SIKKIM CYBER SECURITY POLICY

2026

[DATE]

DEPAETMENT OF INFORMATION TECHNOLOGY, SIKKIM

Table of Content

Introduction

Sikkim, a strategically important Himalayan state, is advancing rapidly in the adoption of Information Technology to strengthen governance, enhance service delivery, and promote digital inclusion. Surrounded by international borders, the state's geographical position demands heightened vigilance against cybersecurity risks. Acknowledging this strategic necessity, the Government of Sikkim is taking decisive steps to implement robust cybersecurity measures that will safeguard digital infrastructure, ensure resilience against threats, and secure long-term digital growth for its citizens and institutions.

The rise of cyberspace has created a highly dynamic environment where governments, businesses, military institutions, citizens, students, and researchers continuously interact and share information. While this interconnected ecosystem fuels innovation and growth, it also expands the attack surface for malicious actors. Cybercriminals are deploying increasingly complex malware, leveraging innovative attack techniques, and exploiting vulnerabilities across digital platforms. The emergence of AI-driven attacks, particularly through generative artificial intelligence, is expected to dominate the threat landscape in the coming years—enabling adaptive, deceptive, and highly innovative attack strategies that demand more sophisticated defences.

Recognizing these realities, Sikkim is actively developing structured and transparent IT policy frameworks to ensure accountability, efficiency, and consistency in digital governance. In this direction, the Department of Information Technology, Sikkim has already introduced an IT Data Policy as part of its broader IT strategy. Building on this foundation, the present Cybersecurity Policy has been designed to provide clear direction and establish guiding principles for protecting IT assets, digital data, and information, while also strengthening decision-making and implementation capacity across the state.

This policy directly addresses emerging challenges, aligns with national laws and global standards, and incorporates industry best practices to create a strong defence posture. It promotes a uniform and collaborative approach across departments and stakeholders, ensuring that responsibilities are well-defined and outcomes are measurable. By laying down clear objectives, scope, and procedures, this policy serves as a comprehensive framework for all concerned stakeholders, enabling secure digital operations, effective execution, and long-term sustainability.

1. Vision

"To create a secure, innovative, and citizen-centric cyberspace in Sikkim by combining strong governance, safeguarding government, citizen, and business data and compliance with emerging technologies, border-state awareness, and capacity building."

2. Objective

A. Protect Sikkim's critical information infrastructure, e-Governance platforms, and sensitive citizen data from theft, misuse, and cyberattacks. Ensure that all digital assets of the state are identified, classified, and secured with robust access control and security policies.
B. Uphold cybersecurity by enforcing encryption, access controls, and secure protocols for confidentiality; using validation, hashing, and digital signatures for integrity; and ensuring redundancy, backups, and incident response for availability.
C. Set up a State Cybersecurity Coordination Cell (SCCC) under the Department of IT as the apex body for cyber governance. Establish CERT-Sikkim as the nodal incident response entity and designate CISOs/ISOs within each government department to enforce accountability and ensure compliance.
D. Conduct continuous cyber awareness campaigns for government employees, businesses, and the public on hygiene, safe practices, phishing prevention, and grievance redressal, with special programs for women, youth, MSMEs, and first-time digital adopters.
E. Introduce cybersecurity curricula at school, college, and technical institution levels. Launch specialized training, certification, and internship programs to develop skilled professionals. Collaborate with universities and research centres to create a pipeline of cybersecurity experts for government and industry.
F. Coordinate with CERT-In, NCIIPC, law enforcement, and global cybersecurity agencies to share real-time threat intelligence. Participate in joint cyber exercises and adopt international standards to align Sikkim with global best practices.
G. Promote AI-driven defence, blockchain identity management, quantum-safe encryption, and secure cloud adoption through a Cybersecurity Centre of Excellence to drive innovation and future-proof IT ecosystem.
H. Set up a 24x7 Cyber Helpline linked to 1930, provide online resources like fact-checking tools, scam alerts, and awareness modules, and promote volunteer peer educator programs for community resilience.
I. Mandate regular VAPT, penetration testing, red-teaming, and supply chain risk assessments across all government entities. Conduct periodic cyber crisis simulations and disaster recovery drills to ensure readiness against large-scale cyber incidents.
J. Introduce departmental cybersecurity scorecards to track compliance. Publish an Annual State Cybersecurity Readiness Report for the State Cabinet and citizens. Commission third-party audits annually to ensure transparency and independent verification.

3. Strategic Pillars

The objectives are structured under a pillar-based framework, ensuring a focused approach to cybersecurity through distinct domains like governance, capacity building, technology, and awareness.
This framework provides clarity, accountability, and alignment of initiatives to strengthen resilience across government, industry, and society.

Pillar 1: Governance & Accountability

- Establish Institutional Cyber Governance
- Monitoring, Reporting & Accountability

Pillar 2: Protection & Resilience

- Safeguard Digital Infrastructure & Assets
- Ensure Confidentiality, Integrity & Availability (CIA)
- Periodic Audits & Resilience Testing

Pillar 3: Awareness & Capacity Building

- Promote Cyber Awareness & Hygiene
- Develop a Skilled Cybersecurity Workforce

Pillar 4: Collaboration & Ecosystem Development

- Strengthen National & International Collaboration
- Citizen Engagement & Grievance Redressal

Pillar 5: Innovation & Future Readiness

- Promote Innovation & Emerging Technologies

4. Scope & Applicability

1. This policy is applicable to all government departments, Government agencies of the state Sikkim. It covers protection of information assets such as Hardware, System Software, Application Software, data, Databases, Network infrastructure and electronic Services of the Departments and agencies of the State Government.

2. This policy acknowledges and is applicable to Critical infrastructure sectors (power, healthcare, finance, transport, water, etc.).

3. This policy is applicable to Private sector entities, Third parties, outsourced partners and personals providing essential digital services to departments of Sikkim or handling citizen data.

4. This policy is applicable to Educational and research institutions connected to the state Network.

5. This policy applies to Citizens and businesses engaged in online services or handling sensitive data.

6. Pillar 1

Governance & Accountability

The Government of Sikkim shall, within a time-bound manner, create a well-defined institutional structure to oversee and enforce cybersecurity across all state departments, agencies, and affiliated entities. A State Cybersecurity Coordination Cell (SCCC) shall be established under the Department of IT as the apex authority. CERT-Sikkim shall be set up and to be notified as the nodal incident response agency, ensuring round-the-clock monitoring and rapid response capabilities. Each department shall designate a Chief Information Security Officer (CISO) or Information Security Officer (ISO), responsible for implementing security directives, ensuring accountability, and reporting compliance. Annual audits, departmental scorecards, and monitoring dashboards shall be institutionalized, to uphold transparency, enforce responsibility, and ensure that cybersecurity remains an integral part of governance and service delivery in the state.

6.1 Policy Agenda

i. At the apex level, a State Cybersecurity Apex Committee shall be constituted under the chairmanship of the Chief Secretary, Government of Sikkim, within 30 days of the Gazette notification of this Policy. The Apex Committee shall include Head of Department of key departments such as IT, Home, Finance, Police, Disaster Management, Tourism, Education, and Health, along with the Director General of Police, the State IT Secretary, NIC , SeMT and the Head of CERT-Sikkim. This committee shall provide strategic direction, approve statewide cybersecurity policies and roadmaps, review annual cybersecurity readiness reports, and coordinate with national bodies such as the National Cyber Security Coordinator (NCSC), CERT-In, and NCIIPC.

ii. At the departmental level, Within 45 days of policy notification, each department shall form a Cybersecurity Steering Committee chaired by its HOD to enforce state directives, secure critical information infrastructure, oversee vulnerability testing, and report incidents. A CISO/ISO shall be designated within 2 months to manage daily implementation, compliance reporting, and serve as the department's cybersecurity nodal officer.

iii. At the district level, District Cybersecurity Steering Committees shall be constituted under the chairmanship of the Deputy Commissioners within 60 days of policy notification. These committees shall ensure

localized enforcement of cybersecurity initiatives, conduct citizen awareness campaigns, and act as first responders to cyber incidents at the district and local body level. They shall coordinate with CERT-Sikkim and state police cyber cells for effective incident handling and reporting.

iv. As the technical arm of this governance structure, the Government of Sikkim shall establish CERT-Sikkim (Computer Emergency Response Team – Sikkim) within 1 months of this policy's notification. CERT-Sikkim shall function as the nodal agency for monitoring threats, detecting, and responding to incidents, coordinating with CERT-In, and providing technical advisories and early warnings to departments and agencies.

6.1.1 State Cybersecurity Apex committee Sikkim

The Department of IT shall constitute a State Cybersecurity Apex committee under the chairmanship of Chief Secretary and shall have the following members.

Sl No	Designation	Position
1	Chief Secretary, Government of Sikkim	Chairman
2	Director General of Police	Member
3	Head of Department, Department of Information Technology, Government of Sikkim	Member Convener
4	Head of Department, Home Department	Member
5	Head of Department, Planning Department	Member
6	Head of Department, Department of Personnel	Member
7	Head of Department, Education Department	Member
8	Head of Department, Health Department	Member
9	Head of Department, Tourism Department	Member
10	Head of Department, Finance Department	Member
11	The Director, Department of IT	Member
12	State Informatics Officer, NIC	Member
13	Chief Information Security officer, Government of Sikkim	Member
14	Representative of NCIIPC/CERT-In, GOI	As Invitee
15	Head SeMT-Sikkim, NeGD	Member
16	Director CERT-Sikkim (on constitution)	Member
17	Representative of other Departments as needed	Member

The Chairman may nominate domain experts from Industry and Academia as members of the committee.

Core Functions

I. Provide guidance about strategic inputs at the policy level to strengthen cybersecurity posture in the State.
II. Review and ensure Identification, classification and notification of Critical Information Infrastructure in alignment with NCIIPC guidelines.
III. Declare a Cyber Crisis when required and oversee in-crisis management, ensuring effective response and recovery.
IV. Review and monitor the progress of cybersecurity initiatives from time to time, and provide guidance related to necessary improvements and updates.
V. Approve, review, and update the State Cybersecurity Policy and related frameworks in alignment with national directives and the Digital Personal Data Protection Act, 2023.
VI. Approve and allocate funds required for implementation, monitoring, and enforcement of cybersecurity measures across departments and agencies.
VII. Convene meetings of the Apex Committee at least once every six months, or earlier if deemed necessary in case of cyber emergencies.
VIII. Recommend changes to the State Cybersecurity Policy, including amendments, updates, and alignment with emerging national/international standards.
IX. Oversee state-level initiatives for awareness, training, and skill development in cybersecurity.
X. Ensure effective coordination between State departments, district-level committees, CERT-Sikkim, law enforcement, and national agencies such as CERT-In and NCIIPC.
XI. Approve and publish an annual report on the State's cybersecurity readiness and maturity level for submission to the Cabinet and dissemination to stakeholders.

6.1.2 Department Level Cyber Security Steering Committee

A Department Level Cyber Security Steering Committee under the Chairpersonship of HOD of the Department shall be constituted within forty five days (45) of the notification of this policy with following constitution:

Sl No	Designation	Position
1	Head of Department	Chairperson
2	Chief/Deputy Information Security Officer (CISO) of the Department	Member
3	Nodal Officer / Head of the Department's IT Project(s) if available	Member
4	Accounts Officer of the Department	Member
5	Technical In-charge (e.g., System Administrator, Network Administrator, Database Administrator, etc.) if available	Member
6	Representative(s) from CERT-Sikkim (on constitution)	Member
7	External Consultants or Project Partners (if required)	Member

Core Functions

I. Enforce and oversee the implementation of the State Cyber Security Policy within the Department.
II. Formally appoint a departmental CISO and define his/her roles, responsibilities, and reporting mechanisms.
III. Identify, evaluate, and periodically update the Department's critical information assets, vulnerabilities, and risks.
IV. Undertake classification of data and IT assets based on criticality and sensitivity, and apply appropriate labelling and protection measures.
V. Establish mechanisms for timely detection, reporting, and response to cyber incidents, in coordination with CERT-Sikkim (on constitution) and the Department of IT.
VI. Ensure that contractors, outsourced agencies, and third-party service providers comply with prescribed cybersecurity requirements and Service Level Agreements (SLAs).
VII. Conduct training, awareness drives, and cyber hygiene campaigns for departmental employees.
VIII. Facilitate periodic audits, penetration testing, and reviews of departmental IT systems, and address audit observations.
IX. Submit compliance reports, risk assessments, and incident updates to the State Apex Cyber Security Committee every six months.
X. Recommend upgrades, policy amendments, and new measures based on emerging threats and evolving technologies.

6.1.3 District Level Cyber Security Steering Committee

A district Level cyber security steering committee under tbe chairpersonship of Deputy Commissioner of the district shall be constituted.

Sl No	Designation	Position
1	District Collector	Chairman
2	Additional District Collector	Member
3	Superintendent of Police	Member
4	District Information Officer, NIC	Member
5	Representative from CERT-Sikkim (on constitution)	Member
6	District IT Officer	Member
7	Representative from local Academia/Industry (as required)	Member

Core Functions

I. Ensure implementation of the State Cyber Security Policy within all district offices, departments, and local bodies.
II. Act as the first responder to cyber incidents in the district; establish local-level reporting mechanisms and coordinate with CERT-Sikkim (on constitution) and law enforcement agencies.
III. Maintain an updated inventory of critical digital assets in the district and identify vulnerabilities specific to district-level systems and services.
IV. Conduct cyber awareness and digital safety campaigns for citizens, schools, MSMEs, and vulnerable groups (youth, women, elderly, first-time digital users)
V. Organize training workshops and awareness drives for district government employees to promote cyber hygiene and incident preparedness.
VI. Monitor adherence of vendors, IT service providers, and contractors operating in the district to cybersecurity guidelines and contract clauses.
VII. Conduct quarterly reviews of cybersecurity implementation in the district and report findings to the Departmental Steering Committee.
VIII. Submit half-yearly reports on district-level cybersecurity posture, incidents, and awareness activities to the Departmental Steering Committee for onward submission to the Apex Committee.

6.1.4 CERT (Cyber Emergency Response Team)-Sikkim

In line with the CERT-In, the Nodal agency for responding to digital security incidents, Government of Sikkim should establish CERT – Sikkim , under the directorate of IT, Department of IT, Government of Sikkim.
CERT-Sikkim shall function as the nodal technical agency for cybersecurity incident monitoring, detection, analysis, response, and advisory services in the State. It shall operate under the administrative control of the Department of Information Technology and maintain close coordination with CERT-In, NCIIPC, law enforcement agencies, and relevant national/international cybersecurity institutions.
CERT-Sikkim shall function as an autonomous body and coordinate with all departments in Government of Sikkim.
CERT-Sikkim shall be primarily responsible for the effective implementation of Cyber Security Policy in collaboration with Head of the departments and under IT department.
CERT-Sikkim shall have the following Structure

Sl No	Designation	Position
1	Director CERT-Sikkim	Head of Organization
2	Joint Director (Operations)	Division Head – Incident Response & Forensics
3	Joint Director (Monitoring & Threat Intel)	Division Head – Monitoring & Threat Intelligence
4	Joint Director (Compliance & Audits)	Division Head – Security Audit & Compliance
5	Joint Director (Awareness & Capacity Building)	Division Head – Training, Awareness & Outreach
6	Joint Director (Research & Innovation)	Division Head – Emerging Technologies & R&D
7	Technical Analysts (SOC, Malware, Forensics, VAPT teams)	Operational Staff
8	Administrative and Support Staff	Support Functions

Core Functions of CERT-Sikkim

I. Provide necessary support to all departments in implementing their security strategies in respect to digital data, information and infrastructure to align with the objective of this policy.
II. Monitor state government IT infrastructure, collect and analyse cyber threat intelligence, and issue advisories/alerts.
III. Act as the first technical responder for reported incidents; perform malware analysis, digital forensics, and recovery support.
IV. Performing independent security audits of various applications and IT assets, vulnerability assessments, and penetration testing (VAPT) for departments, districts, and critical information infrastructure.
V. Provide Technical advisory and support to system administrators/development teams for cyber security mitigations.
VI. Issue Guidelines, Standard Operating Procedures (SOP), white papers related to cyber security
VII. Coordinate and support each department to identify the Chief information Security officer (CISO) and Information security officers(ISO).
VIII. Design and deliver training programmes, cyber hygiene workshops, periodically to CISO ,ISO, and public awareness campaigns in partnership with academic institutions.
IX. Promote adoption of AI-driven cyber defence, blockchain-based security, and quantum-resilient cryptography tailored for Sikkim's needs.
X. Act as the state's technical liaison with CERT-In, NCIIPC, law enforcement agencies, and global CERT communities.
XI. Operate a dedicated helpline integrated with Dial 1930 (national cybercrime helpline) to assist citizens and institutions in reporting incidents.
XII. Conduct statewide cyber drills and mock incident simulations to test readiness of departments and districts.
XIII. Maintain a central repository of all cyber incidents reported in the State, generate trend analysis, and recommend preventive measures.
XIV. Publish an annual report on Sikkim's cyber threat landscape, incident statistics, and state of preparedness for review by the Apex Committee.

6.1.5 Chief Information Security Officer (CISO)

The State Government shall designate a Chief Information Security Officer (CISO) to lead cybersecurity initiatives and ensure compliance with national and state-level security directives.

I. Function in accordance with the roles and responsibilities defined by the Ministry of Electronics and Information Technology (MeitY), GoI, including any amendments issued from time to time.
II. Setup its own dedicated team of experts (Cyber Security Expert, Application and Network Expert, Co-ordinators, Legal Expert).
III. Evaluate and recommend suitable strategic infrastructure, security tools and processes to enhance the security posture of the state's ICT infrastructure and applications.
IV. Establish and maintain a cyber risk register.
V. Compliance to IT Act and its amendments from time to time.
VI. Enhance departmental capacity and awareness through training and guidance on emerging threats.
VII. Provide regular advisories and policy inputs to the State Apex Committee on cybersecurity developments, risk trends, and necessary interventions.

6.1.6 Information Security Officer Of Departments

The ISO shall ensure that all departmental IT/ICT infrastructure, applications, and services comply with the State Cyber Security Policy and directives issued by the State CISO / CERT-Sikkim.

I. Conduct regular risk assessments of departmental systems and identify critical assets in coordination with the State CISO.
II. Maintain a Departmental Risk Register and report findings quarterly.
III. Act as the first point of contact for all cyber incidents in the department.
IV. Ensure timely escalation of incidents to the State CISO and CERT-Sikkim as per the defined Incident Response SOP.
V. Conduct quarterly security awareness sessions for department staff.
VI. Ensure compliance with IT Act 2000 (and amendments), CERT-In directives, and State-specific standards.
VII. Enforce role-based access controls for departmental systems.
VIII. Liaise with State CISO, NIC, and IT service providers to ensure smooth adoption of security measures.
IX. Act as nodal officer for cyber security within the department.
X. Maintain updated disaster recovery plans (DRP) and business continuity plans (BCP) for departmental IT systems

7. Pillar 2

Protection & Resilience

In an increasingly interconnected digital environment, the protection of critical information infrastructure and the resilience of IT systems are central to ensuring uninterrupted governance, service delivery, and public trust. Cyber-attacks today extend beyond simple data breaches; they can disrupt essential services, compromise citizen safety, and erode confidence in digital platforms. Given Sikkim's strategic geographic position and growing reliance on IT-enabled governance, it is imperative for the State to establish a strong cyber defence posture that emphasizes both protection (preventing incidents) and resilience (withstanding and recovering quickly when incidents occur). This requires safeguarding the State Government's hardware, software, applications, networks, and databases against both existing and emerging cyber threats, while also preparing contingency measures such as disaster recovery, redundancy, and crisis management planning.

The agenda under this pillar is not only to prevent cyber incidents but also to ensure continuity of government services and citizen-facing applications, even in the face of sophisticated attacks. To this end, the State shall adopt a structured framework built around five key components:

(i) Protection of critical assets.
(ii) Secure development and application protection.
(iii) Change, incident and problem management.
(iv) Security of digital services and communication.
(v) Endpoint and infrastructure security.

Together, these components ensure end-to-end protection of systems, data, and services, while also institutionalizing mechanisms for swift detection, effective response, and rapid recovery from cyber incidents, thereby creating a resilient and trustworthy digital ecosystem for the State of Sikkim.

7.1 Protection of Critical Assets

This policy mandates the identification, protection, and resilience of critical assets that are vital to the functioning of Sikkim's digital governance ecosystem. These assets include financial systems, healthcare services, emergency response mechanisms (fire, police, disaster management), transportation, utility services, and telecommunications. Any compromise of such assets could result in severe disruption of governance, compromise of citizen safety, loss of public trust, and significant economic impact.
Accordingly, the Government of Sikkim directs all departments, agencies, and associated stakeholders to adopt a structured approach towards

safeguarding these critical assets by ensuring comprehensive risk assessment, layered security architecture, continuous monitoring, and strict compliance with CERT-Sikkim directives.

I. All State Government departments, through their Departmental CISOs/ISOs, shall undertake a comprehensive risk assessment within 90 days of this policy notification to identify and classify their critical assets/applications, including data, systems, networks, physical infrastructure, personnel, and third-party service providers.
II. Each department shall maintain and update a Critical Asset Register annually and share the list with CERT-Sikkim for oversight and verification.
III. Departments and their System Integrators shall adopt a layered security strategy, including:
    a. Secure architecture design,
    b. Strong authentication and authorization controls,
    c. Data encryption,
    d. Secure Development Life Cycle (SDLC) practices,
    e. Regular patch management,
    f. Continuous monitoring and logging,
    g. Host intrusion detection and prevention,
    h. Incident response planning,
    i. Periodic security awareness and training for staff,
    j. Third-party/vendor risk management mechanisms.

IV. Data protection measures shall align with the DPDP Act, ensuring lawful, purpose-limited, and secure handling of personal data.
V. CERT-Sikkim shall conduct periodic security assessments, penetration testing, and ethical hacking exercises on critical assets. Findings shall be shared with asset owners, who must implement mitigation measures within the prescribed timeline (maximum 30 days from reporting).
VI. Departments managing critical assets shall conduct annual Information Security (IS) audits using CERT-In empanelled vendors, with oversight from CERT-Sikkim. Audit reports and corrective action plans must be submitted within 45 days of audit completion.
VII. In case of any major vulnerability or threat identified in critical systems, if not resolved within the stipulated time, CERT-Sikkim shall be empowered to isolate, suspend, or disconnect the affected application from the State network until remediation is complete.
VIII. Departments shall adopt a policy of continuous improvement in cybersecurity practices, aligning with national standards, emerging threats, and guidelines issued by CERT-In, NCIIPC, and MeitY.

7.2 Secure development and application protection.

This policy directs that all applications developed, procured, or maintained by the Government of Sikkim shall embed security throughout the Software Development Life Cycle (SDLC), ensuring that security is not treated as an afterthought but as an integral design principle. From code review and vulnerability scanning to safe hosting and periodic penetration testing, security measures shall be institutionalized as a mandatory compliance requirement.

I. All departments shall integrate security checkpoints (secure coding guidelines, code review, threat modelling) at every stage of application development and procurement.
II. Any application developed in-house or through vendors must undergo security audit and Vulnerability Assessment & Penetration Testing (VAPT) by CERT-In empanelled agencies before deployment.
III. No application shall be hosted in the Sikkim State Data Centre (SSDC) or departmental infrastructure without a valid "Safe Hosting Certificate" issued by CERT-Sikkim or empanelled agencies.
IV. Any major update or system change to an existing application shall trigger a fresh audit and VAPT exercise before re-hosting.
V. Departments shall enable real-time log monitoring, intrusion detection, and alert mechanisms for all critical applications
VI. All vendors, developers, and system integrators shall include security obligations in their contracts (e.g., patch support, vulnerability resolution timelines, incident reporting).
VII. Every application in use by government departments must be re-certified annually for security compliance by CERT-Sikkim.
VIII. CERT-Sikkim shall be empowered to suspend or revoke access/hosting of applications found non-compliant with these directives until the issues are resolved.
IX. Every Applications must integrate security and data-protection controls from the requirements and architecture stage, aligning with the *Digital Personal Data Protection Act (DPDP), 2023*.
X. Systems shall adopt *privacy-by-default* configurations that limit collection, storage, and processing of personal data to the minimum necessary.

7.3 Change, Incident & Problem Management

This policy underscores the need for a robust Incident Response (IR) framework to detect, contain, and recover from cyber-attacks swiftly, minimizing disruption to governance and citizen-facing services

I. A standardized Incidence Response framework shall be notified within 90 days of policy adoption.
II. All incidents must be reported to CERT-Sikkim within 6 hours of detection, in line with CERT-In directives.
III. CERT-Sikkim shall issue sector-specific playbooks (finance, health, utilities, citizen services) to guide departments during cyber incidents.
IV. The Apex Committee shall have authority to declare a State-level Cyber Crisis and activate cross-department coordination.
V. Every incident shall undergo a Root Cause Analysis (RCA) within 15 days of closure, and lessons learned shall be shared with CERT-Sikkim.

7.4 Security of digital services and communication.

This policy recognizes that citizen-facing digital services (such as e-governance portals, payment gateways, utility service applications) and official communications (email, e-Sign, social media, and collaboration platforms) form the backbone of the State's digital ecosystem.

Citizen-facing platforms shall display data privacy notices, obtain explicit consent before collecting personal data, and ensure right-to-withdraw mechanisms in compliance with the DPDP Act.

7.4.1 Electronic Signature (e-Sign)/Digital Signature Certificate

An electronic signature (e-Sign) is an electronic symbol or process, logically associated with a document, executed with the intent to sign the document.

I. All approvals, certificates, and official documents issued through digital platforms shall be authenticated using e-Sign/Digital Signature Certificates.
II. e-Sign shall be implemented across all departments delivering citizen-centric services.
III. e-Sign should be provided to all approving authorities in relevant departments to authenticate citizen-facing documents and approve files and workflows processed through e-Office or ERP systems.
IV. CERT-Sikkim shall provide user training for seamless e-Sign adoption.
V. Departments currently using DSC devices shall mandate the users to register and promote the use of e-Sign for all certification and approvals.

7.4.2 E-mail SECURITY

Departments shall recognize e-mail as a critical official communication tool and implement necessary safeguards to protect against phishing, malware, spam, and unauthorized access.

I. All official communications shall be carried out only through gov.in / sikkim.gov.in domains. Use of private email IDs for government work is prohibited.
II. *Sender Policy Framework (SPF)*, *DomainKeys Identified Mail (DKIM)*, and *Domain-based Message Authentication, Reporting and Conformance (DMARC)* protocols, along with anti-malware scanning and email encryption, shall be implemented across all departmental servers.
III. User awareness training, incident response plan, e-mail usage policies, monitoring and alerts, Data Loss Prevention (DLP) and backup & recovery
IV. e-Mail backups shall be archived and ensured by the department's IT teams
V. CISOs of the department shall frame the department's guidelines for the e-Mail and Password policy and its usage.
VI. CERT-Sikkim shall issue phishing alerts and advisories to departments and citizens.
VII. Implementation of cybersecurity guidelines for government employees, as published by MeitY, shall be ensured by all departments, and CERT-Sikkim shall monitor compliance and provide periodic review reports.

7.4.3 Password Policy

To reduce the risk of unauthorized access or data breaches resulting from weak or compromised passwords, departments shall issue guidelines for creating, managing, and protecting passwords.

I. Two-Factor Authentication (TFA) or Multi-Factor Authentication (MFA) shall be adopted for accessing sensitive systems or resources.
II. To reduce the risk, password must be changed every 45 days.
III. All users shall create complex passwords containing uppercase and lowercase letters, numbers, and special characters, with a minimum length defined by departmental standards.
IV. Password reset or recovery shall be implemented, ensuring user identity verification through alternate means such as security questions or biometric authentication.
V. Departments shall conduct regular compliance monitoring, enforce account lockouts, and initiate disciplinary action in case of password policy violations.

VI. Implementation of cybersecurity guidelines for government employees, as published by MeitY, shall be ensured by all departments, and CERT-Sikkim shall monitor compliance and provide periodic review reports.

7.4.4 Social Media Policy

I. Departments shall designate authorized personnel or nodal officers responsible for managing official social media accounts and ensuring that only approved representatives post or respond on behalf of the department.
II. Content shared through official handles shall be verified, accurate, and non-sensitive in nature. No classified, confidential, or internal information shall be posted on public platforms.
III. Departments maintaining official social media handles must register them with the Department of IT & CERT-Sikkim.
IV. MFA, periodic credential changes, and restricted access shall be enforced for all official Social Media accounts.
V. All officials handling social media accounts shall undergo periodic awareness and capacity-building sessions on safe social media practices and cyber hygiene.
VI. Account recovery options, such as alternative e-mail addresses or phone numbers, shall be configured for all official social media accounts. These recovery details must be kept secure, verified, and regularly updated to ensure timely and authorized account recovery in case of compromise.
VII. CERT-Sikkim shall collaborate with Police and State PR Dept. to establish a misinformation monitoring & rapid response mechanism for viral false news or cyber scams.

7.5 Endpoint & Infrastructure Security

This policy mandates that all user endpoints including desktops, laptops, mobile devices, tablets, and Point of Sale (PoS) terminals to be secured at the same standard as departmental servers and core IT infrastructure. As endpoints often serve as the entry points for cyber threats, securing them is critical to maintaining the integrity of the entire digital ecosystem of Sikkim. Departments shall adopt a layered defence approach, incorporating the following measures:

I. **Network Isolation:** Segregate sensitive systems to limit attack surface and prevent lateral movement of threats.
II. **Separate Domain Trees:** Departments shall create separate security domains for user accounts and resources to reduce the risk of credential theft.
III. **Antivirus and Endpoint Protection Management:** Deploy state-approved antivirus and Endpoint Detection & Response (EDR) tools, ensuring real-time monitoring and centralized incident reporting.
IV. **Patch and Firmware Management:** Enforce regular and automated updates across operating systems, applications, and network devices to reduce vulnerabilities.
V. **Server Monitoring and Logging:** Ensure 24x7 monitoring of critical servers and databases, with Security Information and Event Management (SIEM) integration through the State Security Operations Centre (SOC)
VI. Endpoints handling personal data shall have encrypted storage, access logging, and automatic data erasure features to comply with data retention and protection mandates under the DPDP Act.

7.6 Data Protection & Privacy Compliance

I. All departments shall ensure compliance with the Digital Personal Data Protection Act, 2023, particularly in the collection, processing, storage, sharing, and disposal of personal data.
II. Personal data of citizens shall be used only for legitimate, consent-based purposes and retained for no longer than necessary.
III. Departments shall designate Data Protection Officers (DPOs), preferably the departmental CISOs/ISOs, to oversee data governance and privacy compliance.
IV. Personal data breaches must be reported to CERT-Sikkim and the Data Protection Board of India within the stipulated time frame under DPDP Act.

V. Data localization, anonymization, and secure transfer controls shall be implemented for all state applications handling personal or sensitive citizen data.
VI. All third-party vendors or cloud service providers handling citizen data must sign Data Processing Agreements (DPAs) ensuring DPDP compliance.
VII. Departments shall follow privacy-by-design and data minimization principles in developing digital platforms and citizen services.

8. Pillar 3

Awareness & Capacity Building

This policy recognizes that technology alone cannot ensure cybersecurity .Human awareness and capacity are equally critical. Cyber threats often exploit user negligence or lack of knowledge, making it essential to build a cyber-secure culture across government, businesses, and citizens. For Sikkim, with its growing reliance on e-Governance and digital platforms, cyber awareness and training are fundamental to safeguarding services and ensuring trust.
The agenda under this pillar is to establish sustained awareness programs, capacity-building initiatives, and academic-industry collaborations to create a well-informed citizenry and a skilled cybersecurity workforce.

I. This policy mandates all departments to conduct quarterly cyber awareness workshops covering phishing, password security, and safe IT practices under the leadership of Department Heads in coordination with CISOs/ISOs, to be initiated within 90 days .
II. Every employee of the State Government shall complete mandatory e-learning modules on cybersecurity hosted by NIC/CERT-Sikkim. The Department Heads shall ensure compliance.
III. The Department of IT, in collaboration with the Department of Information and Public Relations, shall launch statewide cyber hygiene campaigns through TV, radio, social media, and local bodies within 120 days of policy notification.
IV. The Department of IT, in consultation with the Departments of Women & Child Development and MSME, shall design and roll out targeted cyber awareness programs for women, youth, elderly, start-ups, and MSMEs.
V. District Cyber Committees, in partnership with NGOs and Self-Help Groups (SHGs), shall train community cyber volunteers as peer educators
VI. The Department of Education, in consultation with the State CISO, shall integrate cybersecurity modules into school and university curricula within 1 year of notification.
VII. The Department of IT shall establish a Cybersecurity Centre of Excellence (CoE) in collaboration with academic institutions for specialized training and certification within 2 years.
VIII. Each department shall designate a Cyber Awareness Nodal Officer responsible for coordination with the State CISO and CERT-Sikkim within 60 days of notification of this policy.

9. Pillar 4

Collaboration & Ecosystem Development

In today's interconnected cyber landscape, no single institution can address the challenges of cybersecurity in isolation. Effective protection and resilience require coordinated efforts among government departments, industry, academia, civil society, and citizens. For Sikkim, collaboration is especially important given its strategic position, reliance on IT-enabled governance, and the growing sophistication of cross-border threats. This pillar seeks to establish robust institutional linkages at the state, national, and international levels, while fostering a vibrant local cybersecurity ecosystem through active engagement of private sector, startups, and research institutions.

I. CERT-Sikkim, in coordination with CERT-In, shall create a real-time threat intelligence sharing mechanism for rapid dissemination of alerts and advisories across all state departments.
II. The Department of IT shall develop formal MoUs with academic and research institutions (such as NIT, IIIT, Sikkim University, etc.) to promote joint research, cyber labs, and student internship programs in cybersecurity.
III. The State Government shall encourage public–private partnerships (PPPs) for establishing Security Operations Centres (SOCs), forensic labs, and cyber ranges, with the first such partnerships to be finalized within 1 year.
IV. Law enforcement agencies (Police Cyber Crime Cell) shall collaborate with CERT-Sikkim and the Judiciary to establish cyber forensic and incident handling frameworks, ensuring standard operating procedures (SOPs) are developed.
V. The State CISO, in collaboration with the Department of Industries, shall create an innovation cluster for cybersecurity startups and SMEs.
VI. The Department of IT shall actively participate in national and international cybersecurity exercises coordinated by CERT-In, NCIIPC, and allied partners.
VII. An Annual Cybersecurity Ecosystem Summit shall be organized by the Government of Sikkim to bring together government, industry, academia, civil society, and international experts to review developments, share innovations, and foster collaborations.
VIII. coordination with the MeitY, and NIC for data privacy incident reporting and compliance.

10. Pillar 5

Innovation & Future Readiness

To strengthen the State's cybersecurity posture and ensure preparedness against evolving threats, departments shall promote innovation, research collaboration, and adoption of next-generation security technologies.

I. CERT-Sikkim shall continuously engage with research agencies, academic institutions, and centres of excellence to evaluate and adopt emerging cybersecurity technologies for securing government IT infrastructure and applications.

II. All departments shall incorporate *cybersecurity-by-design* and *privacy-by-design* principles in system architecture, software development, procurement processes, and infrastructure projects to ensure resilience and data protection from inception.

III. Focus areas under this policy shall include research and development in AI security, IoT protection, blockchain-enabled governance, and quantum-safe cryptography. Emerging technologies such as blockchain for security, homomorphic encryption, deception technologies, behavioural biometrics, and container security shall be progressively adopted to counter sophisticated cyberattacks.

IV. CERT-Sikkim shall establish mechanisms for continuous analysis of malware trends, phishing patterns, and dark web activities, and develop AI-driven threat intelligence dashboards to support proactive defence and incident prediction.

V. Departments shall encourage collaboration with startups, research incubators, and cybersecurity solution providers to pilot innovative tools and frameworks aimed at enhancing the State's cyber resilience and future readiness.