National Cybersecurity Policy, 2016

Draft – Not Approved
August 2016

TABLE OF CONTENT

1. Background

1.1 The government of Nepal defined key priorities with regard to the development of ICT in the 2015 National Information and Communication Technology (ICT) Policy. This includes an increase of broadband access and measures to strengthen and stimulate the e-commerce sector. Based on the policy ICT will play an increasing role in various sectors – from health to education.

1.2 The National Information and Communication Technology Policy highlights the importance of building confidence and security. It underlines the need to protect fundamental rights of the citizens as well as enable the investigation of crime.

1.3 Without any doubt ICT offers unique opportunities for the government, people and businesses in Nepal. Experiences with digitalization in other countries underline the potential. ICT has the potential to stimulate the economy and strengthen the service sector. It can ease the access to knowledge and play an important role in education – not only in developed parts of the country but especially in rural areas. And of course ICT can help to improve the efficiency and reliability of national critical infrastructure such as electricity supply and government services. However, at the same time it is necessary to be mindful, that the integration of ICT is going along with risks and requires risk assessment, risk management and countermeasure in order to minimize such risks and maximize the benefits. While increasing connectivity will support the development of the service sector Cyber attacks have the potential to harm both businesses and private users. Students will benefit from access to knowledge but it is important to be mindful that the same technology provides access to illegal and harmful content. And while ICT can support the operation of critical infrastructure such essential services can in future also be attacked remotely through networks that connect them.

1.4 The government, just like the United Nations and other countries in the region and around the world strongly believes that the potential of ICT by far outweighs the risks. It decided to support the on-going activities to strengthen the use of ICT within the implementation of the ICT Policy by adopting this National Cybersecurity Policy (the Policy) in addition. The Policy builds upon existing policies and sets out the Goals, and Objectives for Nepal in maximizing safety and security in relation to the use of ICT. It pays particular attention to the National ICT Policy, in particular policy issue 7.21 that deals with building confidence and security in ICT. It also reflect – among others - the aims of the Millennium Development Goals, draws upon the recommendations related to ICT arising from the Final Acts of the ITU Plenipotentiary Conference (Busan, 2014) and the ITU Global Cybersecurity Agenda.

1.5 The Policy has been developed by Nepal Telecommunication Authority with technical assistance from International Telecommunication Union (ITU). Discussions were initiated with national, regional and international experts to ensure a broad participation including governmental, non-governmental and open stakeholders consultations. Prior to the process of drafting the policy the situation in the country as well as expectations from the public and private sector were assessed through different instruments including a questionnaire based approach. The input generated was directly included in the drafting of this document.

2. Key Issues and challenges

2.1 Cyber threats are developing at high speed. It is important to ensure that people and businesses in Nepal have access to constantly updated information about threats as well as best practices in defending against them. Nepal will address the challenges by creating institutional capacities within the country that monitor developments and provide related services, guidance and information.

2.2 Today Cyber attacks are largely transnational and offenders act with a great degree of sophistication. In order to effectively deal with those threats international cooperation is key. Nepal will address the challenges by bringing its institutional capacities as well as policy and legal framework in line with international best practices.

2.3 Strong institutional capacities are required to constantly monitor developments in the risk landscape, provide services for government, citizens and businesses, prevent attacks and investigate those that could not be prevented. Nepal will address the challenges by strengthening existing and implement new capacities – such as National Computer Emergency Response Team (CERT)- NepCERT.

2.4 No government, neither in developing nor highly developed countries, is single-handed capable of protecting businesses and citizens from the all-possible Cyber threats. Nepal will address the challenge by defining focus areas for government action; combine this with strong private-public-partnership (PPP) and encouraging and empowering business as well as citizens to take preventive measures.

2.5 The prevention of attacks, the detection off illegal activities as well as the recovery requires skilled experts. Currently there is a lack of such experts in Nepal. Nepal will address the challenge by supporting the process of creating expertise within the country.

2.6 In order to respond to trends and new developments the government in general and the specialized institutions require up-to-date information about attacks in the country. Nepal will address the challenges by developing and reporting mechanism. In this regard the government is committed to support a bi-directional exchange.

3. National Vision

Citizens of Nepal, businesses and government to enjoy the full benefits of a safe, secure and resilient cyber space, enabling them to get access to knowledge and share information while understanding and addressing the risks, to reduce the benefits to criminals, secure stable economic and social development and protect essential democratic structures.

4. Guiding Principle

4.1 With this national vision the government aims to protect the people, businesses and government agencies and provide the necessary secure framework to achieve the aims developed and defined in the National ICT Policy.

4.2 The implementation of the policy shall be guided, among other things by the national vision. The implementation will be Government-led and Private Sector-driven. Public-Private-Partnership (PPP) shall form one of the bases for implementation of this policy.

4.3 The government is aware that the measures defined by the ICT Policy, will have a major impact on the connectivity within the country. In addition the government is aware that with the increase in bandwidth new services will be available and that some of them will go along with security concerns. As a consequence the government gives priority to a timely implementation of this policy to ensure that Cybersecurity measures are implemented in parallel to the increase in services and connectivity.

4.4 This policy shall be supported by appropriate legislation and regulations. The legislation will especially focus improving the fight against criminal abuse of ICT and Cybercrime. Regulations will especially focus on technical minimum standards in relation to Cybersecurity.

4.5 The implementation of this policy shall take into account relevant national, regional and global best practices in building confidence and security in ICT by cultivating strong linkages with the applicable UN GA resolutions as well as the ITU recommendations.

5. Goals of Cybersecurity Policy

5.1 Nepal will develop technical guidelines and other technical and organizational components of a National Cybersecurity Strategy. The documents should take into account national demands as well as international best practices and be developed by a dedicated Cybersecurity Working Group.

5.2 The necessary organizational structures will be strengthened with a focus on utilizing existing structures in Nepal as well as the region. This includes the setup of NepCERT.

5.3 The government, businesses and citizens in Nepal will have access to basic services and actionable intelligence related to Cybersecurity.

5.4 Bringing the level of knowledge about Cybersecurity and ways to protect against cyber threats of the citizens and businesses of Nepal to highest levels and providing expertise as well as basic tools and services for citizens, businesses and government;

5.5 Creating an environment that allows the constant exchange of information among stakeholders.

5.6 The legal and policy framework in Nepal will be strengthened to meet highest regional and international standards with regard to protection of fundamental rights as well as criminalization, investigation, electronic evidence and international cooperation.

5.7 In addition, responding to the global nature of Cybersecurity threats through strengthening Nepal's ability to participate in the international cooperation against such threats.

5.8 Creating a safe environment for children by reducing specific Cyber threats and implementing technical protection measures.

5.9 Strengthening the protection of critical infrastructure with regard to cyber threats.

5.10 The policy will help businesses to diversify and develop new markets, laying the foundations for a prosperous future.

5.11 Nepal's cyber security policy shall maintain a balance between individual and collective security as well as preserving right to privacy and fundamental freedoms of Nepali citizens.

6. Development of a National Cybersecurity Guidelines

6.1 A Cybersecurity working group (National Cybersecurity Strategy Working Group – NCSWG) will be formed with the following structure.

Secretary, Ministry of Information and Communication	Chairperson,
Law Enforcement Agency	Member
Secretary, Ministry of Science and Technology	Member
Secretary, Ministry of Home Affairs	Member
Secretary, Nepal Telecommunications Authority	Member
Representative Private Sector	Member
Representatives Domain Expert	Member
Representatives Civil Society	Member

With regards to classified components the working group should be limited to members with adequate security clearance.

6.2 NCSWG shall develop a set of specific Cybersecurity guidelines. It should go beyond policy statements and focus on concrete measures. It should address the following issues: Responsibility within the government and private sector, definition of processes, technical specifications and risk assessment and emergency plans. The responsibility section should clearly point out the roles and responsibilities of different institutions. This may include technical as well as management responsibilities. The government underlines that maintaining a sufficient crisis and incident management is a key component of any Cyber defence strategy. Taking into account the potential devastating impact of cyber attacks, clear rules and procedures are required that define under which circumstances certain people and institutions need to take action. The processes shall define Cybersecurity related requirements with regard to relevant government processes. It may range from mandatory training procedures for new staff to concrete security procedures for trans-border travel. In order to provide solution-oriented guidance, processes should be described as precisely as necessary. Processes should especially include prevention, preparedness, detection, response and recovery. In addition research and development plans should be addressed in this section. Defining clear, government as well as industry-wide technical specifications for Cybersecurity, such as minimum requirements with regard to the encryption of classified documents, should overcome conflicts caused by differing standards. The risk assessment and emergency plans should provide guidance with regard to the most likely threats scenarios.

6.3 The guidelines should be developed in a way that it allows frequent updates wherever developments (either technical modifications or developments in the threat landscape) require adjustments. In addition the guidelines should clearly point out links to and interdependencies with the private sector.

6.4 NCSWG will be responsible for the coordination and prioritization of Cybersecurity research and development activities with a focus on building and strengthening a local Cybersecurity research community. It will further more identify minimum requirements and qualifications for information security professionals that will serve as basis for the development of a related curriculum.

7. Strengthening the necessary organizational structures

7.1. Creation of NepCERT

7.1.1 An independent National CERT of Nepal (NepCERT) will be created. It shall be supervised and monitored by the Ministry of Ministry of Information and Communications/Ministry of Science and Technology /Nepal Telecommunications Authority. NepCERT will be responsible for providing services related to Cybersecurity to the government, government institutions, law enforcement, businesses and the people. It should focus on promoting Cybersecurity; awareness raising; upon request supporting institutions and businesses in prevention, detection and response to Cyber attacks; maintain 24/7 points of contact; carrying out digital forensic investigations; receiving and distributing reports about incidents and auditing and providing special support to critical infrastructure provider. NepCERT shall create the necessary infrastructure for conformity assessment and certification of compliance with Cybersecurity best practices, standards and guidelines (e.g. ISO 27001).

7.1.2 The mandate of the National Information and Communication Technology Policy Implementation Steering Committee will be amended. It will provide overall guidance and define priority areas with regard to the implementation of this policy.

7.1.3 NepCERT will identify all existing government and non-government institutions that are currently active in the field of Cybersecurity and fighting Cybercrime and draft a report about the mandate, resources and experiences and analysis of potential areas for synergy, overlapping and gaps.

7.1.4 NepCERT will identify local contact points outside of Kathmandu that can facilitate the collection of input about recent developments as well as spreading information to the communities. Within this process public private partnership approaches shall be taken into consideration.

7.1.5 NepCERT will carry out a coordinated survey and assessment, to analyse how far citizens, businesses and government are affected by Cybersecurity incidents and Cybercrime.

7.2. Services to be provided by NepCERT

7.2.1 NepCERT will, upon request, provide the government, government institutions, law enforcement, businesses and the people with information about Cybersecurity. It should maintain resources to handle request, promote the adoption of global best practices in Cybersecurity and compliance, provide training material and practical information as well as refer to publically available tools. It should in addition provide on the ground advisory support to critical infrastructure provider and law enforcement agencies.

7.2.2 Wherever possible NepCERT shall cooperate with institutions and initiatives present in the country that already provide services, material and information on a non-commercial level and evaluate the possibility of building upon existing instead of developing new material.

7.2.3 NepCERT will, upon request, assist the government, government institutions, law enforcement, and businesses in planning and management of information security through a course of action such as policy making.

7.2.4 NepCERT shall facilitate and administer regular cyber security drills at a national, sectorial and entry levels in order to assess the level of emergency preparedness in combating and handling cyber security incidents.

7.3. Creating a Secure Cyber Environment-NepCERT

7.3.1 While the government is committed to protect businesses and the people in Nepal from threats related to Cybersecurity it emphasizes the importance of self-protection and underlines the responsibility of the individual. The government will support the self-protection by providing knowledge through NepCERT.

7.3.2 Each government institution and business in Nepal that utilizes ICT is encouraged to undertake an individual risk assessment, develop and implement a Cybersecurity strategy that addresses the main risks, designate a member of senior management as Chief Information Security Officer, responsible for Cybersecurity efforts and initiatives, maintain state-of-the art Cybersecurity technology that reflects it's risk landscape, implement risk assessment and risk

management processes, have business continuity management and crisis management plans in place and carry out regular exercises. Further requirements apply to the provider of critical infrastructure.

7.3.3 NepCERT shall develop a standard risk assessment framework for businesses in Nepal. Businesses in Nepal are encouraged to utilize this framework.

7.3.4 NepCERT shall develop and implement an evaluation/certification program for Cybersecurity services, products and systems.

7.3.5 NepCERT shall develop and implement technical and organizational protection measures as well as emergency plans to protect essential government services (such a eGovernment).

7.3.6 Government of Nepal through NepCERT shall promote, guide and coordinate activities aimed at improving cyber security measures by strengthening the national capacity to investigate combat and prosecute Cybercrime and other cyber related threats.

7.4. Strengthening the regulatory and legal framework- NepCERT

7.4.1 The government implemented legislation addressing issues of Cybersecurity in the Electronic Transactions Act, 2063 (2008). Under supervision of the Ministry of Law, Justice, Constituent Assembly and Parliamentary Affairs NepCERT shall carry out a review of the existing legislation related to Cybersecurity. This shall include the following areas of law: ~~privacy~~ and data protection, national security, e-commerce, freedom of information, admissibility of electronic evidence, liability of Service Providers (SPs), Children Online Protection and International Co-operation. The review shall include the identification of existing provisions that could be utilized in relation to Cybersecurity, a comparison with international best practices, a gap analysis, suggestions for amendments and the related drafting instructions. NepCERT should seek the assistance of international organizations active in this field to carry out the assessment and comparative analysis.

7.4.2 Priority should be given to the topic Cybercrime. An analysis shall include the following topics: definitions, substantive criminal law, procedural law and investigation instruments of law enforcement, criminal liability of Service Providers and international cooperation.

7.5. Capacity building of NepCERT

7.51 NepCERT shall provide a list of capacity building programs related to Cybersecurity that Nepal could benefit from. To avoid an overlapping NepCERT shall develop a roadmap that lists the different capacity activities that the country require, identify potential programs and make suggestions which programs cover which activity.

7.5.2. The Ministry of Education, the Ministry of Women, Children and Social Welfare and the Ministry of Youth and Sports will in cooperation with NepCERT and other authorities in Nepal develop a curriculum to ensure that all students at primary school and high school receive at least once a year an updated training on Cybersecurity that includes information about latest trends. Training materials, background information for teachers and sample presentations shall be developed. In addition schools should receive a questionnaire to enable them to assess the use of ICT service by students as well child specific Cybersecurity risks.

The anonymous assessment shall be carried out on an annual basis and the results shall be submitted to NepCERT and included in their annual report.

7.5.3 The Ministry of Education and the universities will in co-operation with NepCERT and other authorities in Nepal develop a curriculum for specialized training courses for IT security professionals. The aim is to have adequate number of security professionals trained to handle the security related issues in Nepal.

7.5.4 NepCERT shall develop a sustainable Cybercrime training program for law enforcement officers, Financial Investigation Unit, the judiciary and other stakeholders.

7.6. Information exchange of NepCERT

7.6.1 Citizens, businesses and governments shall be encouraged to report cyber incidents. The provider of critical national infrastructure shall be obliged to submit such reports.

7.6.2 To support the idea of information sharing, NepCERT shall develop routines to detect recent trends in relation to Cybersecurity incidents, create an emergency level system, summarizing incidents in a reporting format and providing background information, developing a network to communicate such reports through the relevant communication channels (e.g. press releases, information submitted to cooperation partners in rural areas) and submitting this information. This shall include the publication of relevant, non-confidential information on a regular basis on a publically accessible website. Once a year, NepCERT shall submit a summary report on their work and especially notifications received. It should provide the government with regular briefings and provide additional information on request. NepCERT shall ensure that the information submitted to the different stakeholders reflect their needs with regard to details (e.g. executive summary for the minister, detailed information for system administrators on technical aspects of an attack) and that information are not distributed to recipients that are not affected.

7.6.3 NepCERT shall forward report about incidents that have a potentially criminal background to the responsible law enforcement agencies. Law enforcement should create a single point of contact and ensure that the secure infrastructure provided by NepCERT is utilized. The government will form an appropriate institutional structure within the law enforcement agency to handle cases of criminal nature reported by NepCERT.

7.64 In order to facilitate the exchange of sensitive and confidential information between NepCERT and others, NepCERT shall set up a system of secure infrastructure, Communications, information collection and reporting shall – if possible - exclusively take place through such infrastructure.

7.6.5 The government recognizes the advantages of mobile communication. NepCERT should enable the possibility to submit reports from mobile devices and explore the possibility to use push services to submit information about recent attacks to citizens and businesses.

7.7. International Cooperation with NepCERT

7.7.1 To ensure that Nepal's legal framework and practice is fully in line with international best practices in relation to international cooperation. NepCERT in cooperation with the Ministry of Law, Justice, Constituent Assembly and Parliamentary Affairs and the Ministry of Foreign

Affairs will analyse the capacities of Nepal to efficiently submit requests for mutual legal assistance as well as timely respond to requests submitted to authorities in the country. NepCERT will develop recommendations for the establishment of a single point of contact. Further more, NepCERT will analyse if the technology used for sending and receiving requests as well as the availability of the contact point are in line with international best practices.

7.7.2 NepCERT will make recommendations with regard to a potential access to international or regional agreements, current processes of developing binding standards where Nepal should participate, as well as 24/7 networks (such as the Interpol Network). With regard to the evaluation of an access to existing instruments the relevance for Nepal, the reflection of legal standards and cultural specifies as well as the usefulness in cooperation with other countries shall be taken into consideration. NepCERT will seek membership of Regional and Global CERTs as required.

7.7.3 NepCERT shall carry out Global Cyber Security Index exercise to foster the culture of cyber security and build confidence and security in the use of ICT in line with ITU.

8. Child Online Protection

8.1 A Child Online Protection Working Group (COPWG) will be formed with the following structure.

Secretary, Ministry of Women, Children and Social Welfare	Chairperson
Joint Secretary, Ministry of Information and Communication	Member
Joint Secretary, Ministry of Education	Member
Nepal Police, Women and Children Directorate (DIG)	Member
NepCERT Representative	Member
Nepal Telecommunications Authority	Member
Child Related Organization	Member

8.2 COPWG will identify areas of child online protection (such as technical protection measures, curriculums for school and information material for parents and guardians) that need to be integrated in Nepal.

8.3 COPWG shall evaluate different technical measures that services providers must introduce to protect children online and parameters that shall be included in a report submitted to guardians upon request (see 8.4). Based upon the evaluation COPWG in cooperation with NepCERT will develop guidelines for technical child online protection measures. This shall include recommendations for measures how to prevent an abuse of the service.

8.4 Based upon the guidelines developed by COPWG commercial provider of Internet access in Nepal shall be obliged to provide – upon request of the user - a restricted Internet access that includes available technical measures aiming to block content that is not appropriate for children. Furthermore, the provider shall be obliged to provide – upon request of the user – a special reporting for parents or guardians that highlights the services used and other parameters defined by the COPWG.

8.5 Based upon the guidelines developed by COPWG each commercial provider of GSM mobile communication services in Nepal shall be obliged to provide – upon request - a SIM card with restricted access to services that may not be appropriate for children. The provider may not charge any additional fees for such service.

9. Protection of Critical Infrastructure

9.1 Definition and Categorization of Critical Infrastructure

The government defines critical infrastructure as the essential services that underpin Nepalese Society and serve as a backbone of Nepal's economy, security and health. The sectors included in the Critical Infrastructures are but not limited to Healthcare and Public Health Sector, Energy Provider Sector, Water and Wastewater Sector, Transportation Sector, Information and Communication Technology Sector, Food and Agriculture Sector, Financial Service Sector, Government Facility Sector, Emergency Service Sector, Law Enforcement and Judiciary, Defence Forces, Critical Manufacturing Sector and Tourism Sector. In the selection process international best practices should be used with regard to the definition of critical infrastructure. The working group will provide the NepCERT with a list of critical infrastructure provider in the country.

9.1.1 The government recognizes that with an increasing use of ICT by the citizens the dependency on the availability of information infrastructure increases. Significant parts of the today information infrastructure can be considered as critical information infrastructure as a failure or limited operation would cause tremendous impact on the vast majority of citizens. And concerns related to possible attacks against critical infrastructure are not limited to information infrastructure – various critical infrastructure providers that do not focus on information infrastructure, such as electricity and transportation provider intensively use ICT. Tremendous impact does therefore not only refer to direct damage but also indirect damages. With this policy the government lays the foundation to increase the ability of a networks and information systems operated or utilized by critical infrastructure provider to resist, at a given level of confidence, accident or malicious action that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data or the related services offered by or accessible via that network and information system.

9.1.2 The government is committed to strengthen the protection of critical infrastructure and especially critical information infrastructure provider with regard to cyber threats. This shall include the owner of critical infrastructure as well as operator of services using critical infrastructure. To ensure that the implementation of any mandatory standards is based upon the needs as well as capacities of the affected operators of critical infrastructure the government will carry out a needs and risk assessment, focusing on critical infrastructure provider, including small medium enterprises as well as large enterprises and public and private operators.

9.1.3 The government will promote a nation wide as well as regional debate, involving all relevant public and private stakeholders, to define priorities for the long term resilience and stability of critical infrastructure against Cyber attacks.

9.1.4 NepCERT will carry out the following tasks specifically focusing on critical infrastructure protection:

I. Information exchange, prevention and early warning
II. Detection with a focus on promoting security
III. Reaction
IV. Crisis Management

It will equip NepCERT with required funding to maintain adequate technical, financial and human resources to carry out in an effective and efficient manner the tasks assigned to them and thereby to fulfil the objectives of this policy goal. It will ensure that NepCERT has all powers necessary to investigate cases of non-compliance of critical infrastructure provider with their obligations and the effects thereof on the security of critical infrastructure with regard to cyber attacks. It will especially ensure that NepCERT has the power to require critical infrastructure provider to provide information needed to assess the security of their networks and information systems, including documented security policies and carry out a security audit. In this regard the government will ensure that the institution has the power to issue binding instructions to critical infrastructure provider. The government will ensure, that any obligations imposed on critical infrastructure provider under this policy goal may be subject to judicial review.

9.1.5 The government will request NepCERT to contribute critical infrastructure related issues to the development of a technical Cybersecurity guidelines. These guidelines should include critical information infrastructure elements. It should in addition maintain an incident management system as well as the necessary technical and human resources to support critical infrastructure provider in dealing with cyber incidents. The purpose of the support is not to substitute the required resources on the side of the critical infrastructure provider but to provider addition support.

9.1.6 NepCERT shall develop a national contingency plan and organise regular exercises for ~~large scale~~large-scale network security incident response and disaster recovery. Those exercises shall include latest trends and developments to allow critical infrastructure provider to prepare for attacks and cover technical components as well as risk management.

9.1.7 NepCERT will set up a working group to determine which infrastructure provider in Nepal should be considered “critical infrastructure provider”.

9.1.8 Based upon the list the NepCERT will create an initial database of critical infrastructure provider and maintain an updated database. Providers of critical infrastructures are obliged to provide the required data. The database should contain information about the size and relevance of the provider (e.g. number of households using a service), an overview about ICT utilized and the relevance for core services, a risk self-assessment, an overview about countermeasure (technical and risk management) and a list of previous incidents.

9.1.9 NepCERT will at least once a year submit a questionnaire to the provider of critical infrastructure to update the database. In addition to the above-mentioned data, NepCERT may request information about the purpose and scope of security standards as well as practical methods for satisfying security standards.

9.1.10 The provider of critical infrastructure are required to take technical and organisational measures to manage the risks posed to the security of the networks and information systems which they control and use in their operations. Having regard to the state of the art, these measures shall guarantee a level of security appropriate to the risk presented. In particular, measures shall be taken to prevent and minimise the impact of incidents affecting their network and information system on the core services they provide and thus ensure the continuity of the services underpinned by those networks and information systems. To coordinate the activities the provider of critical infrastructure shall appoint a member of senior management as Chief Information Security Officer and ensure that it earmarks a specific budget for implementing Cybersecurity measures. Based on the local requirements, NepCERT

will assess and suggest for creation and installation of organizational CERTs in those organizations providing critical infrastructures, based on capital turnover, total number of employees and total number of customers. The CERTs of provider of critical infrastructure should cooperate and exchange information with the NepCERT. Further more the provider of critical infrastructure is obliged to carry out a risk and exposure self assessment at least once a year and document this process. In addition to national exercises they should at least once a year carry out realistic exercises that simulate realistic attack scenarios and allow the provider to verify that technical measure in place are state of the art and risk management processes are adequate.

9.1.11 Based upon an analysis of the assessment the government will decide if in the future precise, mandatory minimum standards should be introduced. In this regard the government is mindful about the speed of the development, different capacities of small and large size provider and the required update of any concrete standards.

9.1.12 NepCERT may provide guidelines and promote good security and manage and monitor progress, as well as a complete set of processes to ensure preparedness, including prevention, protection, response and recovery from natural and malicious threats.

9.1.13 The government considers to introduce a certification for provider of critical infrastructure and will carry out a related feasibility study.

9.1.14 Information sharing are essential components within the response to cyber threats. In order to get a more accurate understanding of the exposure of critical infrastructure with regard to cyber attacks against the provider of critical infrastructure NepCERT will collect relevant information. At the same time NepCERT will be responsible for providing critical infrastructure provider as well as the government and government institutions with required information – especially with regard to status of readiness, incidents, trends and development. The government requests NepCERT to establish a national forum to share information and good policy practices on security and resilience of Cybersecurity in relation to critical infrastructure. This forum should include critical infrastructure provider, government institutions, law enforcement, civil society and other interested parties. NepCERT should in addition take action to foster the cooperation between the public and the private sector on security and resilience objectives, baseline requirements, good policy practices and measures.

9.1.15 The providers of critical infrastructure must classify data to different levels based on the levels of sensitivity and their access. The data shall be classified to three types: Restricted, Controlled and Public.

9.1.16 The providers of critical infrastructure shall not store restricted and/or confidential data within cloud servers located outside Nepal. In case where the cloud service provider is based in Nepal, there are no restrictions in storing such data as long. NepCERT shall assess the physical, technical and organizational security measures appropriate fort he particular cloud service provider.

9.1.175 NepCERT should investigate possibilities to foster innovation through public-private research and development projects focused on the improvement of Cybersecurity of critical infrastructure.

9.1.186 NepCERT shall develop and implement an awareness raising strategy and reach out to critical infrastructure provider within the country.

9.1.197 In order to ensure that NepCERT has access to up-to-date information about on-going developments within the country critical infrastructure providers are obliged to notify NepCERT through the secure infrastructure about any incidents in relation to ICT that has a significant impact on the security of the core services they provide. In this regard NepCERT may adopt guidelines and, where necessary, issue instructions concerning the circumstances in which critical infrastructure providers are required to notify incidents. It shall further more be entitled to It shall be entitled to define the formats and procedures applicable for the reporting. The government emphasizes that it is the intention of the policy to create a bi-directional exchange of information. NepCERT shall analyse the collected information and use it for information sharing and especially incident warning. It may inform the public, or require the critical infrastructure provider to do so, where it determines that disclosure of the incident is in the public interest. It may also inform other critical infrastructure provider about details of an attack if there is a likelihood that other critical infrastructure provider will be targeted in the near future and sharing such information allows other potentially affected critical infrastructure provider to prevent a similar attack. NepCERT will ensure that where ever possible information is anonymized prior to sharing them to protect the interests of the reporting provider.

9.1.2018 NepCERT shall regularly review polices and legislation related to cyber attacks against critical infrastructure as well as the national risk management process.

10. Implementation of policy framework

10.1 A National Cybersecurity Policy Implementation Steering Committee will be formed at the Ministry of Information and Communications with the following structure.

Minister, Ministry of Information and Communications	Chairperson
Secretary, Ministry of Information and Communications	Member
Secretary, Ministry of Home Affairs	Member
Secretary, Ministry of Science and Technology	Member
Secretary, Ministry of Women Children and Social Welfare	Member
Secretary, Ministry of Finance	Member
Chairperson, Nepal Telecommunications Authority	Member

10.2 The primary role of the National Cybersecurity Policy Implementation Steering Committee is to provide overall coordination support for the effective implementation of policy provisions along with monitoring and evaluation of policy interventions.

10.3 The Steering Committee will form a Cybersecurity Policy Implementation Sub-Committee comprising of representation from the stakeholder community and domain experts, including the private sector, to provide it with domain specific expert advice and recommendations in relation to the execution of policy provisions.

11. Formulation of National ICT Master Plan/National e-Strategies

The policy and strategy framework will be implemented through National Cybersecurity Master plan to be developed and endorsed by the Government of Nepal.

12. Resource Mobilization

The overall goals of Cybersecurity Policy will be achieved through the mobilization of both public and private sector resources. The proposed policy framework is expected to create

conditions for a secure environment that creates the foundation of future private and public sector investments. The possible grants and technical assistance from bilateral, multilateral and other international agencies could also be used.

13. Legal Arrangements

Appropriate Legal and regulatory arrangements will be made for the implementation of this policy and provisions therein if deemed necessary.

14. Monitoring and Evaluation

A monitoring and evaluation framework will be developed within the fiscal year 2073/74 (2016/17) to serve as a basis for carrying out periodic monitoring and evaluation of the execution of Cybersecurity Policy. It will be the primary responsibility of Implementation Steering Committee to carry out monitoring and evaluation of programs and policy provisions relating to cyber security.