Title: Implementing Cybersecurity Tools, Techniques, and Procedures in Mumbai's Local Transport System

The growing digitization and interconnectedness of the Mumbai local transportation system have heightened the necessity for cybersecurity measures. This literature study seeks to investigate the use of cybersecurity technologies, tactics, and processes to improve the security and resilience of the transportation system. The assessment examines many cybersecurity frameworks and standards, including the National Cyber Security Policy (NCSP), NIST Cybersecurity Framework (NIST CSF), and ISO/IEC 27001:2013, which serve as recommendations for safeguarding the local transportation system.

The examination digs further into the various cybersecurity technologies and strategies, including firewalls, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS). The necessity of encryption for data at rest and in transit is also covered, along with endpoint security measures such as antivirus software, patch management, and device management. The assessment also emphasises the significance of Security Information and Event Management (SIEM) for real-time monitoring and incident response.

In addition, the literature analysis highlights the necessity for routine security audits, vulnerability assessments, and penetration testing, as well as staff training and awareness programmes addressing security best practises, social engineering, password management, and physical security. It is essential to build incident response and disaster recovery plans, including business continuity planning and backup techniques, to guarantee the resilience of the transportation system against possible threats.

The literature study concludes by emphasising the significance of deploying cybersecurity technologies, strategies, and processes in Mumbai's local transport system in order to strengthen its security and resilience while continually adapting to new threats.