, sub queries, etc. Elasticsearch- API conventions, aggregations, index APIs, CAT APIs, search APIs, Cluster APIs, Query DSL, mapping, analysis, index module, ingest node, index lifecycle, frozen indices, kibana dashboard, filtering by field, data tables, region maps, pie charts, area and bar charts, time series, tag clouds, heat maps, canvas, logs UI, etc. Redis- commands, keys, strings, hashes, lists, sets, sorted sets, HyperLogLog, publish subscribe, transactions, scriptingbackup, security, client connections, pipelining, partitioning, etc. 5. **Good hands-on knowledge of Configuration Management and Deployment tools like Jenkins, Ansible, chef etc.**

		Configuration Management- Configuration Identification, Baselines, Change Control, Configuration Status Accounting, Configuration Audits and review, etc. Jenkins- unit testing, automated testing, reporting, code analysis, distributed builds, automated deployment, metrics and trends, server maintenance, continuous deployment, plugins, security, etc. Ansible- environment setup, yaml basics, ad hoc commands, playbooks, roles, variables, advanced troubleshooting, etc. Chef-architecture, version control system setup, workstation setup, client setup, kitchen setup, knife setup, solo setup, cookbooks, dependencies, roles, environment, chef shell, foodcritic, chefspec, nodes, etc. **6. Proficient in scripting, Git and Git workflows.** Environment, lifecycle, branches, conflicts, pull request, commands, distributed version control, undo, Create and copy Git repositories using git commands, Troubleshoot and remediate Merge conflicts etc. **7. Knowledge of web development in node.js, javascript, html.** Node.js- REPL terminal, callback concept, event loop, event emitter, buffers, streams, file system, global objects,utility module, web module, express framework, RESTFul API, application scaling, etc. Javascript - Cookies, Page redirects, dialog boxes, page printing, HTML DOM, error handling, validation, animation, multimedia, debugging, image map, JavaScript libraries (e.g. ExtJS, Backbone JS, and Angular JS), browser rendering behavior and performance, front-end tools (e.g. Grunt and Gulp JS.), asynchronous request handling, partial page updates, and AJAX; cross-browser compatibility issues and ways to work around such issues, JavaScript module loaders, such as Require.js and AMD, browser rendering behaviour and performance, Javascript Web APIs, Ajax, JSON, etc. HTML and HTML5- tags, elements, attributes, formatting, embed multimedia, marquees, header, style sheet, entities, MIME media types, url encoding, character encodings, web forms 2.0, SVG, MathML, Web storage, Web SQL databases, server-sent events, WebSocket, Canvas, audio and video, Geolocation, microdata, web workers, IndexDB, web messaging, Web CORS, Web RTC, etc. **8. Expert knowledge in Rest APIs** RESTful web APIs, rest constraints, concept of serialization, concept of deserialization, Richardson maturity model, Environment, messages, addressing, methods, statelessness, caching, security, etc. 9. **System admin knowledge (Windows/Linux)** Linux- File management, directories, file permission, environment, basic utilities, pipes, filters, processes, communication, vi editor, shell scripting, special variables, shell loops, loop control, shell substitutions, quoting mechanisms, IO redirections, shell functions, manpage help, regular expressions, file system basics, user administrations, system performance, system logging, signals and traps, etc. Windows- server roles, powershell, remote management, Windows firewall, remote desktop management, resource monitor, active directory, DC Accounts, File System, Group Managed service accounts, group policy overview, DHCP role, DNS role, primary zones, manage records, IIS overview, IIS Security, Hyper-V, advanced configuration, WSUS, WSUS policies and tuning, sharing of files, file manager, print server, network services, backup management, nano server, containers, nested virtualization, etc. 10. **Knowledge of scripting language -Python/Perl/shell/PHP.** Python-classes, objects, reg expressions, data types, type casting, CGI programming, database access, networking, sending email, multithreading, xml processing, GUI programming, etc. Perl- scalars, arrays, hashes, loops, subroutines, file I/O, error handling, special variables, regular expressions, coding standard, sending email, socket programming, object oriented, database access, CGI programming, package and modules, process management, etc. Shell- special variables, shell loops, loop control, shell substitutions, quoting mechanisms, IO redirections, shell functions, manpage help, etc. PHP-web concepts, GET & POST, file inclusion, Files & I/O, functions, cookies, sessions, sending emails, file uploading, coding standard, predefined variables, regular expressions, error handling, bugs debugging, form introduction, validation, etc.

Annexure-III

RELAXATION IN MAXIMUM AGE LIMIT

Relaxation in maximum age limit for the following categories is given as indicated in the table below subject to submission of requisite certificates (as on the crucial date of eligibility).

S. No.	Categories		Relaxation in upper age limit (or) maximum upper age
a)	OBCs (non-creamy layer)		3 years
b)	SC/STs		5 years
c)	Persons with Benchmark Disabilities (UR)		10 years
d)	Persons with Benchmark Disabilities (OBCs-NCL)		13 years
e)	Persons with Benchmark Disabilities (SC/ST)		15 years
f)	Ex-servicemen including Commissioned Officers and ECOs/SSCOs, who have rendered at least 5 years military service as on **last date of receipt of on-line application** and have been released (i) on completion of assignment (including those whose assignment is due to be completed within one year from **last date of receipt of on-line application** otherwise than by way of dismissal or discharge on account of misconduct or inefficiency, or (ii) on account of physical disability attributable to military service, or (iii) on invalidment.	UR	5 years
		OBCs-NCL	8 years
		SC/ST	10 years
g)	Ex-servicemen including ECOs/SSCOs who have completed an initial period of assignment of	UR	5 years

	five years of military service as on **last date of receipt of on-line application** and whose assignment has been extended beyond five years and in whose case the Ministry of Defense issues a certificate that they can apply for civil employment and they will be released on three months' notice on selection from the date of receipt of offer of appointment.	OBCs-NCL	8 years
		SC/ST	10 years
h)	Defense Service Personnel disabled in operation during hostilities with any foreign country or in a disturbed area, and released as a consequence thereof on or before **last date of receipt of on-line application**.	UR	3 years
		OBCs-NCL	6 years
		SC/ST	8 years
i)	Candidates who are serving RailTel Corporation **on last date of receipt of on-line application** as direct contractual executives / outsourced. This relaxation in age is subject to the condition of candidate continuing in RailTel Corporation's/ REL's service till the offer of appointment is issued on their empanelment for appointment in RailTel Corporation.	UR	Period of experience (in years, months and days) in RailTel Corp./REL as on last date of receipt of on-line application.
		OBCs-NCL	Maximum age for OBC-NCL for the post applied + Period of experience (in years, months and days) in RailTel Corp./REL as on last date of receipt of on-line application.
		SC/ST	Maximum age for SC/ST for the post applied + Period of experience (in years, months and days) in RailTel Corp./REL as on last date of receipt of on-line application.

Annexure-IV

INSTRUCTIONS FOR PERSONS WITH BENCHMARK DISABILITIES

Functional classification and functional requirement of PwBDs posts: Only those category(ies) of disabilities mentioned below and meeting the functional requirements mentioned in column no. 4 below, shall be considered for appointment.

S.No.	Categories for which identified	Functional Classification	Functional Requirements for posts
Col.1	Col.2	Col.3	Col.4
1	Category-(a) Visually Impaired (VI)	A person, having not less than 40% visual impairment only is eligible to apply under VI Category. The candidates with the following types of disabilities only where independent mobility is not affected, shall be acceptable under this category: **'Low Vision'**.	S, ST, SE, RW, BN, MF, C, W, H
2	Category-(b) Hearing Impaired	A person, having not less than 40% hearing impairment in the better ear in the conversational range of frequencies, shall be eligible to apply under HH Category. The candidates with the following types of disabilities only shall be acceptable under this category: **'Hard of hearing'**.	S, ST, SE, RW, BN, MF, C, W, H
3	Category-(c) Locomotor Disability including cerebral palsy, leprosy cured, dwarfism, acid attack victim, Muscular Dystrophy.	A person having not less than 40% physical disability of such type with which the independent mobility is not affected, is eligible to apply under OH Category. The candidates with only one of the following types of disabilities shall be acceptable under this category: a) Only one leg affected (right or left). b) Impaired reach of only one leg. c) Weakness of grip of only one leg. d) Only one arm affected (right or left). e) Impaired reach of only one arm. f) Weakness of grip of only one arm.	S, ST, SE, RW, BN, MF, C, W, H

		g) Dwarfism h) leprosy cured i) Acid attack victim	
4	Category (d) - Autism, intellectual disability, specific learning disability, mental illness. Category (e) - multiple disabilities from amongst persons under clauses (a) to (d) above.	A person having not less than 40% physical disability of such type with which the independent mobility is not affected, is eligible to apply under 'D' Category. The candidate should be able to meet the physical requirements indicated in column no. 4 of this table.	S, ST, SE, RW, BN, MF, C, W, H

Legend: Functional Requirements

Codes	Functional Requirement	
S	Work performed by sitting (on bench or chair)	A PwBDs will be considered to be eligible for appointment only if he/she (after such physical examination as the appointing authority may prescribe) is found by the RailTel to satisfy the requirements of physical and medical standards for the concerned posts to be allocated to the PwBDs. It will be necessary that PwBDs should meet the functional requirement detailed in column no. 4 of table given on pre-page.
ST	Work performed by standing	
SE	Work performed by seeing	
RW	Work performed by reading and writing	
BN	Work performed by bending	
MF	Work performed by manipulation of fingers	
C	Work performed by communication	
W	Work performed by walking	
H	Work performed by hearing	