Chief Information Security Officer (CISO)

Chief Information Security Officer (CISO), State Data Authority, State Transformation Commission, Government of Uttar Pradesh will be the senior executive responsible for protecting government data, digital infrastructure, citizen information, and critical technology systems from cyber threats, misuse, breaches, and operational disruption.

Reporting To

Chief Executive Officer, State Transformation Commission, Government of Uttar Pradesh, with independent functional authority and close coordination with the CTO and Chief Data Officer.

Overall Mandate

To establish and enforce a secure, resilient, privacy-conscious, and continuously monitored cyber ecosystem for digital systems, data platforms at STC and connected departments.

2. Core Responsibilities

A. Cybersecurity Governance

- Develop the **State Cybersecurity Strategy** and annual security roadmap.
- Establish security policies, controls, standards, and compliance mechanisms.
- Define minimum security baseline for all departments.

B. Protection of Government Data

- Safeguard citizen, departmental, financial, and sensitive data.
- Ensure encryption, key management, secure backups, and access controls.
- Prevent unauthorized access, insider threats, and data leakage.

C. Security of Digital Infrastructure

- Secure data centers, cloud systems, networks, endpoints, applications, APIs, and mobile apps.
- Oversee identity and access management (IAM), privileged access, and zero-trust principles.

D. Threat Detection & Incident Response

- Establish Security Operations Center (SOC) / CERT-State capability.
- Monitor threats, malware, phishing, ransomware, DDoS, and intrusion attempts.
- Lead incident response, containment, forensic coordination, and recovery.

E. Risk Management & Audits

- Conduct cyber risk assessments of major systems and departments.
- Ensure vulnerability assessments, penetration testing, source code audits, and compliance reviews.
- Maintain risk register and remediation tracking.

F. Privacy & Compliance

- Coordinate privacy controls, logging, audit trails, retention controls, and breach reporting.
- Support compliance with applicable data protection and cybersecurity laws.

G. Capacity Building

- Run phishing awareness, cyber drills, tabletop exercises, and officer training.
- Build security champions in every department.

H. Secure Procurement & Vendor Oversight

- Ensure cybersecurity clauses in RFPs, contracts, SLAs, and vendor onboarding.
- Review third-party risk and managed service providers.

3. Terms of Reference (ToR)

1. Prepare State Cybersecurity Roadmap.
2. Recommend security investments and priority risk mitigation.
3. Advise government during major cyber incidents.

4. Issue security standards for all departments.
5. Define data classification policy (public/internal/confidential/restricted).

6. Mandate periodic cyber compliance reporting.

7. Establish SOC / CERT-State.
8. Implement SIEM/log monitoring across critical systems.
9. Ensure MFA, IAM, backup, DR, endpoint security deployment.

10. Conduct annual audits of critical systems.
11. Require VAPT before go-live of major applications.
12. Review security posture of vendors and cloud providers.

13. Lead response to cyber incidents affecting state systems.
14. Coordinate with national agencies such as CERT-In and law enforcement where required.
15. Issue post-incident corrective action plans.

16. Conduct quarterly cyber drills.
17. Train departmental nodal officers and admins.
18. Publish advisories on emerging threats.

4. Key Deliverables (First 12 Months)

1. State cybersecurity policy approved.
2. Security baseline for all departments notified.
3. SOC / monitoring center operational.
4. MFA enabled for critical users/systems.
5. Top 20 critical systems security audited.
6. Backup and disaster recovery tested.
7. Phishing awareness program launched.
8. Department cyber nodal network established.

5. KPIs for Performance Evaluation

- Number of incidents detected and contained
- Mean time to detect (MTTD) and respond (MTTR)
- % critical systems audited
- % systems with MFA enabled
- Patch compliance rate
- Vulnerability remediation time
- Backup recovery success rate
- Staff training coverage

6. Ideal Eligibility Profile

- Senior cybersecurity professional / technocrat with strong cyber background and Master's degree
- 12–15+ years in information security, SOC, audits, networks, cloud security, governance
- Experience in large-scale enterprise or government systems