SIKKIM

GOVERNMENT GAZETTE

EXTRAORDINARY
PUBLISHED BY AUTHORITY

Gangtok **Friday 19th September, 2025** **No. 364**

GOVERNMENT OF SIKKIM
DEPARTMENT OF INFORMATION TECHNOLOGY
Secretariat Annexe-I, Sonam Tshering Marg
Gangtok, Sikkim
Email id: secy-dit-sik@nic.in visit us at: www.sikkim.gov.in

No: 641/DIT/2025 **Dated: 28.08.2025**

NOTIFICATION

In pursuance of the recommendations of the Ministry of Electronics & Information Technology (MeitY), Government of India, and in compliance with security requirements prescribed by the Reserve Bank of India (RBI), National Payments Corporation of India (NPCI), and other regulatory bodies for the protection of citizen data and electronic transactions, the Government of Sikkim hereby adopts the following policies for mandatory implementation across all Departments, Directorates, Autonomous Bodies, and State Public Sector Enterprises:

1. **National Cyber Security Policy** issued by the Government of India.
2. **National Information Security Policy and Guidelines (NISPG)** issued by Government of India
3. **User-Level Security Policy** (as notified by Government of India)

Scope of Adoption:

- The policies shall be applicable to all ICT/IT systems, applications, databases, and communication networks owned, operated, or maintained by the Government of Sikkim.
- Departments handling citizen services, financial transactions, and Direct Benefit Transfer (DBT) systems shall ensure strict compliance with NPCI security advisories.
- All projects under e-Governance, Digital India, and State IT initiatives must align with these policies for ensuring confidentiality, integrity, and availability of information assets.

Reasons for Adoption:

1. **Regulatory Compliance:** NPCI mandates strong cyber and information security measures for DBT and digital payment systems.
2. **Data Protection:** To safeguard sensitive citizen data and government records from cyber threats, hacking, and unauthorized access.

3. **Standardization:** Ensures uniform security standards across all Departments in line with national guidelines.
4. **Risk Mitigation:** Reduces risks of financial fraud, ransomware, phishing, and data breaches.
5. **Preparedness:** Strengthens incident response, disaster recovery, and resilience of State digital infrastructure.
6. **Alignment with Digital India:** Adoption supports national priorities on cyber hygiene, secure digital transactions, and trusted governance platforms.
7. **Establish a formal cyber security and information security framework** in the State of Sikkim in the absence of an existing State-specific policy.
8. **Safeguard citizen data and government digital services** from unauthorized access, misuse, and cyber incidents.
9. **Promote standardized security practices** across all Government Departments and agencies in alignment with national frameworks.

Implementation Mechanism:

The **Home Department & Department of Information Technology, Government of Sikkim** shall be the Nodal Departments for the implementation, monitoring, and review of these policies.

The designated **Chief Information Security Officer (CISO) from all the departments, Directorates, Autonomous Bodies, and State Public Sector Enterprises** shall coordinate inter-departmental compliance, oversee cyber incident response, and report on the State's overall security posture to the Government of India as and when required.

All Government Departments and agencies shall **strictly enforce these policies**, undertake regular compliance checks, and ensure proper IT asset management, user accountability, and data protection measures.

Effective Date:

This Notification shall take effect forthwith from the date of its publication in the Official Gazette.

By Order and in the name of the Governor of Sikkim

Secretary
Department of Information Technology,
Government of Sikkim