English Translation

National Cyber Security Policy, 2023

1. Background:

With the rapid advancement of information technology, significant changes are occurring in social interaction, public service delivery, and the flow of information. Through the use of secure information technology, transparent and effective public service management is expected. With the continuous development of information technology, its growing use, and increased mobility, unauthorized access to information technology systems has become a day-to-day problem. Since the functioning of the state, development management, public service delivery, and citizens' daily activities now depend on information technology, making the information technology system more reliable and secure is essential to enhance the trust of the general public in services delivered through its use. It has become necessary to ensure defense against cyber-attacks on information systems from national and international levels. To implement the global values of citizens' rights, as well as the fundamental rights ensured by the Constitution of Nepal, there is a need for a national cyber security policy. In this context, to minimize the harm caused by cyber-attacks on information technology and to safeguard against potential future threats, a national cyber security policy has been formulated.

2. Past Efforts:

In Nepal, computer technology was used for the first time in 1971 A.D. to process data for the National Census. In 1974 A.D. the first institution related to computers, named the Center for Electronic Data Processing, was established in Nepal. Its name was later changed to the National Computer Center. With the implementation

of the National Communication Policy, 1992 A.D., Telecommunication Act, 1996 A.D. and Telecommunication Regulation, 1997 A.D. the nation entered an open and competitive era in the telecommunications sector. The Information Technology Policy implemented in 2000 A.D. put forward the concept of information technology as an instrument to achieve the broader goal of the country's development. Likewise, Information Technology Policy, 2010 A.D. promulgated with the goal to reduce the poverty while achieving the goal of social and economic development. In that policy stress was given towards the robust information security and data privacy while using information technology.

Information and Communication Policy, 2015 A.D. has stress in addressing the dimensions including assurance to security and trust in use of information technology, development of system to prevent cyber-crime and prosecution, identification, prevention and defense of cyber-attacks. Periodic Plans has also emphasized in subjects of cyber security. Various activities related to cyber security are also being carried out in both the public and private sectors.

3. Present Condition:

The Constitution of Nepal, under its State Policy, incorporates ensuring easy and simple access to information technology for the general public by developing and expanding Information Technology in line with national needs and making its optimum utilization in national development. With the goal of making electronic transactions managed, secure, and reliable, and of controlling unauthorized person's access to electronic records, the Electronic Transaction Act, 2006 A.D., and the Electronic Transaction Regulation, 2007 A.D., are currently under implementation.

With goals such as promoting good governance through the use of information and communication technology, the Information and Communication Technology Policy, 2015 A.D. was formulated and is currently under implementation. This

policy includes provisions such as the establishment of a cyber security entity and addresses various dimensions including the identification, prevention, and defense against cyber-attacks, the conduction of capacity enhancement programs related to cyber security, and the establishment of a Computer Emergency Response Team to promptly respond to cyber security challenges. The National Security Policy, 2018 A.D. has addressed cyber security as one of the important aspects of national security.

The Information Technology Emergency Response Team Operation and Management Directives, 2018 A.D., were formulated and are currently under implementation with the goal of identifying cyber security risks arising from the development and growing use of information technology, as well as minimizing their impact and managing cyber security emergencies. As per this directive, the National Information Technology Emergency Response Team and the National Cyber Security Monitoring Center were established, and continuous monitoring of government information technology systems is being carried out.

The current periodic plan also emphasizes on the issues of cyber security and privacy, including the establishment of a Cyber Security Monitoring Center to enhance the effectiveness of cyber security. Digital Nepal Framework, 2019 A.D. includes matters related to cyber security including establishing National Cyber Security Center. Addressing the information technology system of Telecommunication and Internet Service Providers Cyber Security Bylaw, 2020 A.D. is currently under implementation. Information Technology System (Management and Operation) Directives, 2014 A.D. and Online Child Safety Directives, 2019 A.D. are under implementation. The annual policies and programs of the Government of Nepal continuously prioritize the issue of cyber security.

4. Problems and Challenges:

With the rapid development and widespread use of information and communication technology, its security is becoming a major global concern. The risk of cyber-

attacks in information and communication technology is increasing day by day. Cyber-attacks are not limited to a specific geography but are happening globally. Increasing criminal activities related to cyber have made difficult to maintain the privacy in personal and institutional matters as well as to secure data including information technology system. To neutralize such kinds of unauthorized access and attacks attempts in information and communication technology system from national and international level there are following problems and challenges: -

4.1 Problems:

(a) Lack of effective legal provisions and institutional structures for cyber security.

(b) Lack of physical and technological infrastructure related to cyber security.

(c) Shortage of skilled human resources and research in cyber security sector.

(d) Lack of awareness related to cyber security.

(e) Lack of internal and external coordination in regard to cyber security.

4.2 Challenges:

(a) Managing policy and structural measures to reduce the risk of cyber-attacks on information communication and technology systems.

(b) Developing and utilizing skilled manpower based on timely research, and capabilities to ensure cyber security.

(c) Identifying and protecting National Critical Infrastructure.

(d) Controlling unauthorized access to public, commercial, and personal information and data.

(e) Ensuring reliable digital systems and cyber security in citizen services.

(f) Cooperating and coordinating nationally and internationally for cyber security.

5. Need for the Policy:

As rapid development in communication and information technology has transformed the world into a global village, extensive use of information technology to achieve economic and social transformation goals and to remain vigilant in cyber security necessitates strengthening existing policy and institutional capacity. The subjects related to cyber security is new as well as complex and challenging. In Nepal, there is a lack of research and capacity-based competent human resources in this sector. Issues such as cyber security, protection of intellectual property, information sensitivity, and convergence need to be addressed. Since, cyber-crime and cyber-attacks have no boundaries, there is a need for international cooperation, coordination, and collaboration to control them.

There is need to formulate the National Cyber Security Policy to enhance confidentiality, integrity, availability, authenticity, and authorization of information that is collected, processed, stored, published, and disseminated through data and information and communication technology, to enhance the risk management capacity of information systems operated by critical infrastructure providers as well as to construct the secure and resilient cyber space.

6. Long-term Vision:

Building a secure as well as Resilient Cyber Space.

7. Mission:

To ensure information and data security and protection of information technology systems through a combination of people, process and technology by developing legal and institutional structure, enhancing public awareness and developing capacity.

8. Targets:

To increase Nepal's Global Cyber Security Index (GCI) score from the current 44.99 to 60% within the next 5 years, 70% within 10 years, and 80% in the 15 years.

9. Objectives:

9.1 Establish legal and institutional frameworks to build a secure cyber space.

9.2 Protect critical national infrastructure while reducing the risk of cyber-attacks.

9.3 Enhance cyber security research, human resource development and enhancing capacity of existing workforce, to ensure a robust and strong cyber space.

9.4 Improve the reliability and security of digital technology-based services.

9.5 Exchange bilateral, regional and international coordination, knowledge sharing, and assistance to reduce cyber security related risks.

10. Strategies:

10.1 Formulation of necessary laws and standards for a secure and resilient cyber space.

10.2 Establish and strengthen institutional structures to protect information and information and communication technology systems.

10.3 Identification and protection of critical national infrastructure while managing robust and strong technology, infrastructure and systems to reform cyber security.

10.4 Develop, research and utilize the competent human resources related to cyber security.

10.5 Operation of digital literacy programs to enhance awareness related to cyber security.

10.6 Coordination and collaboration among public agencies, private sectors, and civil society to construct secure cyber space.

10.7 Cooperation with foreign countries and international organizations to improve cyber security.

10.8 Continuous monitoring for cyber security to construct safe online space.

10.9 Holding software developers or suppliers, hardware manufacturers or suppliers, or service providers accountable as required.

11. Action Plan:

<u>Related to strategy no. 10.1</u> (*Formulation of necessary laws and standards for a secure and resilient cyber space)*

11.1 Amend, refine and review existing laws to align with cyber security.

11.2 Enact laws to control cyber-crime and strengthen cyber security.

11.3 Arrangement of legal and policy mechanism to determine the standards for classification of data generated through the medium of information and technology.

11.4 Develop legal and policy frameworks as per international standards for investigation, evidence collection, and prosecution and control cyber-crime.

11.5 Formulate policies and laws to protect fundamental rights including right to information and right to privacy incorporating national, regional, and international standards.

11.6 Amend and consolidate the related laws for the protection of intellectual property and copyrights created through the medium of information technology.

11.7 Management of cyber security insurance to bear the risk occurred from cyber-attacks and cyber-crime.

11.8 Formulation of National Cyber Security Framework on the basis of international standards to implement the standards of cyber security.

11.9 Formulation and implementation of Critical infrastructure risk assessment and mitigation and incident response plans.

11.10 Formulation and implementation of business continuity plans and disaster recovery plans.

11.11 Formulation and implementation of procedure related to preparedness, protection, detection, response and recovery in the process of cyber security.

11.12 Development of technical guideline for national cyber security strategy.

11.13 Development and implementation of standards for the development, import, and use of standard software, hardware, and network device.

11.14 Manage the systems for Profiling, Licensing, software vetting of communication and information technology related institution.

11.15 Construct minimum technical standards in line with international practices related to cyber security.

11.16 Defining cyber security audit standards and auditor qualifications.

11.17 Promote the use of open standards for easy inter-system communication and data exchange between various communication technology system and service.

11.18 Implement the use of encryption while exchanging data between information technology system and service.

11.19 Formulation and implementation of special laws related to the procurement of consulting services and technical instruments in the fields of information and communication technology and cyber security.

11.20 Formulation of necessary standards for security of data centers.

Related to strategy no. 10.2 ***(Establish and reform the institutional structures to protect information and information and communication technology systems.)***

11.21 Establishment of a National Cyber Security Center to conduct research and development on cyber security issues, promote cyber security and public awareness, function as a Twenty-four hour (24/7) contact agency for preparedness, protection, detection, response, and recovery, and to carry out digital forensic investigations and functions as regulatory agency related to cyber security.

11.22 Expansion of working areas of department of information technology in promotion and regulation of information technology as well as development and regulation of information technology system for government entity.

11.23 Capacity enhancement of the existing institution related to cyber security and cyber-crime investigation.

11.24 Development of digital infrastructure to exchange the information on cyber security attacks.

11.25 Construction of Government Owned Network-Intranet and National Internet Gateway.

11.26 Formulate and implement a National Contingency Plan related to cyber security.

11.27 A National Cyber Security Coordination Committee shall be formed and operated to coordinate and prioritize cyber security-related activities.

11.28 The Nepal Computer Emergency Response Team (NP-CERT) as well as Sectoral Computer Emergency Response Team and in province, Provincial Computer Emergency Response Team shall be formed and operated. Cyber

Security Information Mechanism shall be formed in coordination and collaboration of federal, province and local level.

11.29 Public agencies and institutions shall be encouraged to incorporate information security policies into their business plans.

Related to strategy no. 10.3 (***Identification and protection of critical national infrastructure while managing Robust and strong technology, infrastructure and systems to reform cyber security.)***

11.30 National Critical Infrastructures utilizing information and communication technology shall be identified and protected.

11.31 Public bodies and private sector entities that collect, process, use, and store critical data shall be required to undergo periodic cyber security assessments.

11.32 Arrangements shall be made for the security of individuals' online identities as well as for data security.

11.33 Arrangements shall be made for entities that collect, process, use, and store personal or institutional data to report cyber-attacks, data loss, damage, or theft to the National Cyber Security Center.

11.34 Cyber security infrastructure shall be developed and upgraded.

11.35 Arrangements shall be made to adopt existing laws, standards, and best practices related to cyber security assessment and authentication.

11.36 Measurement of National Cyber Security Maturity through the development of cyber security development indicators.

11.37 The delivery of services and data through electronic means shall be made secure and reliable.

11.38 The use of digital signatures in application software and email of government agencies shall be promoted.

11.39 A system shall be established to conduct regular security audit of hardware, software, and networks used by public and service-providing entities.

11.40 The purchase and use of domestic information and communication technology products shall be encouraged.

11.41 Ethical hacking shall be promoted to reform communication and information technology systems.

Related to strategy no. 10.4 ***(Develop, research and utilize the competent human resources related to cyber security.)***

11.42 Cyber security-related subjects shall be incorporated into school-level and higher education curricula.

11.43 In collaboration with organizations working in the field of cyber security, a Cyber Security Finishing School shall be established to develop skilled human resources in cyber security.

11.44 Skilled human resources in cyber security shall be developed in collaboration with national and international universities.

11.45 Universities shall be encouraged to conduct studies, research, and development in cyber security.

11.46 Training programs aligned with international standards shall be arranged to enhance the capacity of human resources working in cyber security within public entities.

11.47 The capacity of the Nepal Computer Emergency Response Team (NP-CERT) shall be strengthened.

11.48 Skilled human resources in cyber security shall be managed in government agencies as required.

11.49 The qualifications of Information Security Professionals in the public and private sectors shall be recognized, and arrangements shall be made for their regular capacity development.

11.50 A National Cyber Drill shall be conducted annually, involving critical service providers.

Related to strategy no. 10.5 (*Operation of digital literacy programs to enhance awareness related to cyber security.)*

11.51 For the enhancement of knowledge related to cyber security, awareness programs shall be conducted through local level by mobilizing the community.

11.52 In collaboration with federal, provincial, and local levels, public awareness programs shall be conducted up to the community level to ensure protection from cyber security risks.

11.53 Cyber security awareness programs shall be conducted targeting senior citizens, women and children, persons with special needs, and civil society.

11.54 Advisory shall be issued as needed to inform citizens about cyber security-related public concerns, incidents, and other matters.

11.55 Awareness-raising materials on cyber security shall be produced, distributed, and disseminated.

Related to strategy no. 10.6 *(Coordination and collaboration among public agencies, private sectors, and civil society to construct secure cyber space.)*

11.56 The Whole of the Society concept shall be adopted to construct a secure cyber space.

11.57 The government, private sector, and public-private partnership (PPP) model shall be adopted to develop cyber security infrastructure.

11.58 Collaboration and coordination with civil society, academic institutions, and the private sector to reduce cyber security risks.

11.59 Organizations working in cyber security shall be encouraged and regulated.

Related to strategy no. 10.7 ***(Cooperation with foreign countries and international organizations to improve cyber security.)***

11.60 A focal point shall be designated for international cooperation on cyber security-related matters.

11.61 Bilateral and multilateral cooperation shall be undertaken for capacity building, information exchange, and cyber-crime control for cyber security.

11.62 Engagement and collaboration with regional and international organizations and groups working in cyber security to reduce cyber security related risks.

11.63 Active participation in regional and international cyber security institution to reduce cyber security related risks.

Related to strategy no. 10.8 ***(Continuous monitoring for cyber security to construct safe online space.)***

11.64 The dissemination of misleading information through the use of internet and social media shall be controlled.

11.65 Online services targeting against women, children, or gender and sexual minorities shall be prohibited.

11.66 Various forms of violence and discrimination carried out through use of internet and social media shall be controlled.

11.67 The dissemination of digital content that undermines national security, spreads hatred or hostility, engages in online harassment or cyber-bullying, disrupts social or communal harmony, or promotes obscenity shall be prohibited.

11.68 The act of dissemination of spam messages shall be controlled.

Related to strategy no. 10.9 ***(Holding software developers or suppliers, hardware manufacturers or suppliers, or service providers accountable as required.)***

11.69 Software developers shall be held responsible for ensuring the quality and security of the software they develop.

11.70 Hardware manufacturers shall be held responsible for ensuring the quality and security of the hardware they manufacture.

11.71 Information technology service providers shall be held responsible for ensuring the quality and security of the services they deliver.

11.72 Suppliers shall be held responsible for ensuring the quality and security of the software and hardware they supply.

12. Institutional Arrangement:

12.1 Steering Committee:

A Steering Committee shall be formed as follows to provide overall direction, facilitation and guidance for this policy:

(a)	Minister, Ministry of Communications and Information Technology	Chairperson
(b)	Governor, Nepal Rastra Bank	Member
(c)	Secretary, Office of the Prime Minister and Council of Ministers	Member
(d)	Secretary, Ministry of Finance	Member

(e)	Secretary, Ministry of Home Affairs	Member
(f)	Secretary, Ministry of Women, Children and Senior Citizens	Member
(g)	Secretary, Ministry of Defense	Member
(h)	Secretary, Ministry of Education, Science and Technology	Member
(i)	Secretary, Ministry of Federal Affairs and General Administration	Member
(j)	Secretary, Ministry of Communications and Information Technology	Member
(k)	President, Federation of Nepalese Chambers of Commerce and Industry (FNCCI)	Member
(l)	One Subject expert nominated by the Ministry	Member
(m)	Joint Secretary (Information Technology Division), Ministry of Communications and Information Technology	Member-Secretary

Functions, Duties and Powers of the Steering Committee:

(a) Provide necessary guidance for effective policy implementation.

(b) Coordinate, facilitate, monitor and evaluate programs and activities operated under the policy.

(c) Perform other necessary functions.

12.2 National Cyber Security Implementation Committee:

(a) Structure of Implementation Committee:

To strengthen cyber security and also function as a National Cyber Security Strategic Task-Force, the following National Cyber Security Implementation Committee shall be formed:

(1)	Joint Secretary, Information Technology Division, Ministry of Communications and Information Technology	Coordinator
(2)	Director General, Department of Information Technology	Member
(3)	Controller, Office of the Certification Controller	Member
(4)	Chief, Government Integrated Data Center	Member
(5)	Director, Nepal Telecommunications Authority	Member
(6)	Director (Information Technology), Nepal Rastra Bank	Member
(7)	Under Secretary (Information Technology), Office of the Prime Minister and Council of Ministers	Member
(8)	Under Secretary (Information Technology), Ministry of Defense	Member
(9)	Under Secretary (Information Technology), Ministry of Home Affairs	Member
(10)	Lieutenant Colonel (Information Technology), Nepal Army	Member
(11)	Superintendent of Police (Information Technology), Nepal Police	Member
(12)	Superintendent of Armed Police (Information Technology), Armed Police Force Nepal	Member
(13)	Deputy Investigation Director (Information Technology), National Investigation	

	Department	Member
(14)	Representative, Press Council Nepal	Member
(15)	Three subject experts (including at least one woman) nominated by the Ministry from Universities academicians/Private Sectors/CAN Federation	Member
(16)	Chief, National Cyber Security Center	Member-Secretary

(b) <u>Functions and Duties of Implementation Committee:</u>

The Implementation Committee shall perform the following tasks and present them to the Steering Committee:

(1) Identify areas requiring timely improvements in cyber security-related Acts, regulations, policies, strategies, standards and action plans.

(2) Coordinate and prioritize cyber security-related activities.

(3) Monitor protection of national critical infrastructure.

(4) Identify minimum required qualifications for Information Security Professionals.

(5) Analyze cyber security incidents.

(6) Determine necessary steps to be taken considering potential risks of cyber-attacks.

(7) Identify risk assessment, emergency plans, and determine potential risk mitigation measures.

(8) Coordinate with other agencies for cyber security research and skilled human resource development.

12.3 Roles and Responsibilities of Concerned Agencies:

The Ministry of Communications and Information Technology shall have the leading role in implementing this policy. Line ministries shall be responsible for effective implementation of sectoral strategies and action plans.

13. Financial Aspects:

National and international resources and means shall be mobilized to achieve the goal of Cyber Security Policy.

14. Legal Framework:

Necessary laws shall be formulated and existing laws shall be reviewed as required for policy implementation.

15. Monitoring and Evaluation:

(a) The Steering Committee shall have primary responsibility for monitoring policy implementation.

(b) This policy shall be reviewed annually and revised periodically.

16. Potential Risks:

(a) Difficulties in obtaining cooperation from stakeholders.

(b) Difficulties in securing services and accessing information systems of critical infrastructure providers.

(c) Potential difficulties in managing skilled cyber security related human resources.