Syllabus for the post of TECHNICAL SUPERINTENDENT *(Cyber Security)*
(Integrated Information System (IIS) Division)
(WRITTEN TEST & SKILL TEST)

Basic Security	- Basic Networking (Ports, OSI/TCP-IP Model, Network Devices, Network topology etc) - Cybersecurity - Malware - Ransomware - Attacks - Threats - Vulnerabilities - Risk - NICE Framework, MITRE Attack Matrix - IoT, OT - BYOD - Security Controls - Network Flow, Syslog,SNMP - Network Collisions, Jitter, Latency, Delay etc. - Antivirus - Endpoint Management - Beacon - CCTVs - Physical Access Control - DNS , DHCP - QoS
Network Security	- Security devices- Firewall, UTM,NGFW, IDS,IPS - Secure Design - Layer 2 Security- Port Security - Device Access Control - NAT - VPN - DMZ - SDWAN and SDN - Firewall policies - Customised signature and policy design for firewall
Identity and Access Management	- AAA - AD and LDAP - MFA - SSO, RSSO - IAM Life Cycle - Role based and attribute based authentication

Application and Web Application Security	- Software Security (OWASP tools and methodologies, Cross Site Scripting etc) - Basic Idea about Security Testing (Blackbox, Whitebox, Gray Box testing, VAPT) etc. - Cryptography (Symmetric & Asymmetric, Hashing, Digital Signature, Encryption etc) - Secure Software Lifecycle Management
Advanced Security modules	- SNMP, Syslog and Network flow analysis. - Auditing of user authentication and access logs - Firewall log analysis. - Centralised log management and analysis using tools like XDR and SIEM - Cyber Threat Hunting - Active vs Passive Defence - Cloud Security for SAS application - C2C communication analysis - Incident response - Basic idea of Cyber Forensic - Open-Source tools for cyber security - Policy preparation related to Cyber Security. - Secure communication for IoT and OT devices.
Security Governance and Regulations	- IT ACT 2000 and its amendment - Cert-in regulation and guidelines - GIGW - GoI Security Guidelines

*****