The Federal Democratic Republic of Ethiopia

National Cyber Security Policy

June 2024

The Federal Democratic Republic of Ethiopia

National Cyber Security Policy

June 2024

Contents

Definition of Terms

In this policy, unless the context otherwise requires:-

- **Critical Information Infrastructure:** Refers to physical and digital assets, including essential services and information systems, an attack on which would severely impact public security and national interests.
- **Cyberspace:** A virtual environment comprising interconnected information, information infrastructure, information systems, and human resources that convert and utilize information as knowledge, along with the associated institutional and social culture.
- **Digital Identity:** An identity adopted or claimed in cyberspace by an individual or an institution.
- **Digital Identity Protection**: The act of safeguarding the digital identity of individuals or institutions utilizing cyberspace, preventing unauthorized access, and securing common digital identities.
- **Cyber-attack:** Malicious acts within cyberspace that include, but are not limited to, disruption of critical infrastructures, unauthorized access, data theft, psychological warfare, and other forms of cyber threats.
- **Data Privacy:** The right to personal data privacy and protection, which encompasses safeguarding against unauthorized access to personal data, preventing its disclosure to third parties without the owner's consent, and ensuring the integrity of the information.

Acronyms

FDRE	Federal Democratic Republic of Ethiopia
ICT	Information and Communication Technology
INSA	Information Network Security Administrtion

Introduction

The contemporary world is progressively digitized, with Information and Communication Technologies (ICTs) becoming foundational to all facets of life, encompassing social, economic, political, and security sectors. While this digital transformation presents immense opportunities, it concurrently introduces novel and intricate challenges, particularly within the domain of cybersecurity. Cyber threats are evolving with remarkable rapidity, posing substantial risks to national critical infrastructures, sensitive data, and the holistic well-being of citizens.

Ethiopia, akin to many nations, acknowledges the imperative need to safeguard its digital assets and cultivate a secure and resilient cyberspace. This National Cyber Security Policy (NCSP) has been meticulously developed to address these dynamic challenges, leverage the advantages of digital transformation, and robustly protect national interests within the digital realm. It meticulously delineates the strategic approach, overarching objectives, and comprehensive implementation framework requisite for establishing a formidable national cybersecurity posture.

Part One

Policy Need, Vision, Mission, and Objectives

1.1 The Need for the Policy

- An up-to-date national cybersecurity policy is essential to leverage the opportunities presented by cyberspace and to mitigate the risks associated with its complex, dynamic, unpredictable, and technologically advanced nature.
- Cyberspace significantly impacts Ethiopia's socio-cultural, political, economic, and security landscape, necessitating cybersecurity policy directions that consider the existing national context.
- It is imperative to defend against and respond to the progressively increasing cybersecurity threats, vulnerabilities, and attacks on information and critical infrastructures, particularly given the widespread ICT infrastructure development in the country.
- There is a critical need to enhance coordination and partnership among public and private institutions and other stakeholders, ensuring an equitable and complementary role in leading and administering the cybersecurity sector.
- It is necessary to develop, lead, and shape cyberspace in cooperation with the private sector, acknowledging its growing involvement in critical infrastructure and its multifaceted future potential.

- These mechanisms will facilitate the formulation of legal frameworks and regulatory systems, build research and development capabilities, and enhance awareness to effectively mitigate existing and potential cybersecurity threats and vulnerabilities.

1.2 Fundamental Assumptions

- **Government Leadership and Commitment:**
  The government will provide strategic direction for the coordinated allocation of resources and capabilities necessary for the effective implementation of the National Cybersecurity Policy (NCP).

- **Shared Responsibility:**
  Recognizing that cybersecurity is a concern for all stakeholders, citizens, the government, the private sector, and other relevant entities will implement the NCP with a strong sense of ownership.
- **Rule of Law:**
  All cybersecurity activities will be conducted based on the rule of law, respecting constitutional rights, freedoms, equitable benefits of citizens, and ensuring transparency.
- **International Cooperation and Partnership:**
  Strong international cooperation and partnerships will be fostered, acknowledging the cross-border nature of cybersecurity threats, vulnerabilities, and attacks.
- **Ethiopian Values:**
  The National Cybersecurity Policy will be implemented in a manner that respects and upholds Ethiopian values.

1.3 Vision

To foster a globally competent and resilient national cybersecurity capability that positions Ethiopia as a model for African prosperity.

1.4 Mission

To protect the national interests of the country by building a self-reliant cybersecurity capability that safeguards the nation's information and critical information infrastructure from cyber

1.5 Objectives

- To build a resilient cybersecurity capability that can monitor, detect, and warn against threats and vulnerabilities, and promptly prevent and respond to cyberattacks.
- To ensure that cybersecurity, in its process and outcome, protects citizens' privacy, human rights, and democratic rights, thereby assuring sustainable peace and development.
- To establish strong national, regional, continental, and international partnerships and collaboration on cybersecurity.
- To build indigenous technological capabilities and deploy systems that sustain critical infrastructure and information resources through Research & Development (R&D) that meet international standards.
- To foster a rational and aware society that uses cyberspace with knowledge and reason by building a national cybersecurity culture.

1.6 Principles

- **Responsibility:** All public and private institutions are responsible for protecting the security of their information, information infrastructures, and systems, as well as ensuring the secure and proper use of cyber technology products and services.
- **Resilience:** It is imperative to sustain cybersecurity by withstanding challenges in cyberspace, maintaining resilience, and remaining stronger and more agile.
- **Sovereignty-Centric:** The country must ensure that its cyber sovereignty and national interests remain intact in all its international cooperation, negotiations, and agreements related to cybersecurity.
- **Coordination and Partnership:** As ensuring cybersecurity requires the participation of all concerned bodies, public and private institutions, and other stakeholders must work in coordination and partnership.
- **Global Compliance:** The task of securing cyberspace is an international practice and will be accomplished in alignment with international laws, principles, and agreements.
- **Balancing Privacy and Security:** The NCSP will be implemented in a way that strikes a balance between the protection of cybersecurity and respecting the rights and privacy of individuals.

1.7 Scope of the NCP

The National Cybersecurity Policy (NCP) applies to all public, private, and non-governmental institutions, as well as all citizens within the country

Part Two

Focus Areas and Strategies

2.1. Policy Issues

Maintaining state sovereignty in the cyber world is increasingly challenging. A state that has not developed competent cyber capabilities will find its cyber sovereignty compromised. This is largely due to the difficulty in accessing technology, which is often controlled by a few leading nations, and the i nherent dominance such technology provides. Consequently, states lagging in technological advancement are highly vulnerable. However, given current realities, excluding oneself from cyberspace is not an option; countries have become integral to this globalization. Therefore, nations have chosen to ensure cybersecurity by developing regulatory mechanisms alongside building robust cyber technology capabilities.

Although Ethiopia is categorized as a developing country, it is not immune to the vulnerabilities associated with cyber technology. Thus, it must establish a regulatory framework in addition to enhancing its cyber defense capabilities through internal research and development initiatives or strategic procurement of cybersecurity technology. In this process, it is essential to build a knowledge-based system by understanding the inherent complexities of the cyber world.

Considering both global and national cybersecurity realities, key policy issues have been identified. Accordingly, the National Cyber Security Policy (NCSP) comprises seven major policy focus areas: Legal and Regulatory Framework, Awareness, Capacity Building, Research and Development, Digital Identity and Personal Data Protection, Critical Information Infrastructure Protection, and International and National Cooperation.

2.2.Legal and Regulatory Framework

2.1.1. Policy Statement

It is crucial to develop and implement up-to-date legal and regulatory frameworks consistent with current realities. These frameworks are essential to reduce progressively increasing cybersecurity vulnerabilities and threats, defend against attacks, and hold perpetrators accountable. Therefore, it is

vital to develop and implement cybersecurity laws, policies, strategies, standards, and other regulatory mechanisms to prevent cybercrime, cyberterrorism, cyber espionage, and other illegal activities within the country. To this end, the following legal and regulatory goals, strategies, and tactics have been designed and will be implemented.tegies, and tactics are designed and implemented.

2.1.2. Goals

The goals of the legal and regulatory framework shall be to:

- Develop and regularly revise cybersecurity legal and regulatory frameworks that align with international laws and standards adopted by the country.
- Build the capacity of executive, judicial, and legislative bodies to prevent cybercrime, cyberterrorism, cyber espionage, and other illegal activities.
- Establish a regulatory system that ensures domestic and imported cybersecurity products and services, as well as the installation of key infrastructures, meet the country's cybersecurity standards.
- Establish standardized legal and regulatory frameworks for data collection, analysis, dissemination, usage, storage, and disposal to enhance public trust in the country's cybersecurity capabilities.

2.1.3. Strategies and Tactics

1. **Developing and revising binding and up-to-date substantive and procedural legal frameworks and regulatory systems that align with national cybersecurity conditions.**

Tactic One : Cybersecurity laws, standards, and systems applicable to government and key private institutions will be developed and implemented.

Tactic Two : All stakeholders will be engaged in the development process of cybersecurity legal and regulatory frameworks to enhance their acceptance and enforcement.

Tactic Three : Regulatory technologies will be applied to ensure legal accountability in cybersecurity activities.

2. **Producing and continuously building the capacity of competent executive, judicial, and legislative bodies in the area of cybersecurity laws and regulatory mechanisms.**

   Tactic : To enforce cybersecurity legal and regulatory frameworks, the capacity of investigators, prosecutors, judges, and other judicial bodies will be continuously built through education, training, discussion forums, conferences, and other mechanisms.

3. **Developing quality control and other regulatory standards that govern the supply of cybersecurity products and services, and the disposal of deteriorated products.**

   Tactic : Quality and reliability checks on domestic and imported cybersecurity products will be conducted, and the capacity of implementers will be continuously builty.

4. **Investigating and prosecuting illegal cyber activities and creating deterrence to ensure the confidentiality, integrity, and availability of information.**

   Tactic One : Practical monitoring and controlling mechanisms for cybercrime will be established.

Tactic Two : Criminals will be prosecuted in collaboration with the judiciary.

Tactic Three : Court cases related to cybersecurity issues will be made public.

2.3. Cyber Security Awareness

2.3.1. Policy Statement

Cybersecurity results from the interaction between technology, processes, and humans. Therefore, it is critical to prevent cybersecurity threats, vulnerabilities, and attacks that may arise, especially due to a lack of knowledge, distorted attitudes, and performance gaps among public and private institutions and citizens. The government will focus on the following goals, strategies, and tactics to foster a knowledge-based information-sharing culture regarding information value and cyberattacks, thereby achieving attitudinal and behavioral changes within the country.

2.3.2. Goals

The goals of cybersecurity awareness shall be to:

- Build knowledge and improve attitudes towards cybersecurity among public and private institutions, professional and civic associations, and citizens.
- Reduce cybersecurity vulnerabilities and threats, and prevent cyberattacks that may arise from carelessness, ignorance, and negligence.

- Raise public awareness and bolster a national cybersecurity culture to further reduce cybersecurity vulnerabilities and threats, and prevent cyberattacks.

2.3.3. Strategies and Tactics

- **Establishing institutional structures and systems that enable the enhancement of cybersecurity awareness.**

  Tactic One : Cybersecurity awareness schemes will be made available to society through expanding and strengthening the institutional structure of entities engaged in cybersecurity.

  Tactic Two : Awareness-raising activities will be performed using technologies that provide a quick response to cybersecurity incidents.

  Tactic Three: Cybersecurity Awareness Clubs will be established in educational institutions.

  Tactic four : Cybersecurity awareness programs will be expanded using social institutions.

- **Developing standardized national cybersecurity awareness frameworks and programs to be implemented in public and private institutions.**

  Tactic One : Periodic and continuous discussions, forums, and similar awareness creation events on the security of key information infrastructures will be organized.

  Tactic Two : National cybersecurity awareness campaigns will be carried out.

  Tactic Three : Public and private institutions will allocate sufficient and equitable resources for awareness creation programs for their workers and leaders.

6.943
6.496
0.689
0.369
4.604
3.798
0.857
0.570
7.050
5.805
8.585
0.548
0.458
-0.3

- **Equipping mass media with systems that enable them to raise and develop awareness on the value of information and the basics of cybersecurity awareness.**

    Tactic One : Various up-to-date cybersecurity awareness programs will be produced and broadcast by mass media to raise public awareness and understanding.

    Tactic Two : Mass media, private entities, civic organizations, and other bodies involved in cybersecurity awareness will be recognized and commended.

2.4. Capacity Building on Cyber Security

2.4.1. Policy Statement

The lack of trained personnel and robust cybersecurity systems and institutional structures has contributed to the country's lower level of cybersecurity capacity. As a consequence, citizens, government, and private institutions have become vulnerable to various forms of attacks and have been deprived of the benefits cyberspace could have provided. Therefore, recognizing that building strong cybersecurity capability plays a significant role in a country's economic, political, and social development and transformation, the government sets forth the following goals, strategies, and tactics. These aim to foster a strong cybersecurity culture, expand educational and training programs, build institutional and structural capacity, establish work processes, and ultimately create a resilient and dynamic national cyber capability.

2.4.2. Goals

Cybersecurity capacity building shall have the following goals:

- Establish structures and build capabilities that enable the detection of and response to cybersecurity threats, vulnerabilities, and attacks.
- Strengthen the cybersecurity capacity of public, private, and higher education institutions.
- Produce competent cybersecurity experts and leaders at the national level.

2.4.3. Strategies and Tactics

- **Establishing a standardized cybersecurity education and training program in the country by developing a cybersecurity curriculum for primary, secondary, and higher education institutions.**

  Tactic One : Cybersecurity education will be included in the country's education policy.

  Tactic Two : Up-to-date educational and training certification programs will be made available for professionals to enhance their cybersecurity capabilities.

  Tactic Three : A competency standard for cybersecurity professionals will be set.

- **Developing efficient and capable institutional structures and systems that enable the cybersecurity capacity building scheme.**

  Tactic One : Public and private institutions shall implement systems that facilitate cybersecurity knowledge transfer.

  Tactic Two : Structures for fostering cybersecurity knowledge and skills shall be established and implemented by public and private institutions.

Tactic Three : Institutions that train, recruit, and enhance talent in cybersecurity shall be established, and existing ones shall be strengthened.

- **Establishing an efficient cybersecurity knowledge management and transfer system at the national level.**

Tactic One : Platforms for sharing best practices, experiences, and knowledge on cybersecurity among government, private, and higher education institutions shall be set up.

Tactic Two : A permanent exhibition center and libraries that facilitate cybersecurity knowledge transfer shall be established.

- **Developing a strong and competent workforce through creativity and talent-based programs that help protect national interests.**

Tactic One : Competency building schemes shall be implemented for experienced and newly recruited professionals in key information infrastructure institutions, with special attention to their personality and talent.

Tactic Two : Forums to develop creativity and talent will be organized in coordination with international institutions engaged in cybersecurity.

Tactic Three : Cybersecurity competitions and exercises that help identify and promote innovations and talents will be organized.

2.5. Cybersecurity Research and Development

2.5.1. Policy Statement

Given the inherently complex, dynamic, and unpredictable nature of cyberspace, it is crucial to study challenges associated with emerging technologies and propose solutions. It is also vital to focus on Research and Development (R&D) that fosters knowledge, skills, and innovations in this area. Furthermore, it is imperative to develop cyber infrastructures and technologies, expand technology transfer and innovations, and conduct R&D that has a national and international impact at various levels. Consequently, the government strives to cultivate indigenous research capacity in the area, build a cybersecurity industry through organized research and development, and protect intellectual property rights. To this end, the government identifies the following goals and strategies and works to achieve them.

2.5.2. Goals

Cybersecurity research and development shall have the following goals:

- Ensure cybersecurity products and services that protect critical information infrastructures are based on R&D.
- Identify cybersecurity threats, vulnerabilities, and attacks through research and provide solutions.
- Build R&D capacity based on indigenous knowledge and innovation to ensure cybersecurity.

- Foster an internationally competent and integrated national cybersecurity R&D culture.

2.5.3. Strategies and Tactics

- **Supporting indigenous cybersecurity products and services with research and development.**

  Tactic One : Activities enabling the leadership of the cybersecurity industry through research and development shall be initiated.

  Tactic Two : Research-based indigenous cybersecurity solutions that protect key infrastructure from attacks shall be made accessible to users.

  Tactic Three : Various incentives to motivate the innovation of new products and services that promote cybersecurity research shall be provided.

  Tactic four : R&D programs that produce value-added products and services by adopting new technologies shall be designed.

- **Expanding programs that enable the building of R&D capacity on cybersecurity by fostering cooperation and partnership between higher education institutions and the industry.**

  Tactic One : Knowledge, skills, experience, and technological capacity necessary to accomplish R&D tasks shall be built.

  Tactic Two : Cybersecurity Centers of Excellence in various research institutions, security agencies, and higher education institutions shall be established, if deemed necessary.

  Tactic Three : Knowledge and experience-sharing forums, conferences, and other events that build R&D capacity among cybersecurity

stakeholders shall be held.

Tactic four : R&D activities shall be carried out by government and private institutions in coordination with higher educational institutions.

Tactic five : A standard that determines the capability and quality of bodies involved in cybersecurity R&D capacity building shall be set.

- **Supporting R&D that continuously enables the reduction of threats and vulnerabilities, the defense against and response to attacks, and the building of resilience.**

  Tactic One : Continuous R&D support shall be provided to protect against vulnerabilities and attacks facing key information infrastructures.

  Tactic Two : A conducive environment that enables the private sector to participate in the country's cybersecurity R&D programs will be created.

- **Promoting R&D in cybersecurity issues that constitute a national priority, considering actual and potential cyber threats.**

  Tactic One : R&D activities shall be conducted with special attention to threats arising from technological development that may cause damage to the country's security.

  Tactic Two : A resilient national cyberspace and cybersecurity industry development shall be supported with R&D.

2.6. Digital Identity and Personal Data Protection

2.6.1. Policy Statement

Inadequate protection of digital identities and personal data can lead to cyberattacks on citizens, identity-based attacks, and deviations from societal culture and values, resulting in compromised privacy and human rights. Therefore, the government sets the following goals and strategies to prevent psychological attacks on citizens, raise public awareness, reduce the risk and vulnerability of digital identity and personal data, and ensure the security of information infrastructures used by citizens.

2.6.2. Goals

The protection of digital identity and personal data shall have the following goals:

- Ensure credible digital services and personal data protection for citizens.
- Protect national values and norms from cybersecurity threats, vulnerabilities, and attacks by enhancing the constructive role that cyberspace can play in educating children.
- Protect against and minimize gender-based cyberattacks, sexual harassment, and psychological influence that may occur in cyberspace.
- Protect against religious, ethnic, and other identity-based digital attacks.

2.6.3. Strategies and Tactics

- **Developing binding legal frameworks for the protection of digital identity and personal data, and establishing technology-based systems.**

  Tactic One : Frameworks to ensure the security of personal data shall be developed and implemented in a coordinated manner.

  Tactic Two : A technology-based cybersecurity regulatory system that does not compromise data privacy will be implemented.

  Tactic Three : Directives for personal data collection, processing, and regulation shall be developed.

  Tactic four : There shall be a balanced approach towards personal data protection in the due process of ensuring cybersecurity.

- **Establishing a system to ensure the security of government electronic services.**

  Tactic One : A personal data protection agreement that addresses the rights and obligations involved during personal data collection, storage, and usage by concerned institutions shall be reached.

  Tactic Two : Institutions shall be overseen to include provisions for the protection of individual privacy rights in their cybersecurity directives and other guidelines.

  Tactic Three : Continuous monitoring and analysis regarding personal data protection of individuals shall be carried out in every institution.

- **Establishing a system to prevent religious and ethnic-based derogatory comments and similar identity-based attacks using cyberspace.**

SCANNING...

Tactic One : Regulations and operational procedures that prohibit hate speech and related issues, and that promote the proper use of cybersecurity, shall be implemented.

Tactic Two : Regulatory technologies to detect and protect against cyber-based hate speech and fake news shall be applied.

- **Developing frameworks and establishing operational procedures that protect the good character and security of teenagers in cyberspace.**

Tactic One : Monitoring mechanisms to prevent the violation of digital rights of children shall be in place.

Tactic Two : Institutions shall perform their tasks while respecting the digital rights of children.

Tactic Three : Controlling mechanisms to protect children from anti-cultural content focused on children in cyberspace shall be in place.

- **Supporting institutions to develop programs that protect the digital identity of women and children.**

Tactic One : Public campaigns shall be organized to strengthen the protection of digital identity and personal data of women and children

Tactic Two : Discussion forums on digital privacy rights protection for women and children shall be facilitated.

Tactic Three : Actions shall be taken to reduce cyber-based psychological attacks on women.

2.7. Critical Information Infrastructures Protection

2.7.1. Policy Statement

As information becomes an increasingly valuable resource, it is crucial to protect critical information infrastructures from cyberattacks, reduce cyber threats and vulnerabilities, and enhance resilience. Recognizing the importance of protecting critical information infrastructure for ensuring cybersecurity and fostering trust, the government gives due attention to this sector. Therefore, to prevent cyber incidents and attacks that may target critical information infrastructures, and to properly govern and manage the country's economic, social, and political issues in coordination and partnership with the private sector, the government will operate by setting the following goals and strategies.work by setting the following goals and strategies

2.7.2. Goals

Strategies and Tactics

- Develop the capacity to identify, prevent, and respond to cyber threats, vulnerabilities, attacks, and damages to critical information infrastructures and institutions.
- Ensure the security of imported and local critical information infrastructure products and services.
- Create coordination and partnership between the public and private sectors to provide special protection for critical information infrastructures.

2.7.3. Strategies and Tactics

- **Building institutional structures and capacity, and establishing operational procedures that enable the identification, defense against, and response to potential threats, vulnerabilities, attacks, and damages to critical information infrastructures.**

  Tactic One : A coordinated national cybersecurity system will be implemented to ensure the cybersecurity of critical information infrastructure within public and private institutions.

  Tactic Two : An entity capable of detecting and providing rapid responses to attacks on critical information infrastructures shall be included in the organizational structure of each critical infrastructure.

  Tactic Three : A national critical information infrastructure security governance system will be established and continuously updated in compliance with new developments.

- **Building capacity to develop standardized control systems for preventing attacks on critical information infrastructures**

  Tactic One : Public and private institutions shall implement international standards and nationally contextualized cybersecurity laws, policies, standards, and frameworks.

  Tactic Two : Critical information infrastructure sectors will be required to design and incorporate programs that address international issues, complying with the country's information security standards and operational procedures.

CARGO TERMINAL
Ethiopian
የኢትዮጵያ

Tactic Three : Education and training on current issues will be conducted, and discussion forums will be organized for stakeholders to detect, prevent, and respond to threats, vulnerabilities, attacks, and damages to critical information infrastructures.

Tactic four : Capacity will be built to produce and supply indigenous products and services used to secure critical information infrastructures.

- **Developing secure information infrastructure products, services, communication systems, reliable networks, and control systems technology.**

Tactic One : A standard for ensuring the security of critical information infrastructures, ICT products, and services shall be employed.

Tactic Two: Information and information

Tactic Two : Information and information infrastructure vulnerability assessments, penetration testing, and security audits shall be conducted, and immediate remedial action will be taken at any time

- **Enhancing the role of public and private institutions, and other concerned stakeholders to provide special protection for critical information infrastructures.**

Tactic One : By persistently identifying critical information infrastructures, criteria for setting their roles and responsibilities will be prepared and implemented.

Tactic Two : A 24/7 physical and virtual protection is provided for critical information infrastructure and systems;

Tactic Three : The duties and responsibilities of all stakeholders will be identified to provide special protection for critical information infrastructures.

2.8. National and International Cooperation

2.8.1. National Coordination and Partnership

2.8.1.1. Policy Statement

Given that cyberspace and attacks within it are complex, unpredictable, dynamic, and borderless, its security cannot be managed by a single government or a limited number of institutions alone. Hence, establishing national coordination and partnership and tackling cybersecurity threats should be a shared responsibility of all stakeholders. In particular, the development of cybersecurity products and services requires the active participation of the private sector.

The private sector has been making progress in involving itself in the information technology industry development sector. However, while the private sector can play a key role in accelerating the country's cybersecurity efforts, its current participation in this area is limited. To change this scenario, the government encourages the involvement of the private sector in the development of the cybersecurity industry. Therefore, to ensure cybersecurity at the national level, the government mobilizes and utilizes available national capacity and enhances the role of the private sector. To this end, it sets the following objectives and strategies and implements them.

2.8.1.2. Goals

The goal of national coordination and partnership shall be to:

- Establish and strengthen coordination and partnerships among government, the private sector, and relevant stakeholders to ensure national cybersecurity.
- Enable local private sectors engaged in cybersecurity product and service delivery to be competitive in both local and international markets.

2.8.1.3. Strategies and Tactics

- **Establishing a system of coordination and partnership between public and private sectors that play a key role in national cybersecurity.**

  Tactic One : A system that governs cybersecurity coordination and partnership shall be established and implemented.

  Tactic Two : National cybersecurity discussion platforms that strengthen coordination and collaboration will be formed and regularly held at the national level.

2. **Enabling citizens, the private sector, civic societies, and other stakeholders to play their part in defending against cyber attacks;**

   Tactic One : Enabling citizens, the private sector, civil societies, and other stakeholders to play their part in defending against cyberattacks.

   Tactic Two : There shall be an experience-sharing and knowledge transfer scheme among cybersecurity stakeholders.

- **The Ethio-CERT will be used as a bridge among all public and private institutions for cybersecurity.**

  Tactic One : Both public and private institutions shall be enabled to have a Computer Emergency Response Unit for experience-sharing on cyber incidents.

  Tactic Two : The systems of the Computer Emergency Response Units of both public and private institutions shall be coordinated and aligned with the national CERT.

- **Establishing a system of coordination and partnership that will increase and strengthen the participation and contribution of the local private sector in the development of cyber security industry;**

  Tactic One : Programs shall be developed and implemented to help create new institutions and strengthen existing ones.

  Tactic Two : An incentive system shall be established for entities that produce cybersecurity products for the benefit of the public.

  Tactic Three : A supporting mechanism that enables standardized cybersecurity products and services to compete in the domestic market shall be in place.

  Tactic four : Due focus shall be given to the private sector to make it competitive in international markets.

2.8.2. International Cooperation

2.8.2.1. Policy Statement

To mitigate threats and vulnerabilities and to defend against attacks that may arise from the dynamic and borderless nature of cyberspace, countries formulate and implement diverse policies, strategies, standards, practices, and perspectives. While this is a step forward, without cooperation among countries, it will be challenging to maintain cybersecurity at the required level. As a result, countries opt for international cooperation to defend against cybersecurity threats, vulnerabilities, and attacks, to enhance cybersecurity levels, and to create a secure cyberspace. Recognizing this fact, the government has set international cooperation as a policy focus area to enable knowledge and technology transfer and to facilitate the prevention of organized cybercrime, such as cyberterrorism, cyber espionage, and other transnational cybercrimes.

2.8.2.2. Goals

The goal of international cooperation shall be to:

- Foster cooperation to prevent cybercrime, cyberterrorism, cyber espionage, and related cross-border security threats.
- Integrate international cooperation on cybersecurity into the country's cyber diplomacy.
- Encourage and promote bilateral and multilateral cybersecurity agreements.

2.8.2.3. Strategies and Tactics

- **Establishing a system of cooperation to address legal issues related to cybercrime, cyber terrorism, cyber espionage, and related cross border cyber security threats;**

  Tactic : International cooperation and partnership agreements on cybersecurity will be made.

- **Establishing international cooperation based on tech-**

nical and legal frameworks to prevent cross-border cybercrime, cyberterrorism, cyber espionage, and related attacks

Tactic One : : Experience-sharing mechanisms with various countries and international organizations for defending against cyberattacks will be facilitated.

Tactic Two : There will be information-sharing and technical cooperation and assistance arrangements with other countries.

Tactic Three : Cybersecurity will be an integral part of foreign policy.

- **Establishing a system to accelerate international experience sharing and knowledge transfer.**

Tactic One : Studies that enable active participation in international, continental, and regional agreements and negotiations will be conducted.

Tactic Two : A conducive environment will be created for private and public institutions to strengthen their cybersecurity ties with other governments and private institutions.

Tactic Three : International training will be facilitated to develop competent human resources on cybersecurity issues.

- **Creating compliance between the country's cybersecurity laws and policies with international legal frameworks and standards.**

Tactic One : There will be active participation in international cybersecurity cooperation forums in line with the country's needs.

Tactic Two : Awareness will be created regarding relevant international laws signed and ratified by the country, and on the trends of the sector.

Part Three

Policy Implementation Framework

3.1. Success Indicators

The success of the National Cyber Security Policy will be measured by the following indicators:

- Achieving stable socio-cultural, economic, and political conditions through the reduction of cybersecurity risks, threats, vulnerabilities, and attacks.

- Developing robust cybersecurity capabilities and systems at national, sectoral, and institutional levels.

- Delivering cybersecurity products and services through enhanced national capabilities.

- Fostering a security-aware society that utilizes cyberspace responsibly and cultivating a strong national cybersecurity culture.

- Establishing a thriving cybersecurity industry with active private sector participation.

- Forming mature and impactful cybersecurity partnerships and collaborations at international, regional, and national levels that contribute to the maintenance of national interests.

- Developing an integrated national database that reflects national capabilities.

3.2. Policy Revision

To ensure cyber security in our country, it is necessary to create strong institutions and to strengthen the existing ones. Cognizant of this fact, the government has established INSA and Ethio-CER2T to protect and respond to cyber attacks targeting the country and its key infrastructures.

To ensure cyber security, it is important to cooperate and work in partnership with various national institutions. To make this collaboration and partnership effective, National Cyber Security Council, which comprises the concerned government and private bodies, and other stakeholders, will be established. The government may establish new institutions and task forces at the national and sectoral levels to facilitate the implementation of the policy, or assign additional responsibilities to the existing institutions. The institutional structure will be formulated in away that it enables the due implementation of this NCSP taking into account the private sector involvement.

3.3. Roles and Responsibilities of Stake holders

INSA will oversee the administration of the policy. However, it is incumbent on all government institutions, private sectors with key information infrastructures, and other concerned stakeholders to implement this NCSP. They also have the responsibility for designing and implementing the respective cyber security programs in consistence with this NCSP and international standards.

3.4. Monitoring and Evaluation

To measure the effectiveness of the NCSP at all levels and to realize the execution process, a monitoring and evaluation system which includes the following key issues shall be in place:

1. An action plan for the implementation of the policy shall be prepared by INSA; the Cyber Security Council will play its role for the implementation.
2. A monitoring and evaluation system shall be established to ensure that public and private institution and other stakeholders carry out the relevant activities specified in the NCSP, perform activities listed in the NCSP implementation frameworks, establish the necessary institutional structure, and allocate the required budget and resources;
3. To assess the implementation of NCSP, data collection, organization, and analysis activities will be carried out, and a reporting system will be established through coordination by INSA;
4. An annual stakeholders meeting will be organized by INSA to evaluate the implementation of the NCSP;
5. Based on the results of the monitoring and evaluation of NCSP implementation, directions will be given to develop other necessary frameworks and, if need be, to revise the existing NCSP.

3.5. Legal Issues

Legislation that help implement the policy may be formulated and enacted.

3.6 Financial Issues

1. The budget required to implement the NCSP and to carry out other related activities shall mainly be allocated by the government;
2. The budget allocated for the implementation of the NCSP shall be run following the monitoring and evaluation system set in the policy and by the decision of the body endowed with a legal responsibility to oversee the NCSP.
3. Projects and programs designed to implement the policy goals, strategies, and tactics will be carried out in collaboration with the relevant bodies as needed;
4. As cyber security is a shared responsibility, all stakeholders that have a stake in the implementation of the NSCP allocate their own budgets and carry out the respective duites and responsibilities.
5. INSA will generate income from the products it delivers and the services it provides based on the provisions in the appropriated laws so as to enable it to implement the policy.

3.7 Success Indicators

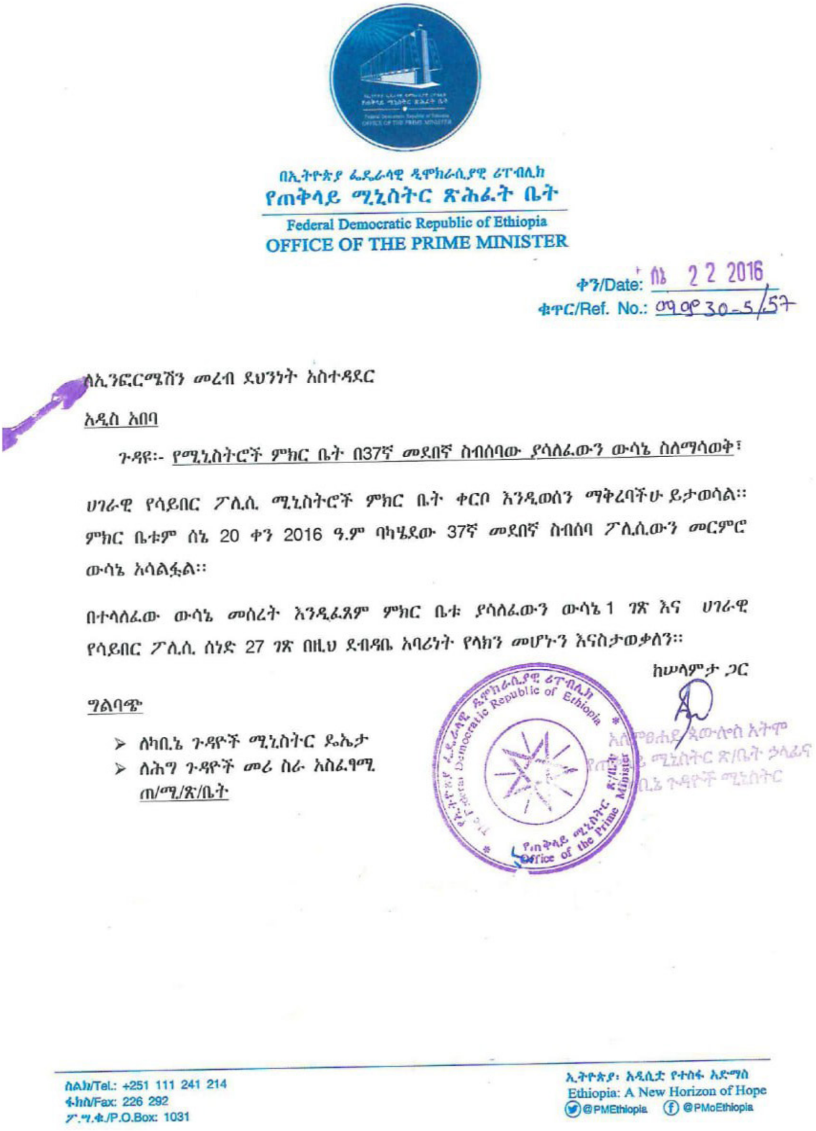
The success of the National Cyber Security Policy will be measured by the following indicators:

- Achieving stable socio-cultural, economic, and political conditions through the reduction of cybersecurity risks, threats, vulnerabilities, and attacks.

- Developing robust cybersecurity capabilities and systems at national, sectoral, and institutional levels.
- Delivering cybersecurity products and services through enhanced national capabilities.
- Fostering a security-aware society that utilizes cyberspace responsibly and cultivating a strong national cybersecurity culture.
- Establishing a thriving cybersecurity industry with active private sector participation.
- Forming mature and impactful cybersecurity partnerships and collaborations at international, regional, and national levels that contribute to the maintenance of national interests.
- Developing an integrated national database that reflects national capabilities

3.8 Policy Revision

The National Cybersecurity Policy (NCP) may be revised due to the impact of political, economic, social, and technological changes within the country on cybersecurity efforts. Revisions may also occur when new requirements emerge from the evolving roles and responsibilities of public and private sector institutions in the cybersecurity domain, or based on directives issued from the findings of NCP monitoring and evaluation. Accordingly, the NCP will undergo revision every five years from its ratification date.



በኢትዮጵያ ፌዴራላዊ ዲሞክራሲያዊ ሪፐብሊክ
የጠቅላይ ሚኒስትር ጽሕፈት ቤት
Federal Democratic Republic of Ethiopia
OFFICE OF THE PRIME MINISTER

ቀን/Date: ሰኔ 22 2016
ቁጥር/Ref. No.: ጠሚ30-5/57

ለኢንፎርሜሽን መረብ ደህንነት አስተዳደር

አዲስ አበባ

ጉዳዩ፡- የሚኒስትሮች ምክር ቤት በ37ኛ መደበኛ ስብሰባው ያሳለፈውን ውሳኔ ስለማሳወቅ፣

ሀገራዊ የሳይበር ፖሊሲ ሚኒስትሮች ምክር ቤት ቀርቦ እንዲወሰን ማቅረባችሁ ይታወሳል። ምክር ቤቱም ሰኔ 20 ቀን 2016 ዓ.ም ባካሄደው 37ኛ መደበኛ ስብሰባ ፖሊሲውን መርምሮ ውሳኔ አሳልፏል።

በተላለፈው ውሳኔ መሰረት እንዲፈጸም ምክር ቤቱ ያሳለፈውን ውሳኔ 1 ገጽ እና ሀገራዊ የሳይበር ፖሊሲ ሰነድ 27 ገጽ በዚህ ደብዳቤ አባሪነት የላክን መሆኑን እናስታውቃለን።

ከሠላምታ ጋር

የኢትዮጵያ ፌዴራላዊ ዲሞክራሲያዊ ሪፐብሊክ
Federal Democratic Republic of Ethiopia
የጠቅላይ ሚኒስትር ጽ/ቤት
Office of the Prime Minister

አለምፀሐይ ጳውሎስ አትሞ
የጠቅላይ ሚኒስትር ጽ/ቤት ኃላፊና
ካቢኔ ጉዳዮች ሚኒስትር

ግልባጭ

- ለካቢኔ ጉዳዮች ሚኒስትር ዴኤታ
- ለሕግ ጉዳዮች መሪ ስራ አስፈፃሚ
  ጠ/ሚ/ጽ/ቤት

ስልክ/Tel.: +251 111 241 214
ፋክስ/Fax: 226 292
ፖ.ሣ.ቁ./P.O.Box: 1031

ኢትዮጵያ፡ አዲሲቷ የተስፋ አድማስ
Ethiopia: A New Horizon of Hope
@PMEthiopia @PMoEthiopia