

मुख्य कार्यकारी अधिकारी
स्टेट ट्रांसफार्मेशन कमीशन अनुभाग-1
(नियोजन विभाग)

संख्या: (914/26) UPSPC-STC 1017 M/96/2026-SPCSL

लखनऊ: दिनांक: 28 अप्रैल, 2026

कार्यालय-ज्ञाप

शासन द्वारा वर्ष 2026-27 के बजट में स्टेट ट्रांसफार्मेशन कमीशन, उत्तर प्रदेश (State Transformation Commission (STC-UP) द्वारा स्टेट डाटा अथॉरिटी के गठन के लिए अनुदान स्वीकृत किया गया है। स्टेट डाटा अथॉरिटी के कार्य को प्रारम्भ करने के लिए स्टेट ट्रांसफार्मेशन कमीशन में सीनियर कन्सल्टेंट्स (नीति आयोग, भारत सरकार द्वारा निर्गत गाईडलाइन 07 जुलाई, 2023) के पदों पर चीफ डाटा ऑफिसर, चीफ टेक्नोलॉजी ऑफिसर, चीफ इन्फॉर्मेशन सिस्टीम ऑफिसर तथा चीफ आर्टिफिशियल इन्टेलीजेंस एवं मशीन लर्निंग ऑफिसर के पदों पर चयन व तैनाती हेतु कार्य क्षेत्र, टर्म्स ऑफ रेफरेंस एवं इलिजिबिलिटी क्राइटेरिया तैयार किया गया है। उक्त विवरण इस पत्र के साथ संलग्न कर आपको इस आशय से प्रेषित है कि कृपया इस पर अपना परामर्श व सुझाव 07 दिन के अन्दर उपलब्ध कराने का कष्ट करें। सुझाव ई-मेल- ceostc.up@gmail.com पर भी भेजा जा सकता है।

संलग्नक-यथोक्त।

(मनोज कुमार सिंह)
मुख्य कार्यकारी अधिकारी
स्टेट ट्रांसफार्मेशन कमीशन
उत्तर प्रदेश।

संख्या: (914/26) UPSPC-STC 1017 M/96/2026-SPCSL तददिनांक।

प्रतिलिपि: निम्नलिखित को सूचनार्थ एवं आवश्यक कार्यवाही हेतु प्रेषित:-

1. सचिव, मा0 मुख्यमंत्री जी (अध्यक्ष, स्टेट ट्रांसफार्मेशन कमीशन) उत्तर प्रदेश।
2. मुख्य सचिव, उत्तर प्रदेश शासन।
3. समस्त अपर मुख्य सचिव/प्रमुख सचिव, उत्तर प्रदेश शासन।
4. अवस्थापना एवं औद्योगिक विकास आयुक्त, उत्तर प्रदेश शासन।
5. प्रबन्ध निदेशक, यू0पी0डेस्क, उत्तर प्रदेश, लखनऊ
6. डायरेक्टर, सूचना, उत्तर प्रदेश, लखनऊ
7. एस0आई0ओ0, एन0आई0सी0, उत्तर प्रदेश, लखनऊ
8. अपर मुख्य कार्यकारी अधिकारी, स्टेट ट्रांसफार्मेशन कमीशन, उत्तर प्रदेश।
9. समस्त अधिकारी, स्टेट ट्रांसफार्मेशन कमीशन, उत्तर प्रदेश।
10. समस्त अनुभाग अधिकारी, एस0टी0सी0 अनुभाग।

आज्ञा से,

(मनोज कुमार सिंह) 28.4.26
मुख्य कार्यकारी अधिकारी
स्टेट ट्रांसफार्मेशन कमीशन
उत्तर प्रदेश।

State Data Authority, State Transformation Commission, Government of Uttar Pradesh

Chief Data Officer (CDO)

Chief Data Officer, State Data Authority, State Transformation Commission, Government of Uttar Pradesh

Reporting To

Chief Executive Officer, State Transformation Commission, Government of Uttar Pradesh.

Overall Mandate

To create a unified state data ecosystem enabling evidence-based policymaking, integrated citizen services, efficient governance, fraud reduction, and innovation while ensuring privacy, security, and compliance. The role will include policy formulation for state-wide data strategy, standards, data sharing, analytics, innovation, open data.

2. Core Responsibilities

A. State Data Strategy & Policy

- Prepare and implement the **State Data Policy and Strategy**.
- Draft state data governance policy, sharing policy, open data policy, and retention policy.
- Establish data ownership and stewardship framework across departments.

B. Data Integration Across Departments

- Integrate datasets from Health, Revenue, Agriculture, Education, Urban Development, Police, Social Welfare, etc.
- Develop a Single Source of Truth architecture.
- Create common identifiers and master registries (citizen, land parcel, enterprise, beneficiary, school, hospital).

C. Data Quality & Standards

- Define standards for metadata, data dictionaries, formats, APIs, and master data.
- Ensure data quality, timeliness, completeness, deduplication, and accuracy.
- Institutionalize departmental data audits.

D. Analytics & Decision Intelligence

- Build executive dashboards for CM Office / Chief Secretary / departments.
- Use AI/ML for forecasting, fraud detection, targeting schemes, grievance trends, traffic, health alerts.
- Promote district performance scorecards.

E. Citizen Service Transformation

- Enable proactive delivery of schemes through data-driven eligibility discovery.
- Support one-stop digital citizen platforms.
- Reduce repeat document submissions through trusted data exchange.

F. Privacy, Security & Responsible Use

- Ensure compliance with applicable data protection laws.
- Create consent, access control, anonymization, and audit mechanisms.
- Lead ethical AI and responsible data governance.

G. Open Data & Innovation

- Launch and manage state open data portal.
- Release non-sensitive datasets for startups, academia, and researchers.
- Promote hackathons and innovation challenges.

H. Capacity Building

- Develop data literacy among officers.
- Create departmental Chief Data Officer / Nodal Officer network.
- Build cadre of data analysts in departments.

3. Terms of Reference (ToR)

Strategic ToR

1. Prepare 3-year and annual State Data Action Plans.
2. Recommend legal, institutional, and policy reforms.
3. Advise government on emerging technologies and data economy opportunities.
4. Establish State Data Exchange Platform.
5. Set up enterprise data warehouse / Lakehouse.
6. Approve departmental data standards and integration roadmaps.
7. Oversee data quality scorecards across departments.
8. Review high-value datasets monthly.
9. Convene departmental CDO forum quarterly.
10. Resolve inter-departmental data-sharing issues.
11. Deliver KPI dashboards for top priorities.
12. Support evidence-based budgeting and policy evaluation.
13. Identify leakages and efficiency gains.
15. Coordinate with CISO for cyber and access controls.
16. Ensure privacy impact assessments for major projects.
17. Maintain audit trails and compliance reports.

4. Key Deliverables (First 12 Months)

1. State Data Policy approved.
2. Inventory of all departmental databases.
3. State master data architecture.
4. 10 priority departments integrated.
5. CM dashboard live.
6. Beneficiary deduplication engine launched.
7. Open data portal operational.
8. District performance analytics system live.

5. KPIs for Performance Evaluation

- Number of departments integrated
- Improvement in data quality scores
- Reduction in duplicate beneficiaries
- Faster service delivery time
- Savings detected through analytics
- Number of datasets published
- Dashboard usage by departments
- Training coverage of officers

6. Ideal Eligibility Profile

- Senior technocrat / domain expert with Master's degree.
- 15+ years in digital governance, analytics, IT systems, reform delivery
- Experience with large-scale public platforms and change management

Chief Technology Officer (CTO), State Data Authority, Government of Uttar Pradesh

The Chief Technology Officer (CTO) in the State Data Authority, State Transformation Commission, Government of Uttar Pradesh should be the senior executive responsible for the technology backbone, digital architecture, platforms, interoperability, scalability, and modernization needed to make government data systems function reliably at scale. The CTO should ensure that departmental systems can securely connect, exchange data, and support citizen-centric digital services.

Reporting To

Chief Executive Officer, State Transformation Commission, Government of Uttar Pradesh with close coordination with the Chief Data Officer and Chief Information Security Officer.

Overall Mandate

To design, build, operate, and continuously improve the state's digital public infrastructure, enterprise technology platforms, and interoperable systems for data-driven governance.

2. Core Responsibilities

A. State Technology Architecture

- Define the **State Enterprise Architecture** for digital governance.
- Standardize technology stacks, APIs, hosting, identity integration, and shared platforms.
- Create future-ready architecture for scale across districts and departments.
- Create AI ready data bases and architecture.

B. Digital Public Infrastructure (DPI)

- Build and maintain shared state platforms such as:
 - API gateway
 - State data exchange
 - Workflow engine
 - Notification platform (SMS/WhatsApp/email)
 - Payment integration
 - Authentication / SSO
 - Document vault
 - GIS platforms

C. System Integration & Interoperability

- Integrate departmental applications across Health, Revenue, Education, Agriculture, Urban, Transport, etc.
- Enable real-time data exchange using secure APIs.
- Remove siloed legacy systems.

D. Cloud & Infrastructure Modernization

- Lead migration to secure cloud / hybrid cloud.
- Ensure uptime, disaster recovery, business continuity, backups.
- Optimize infrastructure costs.

E. Citizen Service Technology

- Enable one-stop citizen service portals and mobile apps.
- Improve speed, reliability, multilingual access, accessibility, and grievance systems.
- Support proactive service delivery.

F. Emerging Technologies

- Evaluate and deploy AI, GIS, IoT, drones, blockchain (where useful), automation, digital twins.
- Run pilots and scale proven solutions.

G. Vendor & Program Management

- Oversee system integrators, OEMs, consultants, and managed service providers.
- Standardize procurement specifications and SLAs.
- Ensure timely delivery of technology projects.

H. Security by Design

- Coordinate with CISO to embed security, logging, access control, encryption, and secure coding into all systems.

3. Terms of Reference (ToR)

Strategic ToR

1. Prepare State Technology Roadmap.
2. Recommend modernization priorities for legacy systems.
3. Advise on emerging tech adoption and architecture choices.
4. Establish State API Gateway.
5. Build State Data Exchange Platform.
6. Create common identity / SSO framework.
7. Build shared notification, workflow, and document systems.
8. Approve interoperability standards for all new departmental systems.
9. Ensure all major departments connect through APIs.
10. Resolve technical integration bottlenecks.
11. Define cloud strategy and hosting standards.
12. Maintain disaster recovery and uptime targets.
13. Optimize hardware/software licensing and recurring costs.

14. Review progress of all priority technology projects monthly.
15. Approve technical designs of major new systems.
16. Enforce SLAs and performance of vendors.

17. Run sandboxes / pilots for AI, IoT, GIS, automation.
18. Promote reusable open standards and open-source where appropriate.

4. Key Deliverables (First 12 Months)

1. State enterprise architecture approved.
2. API gateway operational.
3. 10 major departmental systems integrated.
4. State SSO launched.
5. Shared notification engine live.
6. DR and uptime framework operational.
7. Citizen unified services portal upgraded.
8. Cloud optimization plan implemented.

5. KPIs for Performance Evaluation

- Number of systems integrated
- API transactions per month
- Platform uptime (%)
- Average page/app response time
- Reduction in duplicate tech spend
- Project delivery timeliness
- Vendor SLA compliance
- Citizen satisfaction with digital services

6. Ideal Eligibility Profile

- Senior technocrat with Master's degree and deep digital governance exposure
- 15+ years in enterprise IT, cloud, architecture, public platforms, large programs
- Experience handling scale, vendors, cybersecurity coordination, and transformation delivery

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

Chief AI & ML Expert

The AI & ML Expert in a State Data Authority should be the senior technical specialist responsible for applying Artificial Intelligence (AI) and Machine Learning (ML) to improve governance outcomes, public service delivery, forecasting, fraud detection, operational efficiency, and evidence-based decision making. The role will include converting government data into practical, scalable solutions with measurable impact.

Reporting To

Chief Executive Officer, State Transformation Commission, Government of Uttar Pradesh in close coordination with Chief Data Officer, CTO and CISO.

Overall Mandate

To design, deploy, and govern AI/ML solutions that improve governance efficiency, citizen outcomes, and administrative decision-making while ensuring ethical, secure, and responsible use of AI.

2. Core Responsibilities

- Prepare **State AI Roadmap** aligned to development priorities.
- Identify high-impact use-cases across departments.
- Promote responsible adoption of AI in governance.

- Demand forecasting (health, transport, utilities, schools).
- Crop/yield prediction and weather-linked advisories.
- Disease outbreak early warning systems.
- Urban congestion and pollution prediction.

- Duplicate beneficiary detection.
- Suspicious transaction / claim analytics.
- Procurement anomaly detection.
- Revenue leakage analytics.

- AI chatbots and multilingual assistants.
- Intelligent grievance routing.
- Document processing (OCR/NLP).
- Smart recommendation systems for schemes/services.

- Build reusable ML pipelines, feature stores, model registries.
- Standardize datasets for AI readiness.

- Deploy MLOps frameworks.
- Bias testing, fairness checks, explainability.
- Human-in-the-loop decision systems.
- Privacy-preserving analytics and anonymization.
- AI model monitoring and audit trails.
- Train officers in AI use-cases.
- Build state data science teams.
- Run hackathons, innovation challenges, partnerships.

3. Terms of Reference (ToR)

Strategic ToR

1. Prepare State AI Strategy.
2. Recommend priority sectors for AI adoption.
3. Develop annual AI implementation plan.
4. Identify top 25 high-impact AI use-cases.
5. Build pilots and scale successful models.
6. Create reusable models across departments.
7. Establish State AI Lab / Centre of Excellence.
8. Build ML pipelines and deployment standards.
9. Ensure integration of AI outputs into departmental workflows.
10. Frame Responsible AI Guidelines.
11. Conduct model validation and periodic review.
12. Maintain inventory of all government AI systems.
13. Coordinate with CISO for secure AI deployment.
14. Ensure privacy safeguards in training datasets.
15. Prevent misuse of generative AI systems.
16. Engage with universities, startups, industry, and research bodies such as Indian Institute of Technology Kanpur, Indian Institute of Technology Delhi, and NITI Aayog where relevant.
17. Run challenge grants and innovation pilots.

4. Priority Use Cases for Uttar Pradesh

1. Maternal and child health risk prediction
2. School dropout early warning
3. Crop disease / irrigation advisories
4. Land record anomaly detection
5. Police hotspot and traffic analytics
6. Welfare duplication detection
7. Urban waste route optimization
8. Power demand forecasting

9. Employment trend analytics
10. Real-time CM dashboard insights

5. Key Deliverables (First 12 Months)

1. State AI policy / roadmap approved.
2. AI Centre of Excellence at GBU operational.
3. 10 pilots launched.
4. 3 models scaled statewide.
5. Fraud analytics engine live.
6. Multilingual citizen chatbot launched.
7. Responsible AI framework notified.
8. AI training for officers completed.

6. KPIs for Performance Evaluation

- Number of AI use-cases deployed
- Financial savings / leakages prevented
- Accuracy of prediction models
- Reduction in service response time
- Citizen satisfaction with AI services
- Number of departments using AI tools
- Time from pilot to scale-up
- Compliance with Responsible AI standards

7. Ideal Eligibility Profile

- Masters in AI, ML, Data Science, Computer Science, Statistics, or related field
- 10+ years in analytics / AI deployments
- Experience with large public-sector or enterprise data systems
- Strong knowledge of MLOps, NLP, forecasting, and governance use-cases