Job Description -- Chief Information Security Officer (CISO)

Role Purpose:

- The **Chief Information Security Officer** will be responsible for establishing a resilient cybersecurity framework that safeguards the Integrated Command and Control Centre (ICCC), Internet of Things (IoT) systems, cloud environments, smart mobility, public Wi-Fi, surveillance infrastructure and data-driven applications aligned with the Digital India and Smart Cities Mission.
- The role will ensure compliance with national cyber regulations, protect critical information infrastructure (CII) and lead risk mitigation, incident response and security awareness programs for the city's digital landscape.

Key Responsibilities:

1. Cybersecurity Strategy & Governance

- Develop and execute a robust cybersecurity strategy for SSCL covering ICCC, surveillance systems, smart traffic signals, IoT devices and citizen service portals.
- Formulate and implement cybersecurity policies and Standard Operating Procedures (SOPs) in line with CERT-In guidelines, NDMA advisory and state IT policies.
- Align the security posture with national frameworks including NCIIPC, Digital India and MeitY's cybersecurity directives.

2. Risk Management & Compliance

- Conduct risk assessments, security audits and VAPT (Vulnerability Assessment & Penetration Testing) for all ICT systems and platforms.
- Ensure regulatory compliance with the IT Act 2000 (amended), Digital Personal Data Protection (DPDP) Act 2023 and Meghalaya State Digital Security guidelines.
- Define and monitor Key Risk Indicators (KRIs) and Key Performance Indicators (KPIs) for smart city cybersecurity performance.

3. Security Operations & Incident Response

- Establish and operationalize a 24x7 Security Operations Centre (SOC) integrated with ICCC for real-time threat detection and incident response.

- Lead cyber incident response teams during data breaches or DDoS attacks and coordinate with CERT-In, NIC and state cyber cells for remediation.
- Maintain and regularly test Business Continuity and Disaster Recovery Plans (BCP/DRP).

4. Infrastructure and Data Security

- Oversee secure architecture for SSCL's hybrid cloud platforms (AWS/Azure), CCTV networks, city surveillance, sensor networks and SCADA systems.
- Implement Identity and Access Management (IAM), encryption standards, firewall policies, intrusion detection/prevention systems (IDPS) and DLP solutions.
- Safeguard personal data of citizens using SSCL portals by enforcing data protection by design and default.

5. Capacity Building and Stakeholder Engagement

- Conduct cyber hygiene workshops for SSCL staff, technology vendors and field operators.
- Drive cybersecurity awareness for Shillong citizens using digital campaigns and smart kiosks.
- Engage with stakeholders including NIC, MeitY, industry partners and academic institutions for collaborative security innovation.

6. Vendor and SLA Compliance

- Define cybersecurity clauses in vendor contracts, RFPs and SLAs for ICT and civil contractors.
- Audit third-party compliance with ISO/IEC 27001, GDPR-equivalent standards and Smart City Data Management Policy.

Job Description -- Business Intelligence Analyst

Role Purpose:

- The **Business Intelligence Analyst** will play a key role in managing and analyzing data from various urban systems integrated with ICCC. This role is essential to generate insights, improve service delivery, monitor KPIs, and support data-driven decisions across transport, utilities, safety, and citizen services.

Key Responsibilities:

- Collect, clean and process data from multiple smart city platforms including traffic, waste management, energy, surveillance and citizen feedback systems.
- Design and develop interactive dashboards and reports using BI tools (e.g. Power BI, Tableau).
- Perform statistical analysis and create predictive models to support proactive urban management.
- Identify patterns, trends and anomalies to aid in improving service efficiency.
- Support real-time monitoring and alert systems using analytics.
- Collaborate with ICCC operations teams, technology vendors and administrative departments to ensure accurate data flow and interpretation.
- Establish and maintain data quality and governance standards.
- Prepare data documentation, analytics reports and presentations for stakeholders and leadership.

Job Description -- Smart Element Support Technician

Role Purpose:

- The **Smart Element Support Technician** will be responsible for the field-level operation, maintenance and troubleshooting of smart devices and IoT-based systems deployed across the city. The role ensures uptime, connectivity and real-time data transmission from field sensors and smart infrastructure to the ICCC platform.

Key Responsibilities:

- Perform regular health checks, diagnostics, and maintenance of field-deployed smart elements (e.g., smart poles, smart cameras, environmental sensors, LED lighting, traffic systems, smart meters).
- Install, calibrate and configure IoT sensors and devices as per OEM guidelines.
- Ensure uninterrupted connectivity of smart devices using wired/wireless (RF/LoRa/Wi-Fi/4G) networks.
- Troubleshoot and repair defective hardware and coordinate with OEMs for replacements.
- Conduct firmware upgrades and basic configuration updates remotely or onsite.
- Verify data transmission integrity between field devices and ICCC data platforms.
- Maintain detailed service logs, maintenance records, and field reports.
- Respond to alerts and system failures reported by ICCC or city operations staff in a timely manner.
- Assist the network and software teams in end-to-end diagnostics of smart infrastructure integration issues.