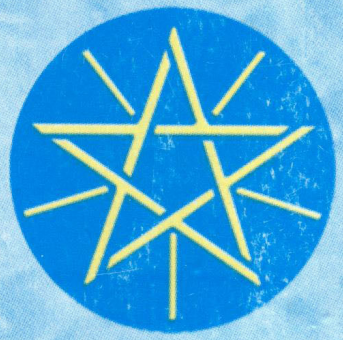

የኢትዮጵያ ፌዴራላዊ ዲሞክራሲያዊ ሪፐብሊክ ሃገራዊ

የኢንፎርሜሽን ደህንነት ፖሊሲ

NATIONAL INFORMATION SECURITY POLICY OF THE FEDERAL DEMOCRATIC REPUBLIC OF ETHIOPIA

መስከረም 2004 ዓ.ም

September 2011

ማውጫ

Table of Contents

የቃላት ፍቺ

በዚህ ፖሊሲ ውስጥ የቃሉ አገባብ ሌላ ትርጉም ካልተሰጠው በስተቀር፣

"ኢንፎርሜሽን" ማለት ከማንኛውም ጥሬ ዳታ የሚመነጭ በድምፅ፣ በፅሁፍ ፣ በምስል፣ በካርታ ወይም በማንኛውም መልኩ ተቀናብሮ የሚገኝ ሃብት ነው።

"ዳታ" ማለት ያልተተነተነና አይነተኛ ትርጉም ያልተሰጠው ለጠቀሜታ የሚውል የኢንፎርሜሽን ግብአት ነው።

"የኢንፎርሜሽን ደህንነት" ማለት ኢንፎርሜሽን በሚሰበሰብበት፣ በሚተነተንበት ፣ በሚከማችበትና በሚሰራጭበት ወቅት ታአማኒ ነቱን ፣ ሚስጢራዊነቱንና ተደራሽነቱን ከሚያሳጡ ጥቃቶችን መጠበቅ ነው።

"የኢንፎርሜሽን ጦርነት" ማለት የሳይበርና የኤሌክትሮማግኔቲክ ቴክኖሎጂዎችንና ስርዓቶችን በመጠቀም በብሄራዊ ጥቅሞች፣ በህገ

Definitions

In this policy, unless the context otherwise requires:

1. "Information" means a resource generated from any raw data obtained in the form of audio, texts, visual, map or orchestrated in any form;
2. "Data" means a source of information unprocessed and undefined that could be put in use;
3. "Information security" means securing information from attacks that obliterate its integrity, confidentiality and availability while collecting, processing, preserving and communicating;
4. "Information infrastructure" includes telecommunication, information communication technology, geospatial information

የቃላት ፍቺ

በዚህ ፖሊሲ ውስጥ የቃሉ አገባብ ሌላ ትርጉም ካልተሰጠው በስተቀር፣

"ኢንፎርሜሽን" ማለት ከማንኛውም ጥሬ ዳታ የሚመነጭ በድምፅ፣ በፅሁፍ ፣ በምስል፣ በካርታ ወይም በማንኛውም መልኩ ተቀናብሮ የሚገኝ ሃብት ነው።

"ዳታ" ማለት ያልተተነተነና አይነተኛ ትርጉም ያልተሰጠው ለጠቀሜታ የሚውል የኢንፎርሜሽን ግብአት ነው።

"የኢንፎርሜሽን ደህንነት" ማለት ኢንፎርሜሽን በሚሰበሰብበት፣ በሚተነተንበት ፣ በሚከማችበትና በሚሰራጭበት ወቅት ታአማኒ ነቱን ፣ ሚስጢራዊነቱንና ተደራሽነቱን ከሚያሳጡ ጥቃቶችን መጠበቅ ነው።

"የኢንፎርሜሽን ጦርነት" ማለት የሳይበርና የኤሌክትሮማግኔቲክ ቴክኖሎጂዎችንና ስርዓቶችን በመጠቀም በብሄራዊ ጥቅሞች፣ በህገ

Definitions

In this policy, unless the context otherwise requires:

1. "Information" means a resource generated from any raw data obtained in the form of audio, texts, visual, map or orchestrated in any form;
2. "Data" means a source of information unprocessed and undefined that could be put in use;
3. "Information security" means securing information from attacks that obliterate its integrity, confidentiality and availability while collecting, processing, preserving and communicating;
4. "Information infrastructure" includes telecommunication, information communication technology, geospatial information

መንግስታዊ ስርዓቱና በዜጎች ስነ ልቦና ላይ የሚሰነዘር ጦርነት ነው።

"ክሪፕቶግራፊ" ማለት ከታሰበው ተቀባይ ውጭ መልእክትን ማንም ሰው እንዳያነበው ወይም እንዳይቀይረው ለማድረግ የሚያስችል የሚስጥር ሳይንስ ነው።

"ቁልፍ የደህንነት መሰረተ ልማት" ማለት የሚሰራጨው ኢንፎርሜሽን ደህንነትና የላኪና የተቀባይ ማንነት ትክክለኛነት የተጠበቀ እንዲሆን የሚያስችል የደህንነት መሰረተ ልማት ነው።

"የኢንፎርሜሽን መሰረተ ልማት" ማለት ኢንፎርሜሽን የሚሰበሰ ብበት፣ የሚከማችበት፣ የሚተነተንበትና የሚሰራጨበት ስነ-ምህዳር ነው።

"የሳይበር ክልል" ማለት እርስ በርሳቸው በተሳሰሩ የኢኮቴ ሲስተሞችና መሰረተ ልማቶች አማካኝነት ኤሌክትሮኒክስና ኤሌክ ትሮማግኔቲክ ስፔክትረምን በመጠቀም መረጃ የሚፈጠርበት፣ የሚሰበሰብበት፣ የሚከማችበት፣ የሚተነተንበት፣ የሚሰራጭበት፣ የሚለዋወጥበትና ጥበቃ የሚደረግበት አለም አቀፍና ድንበር የለሽ ክልል ነው።

"አካባቢያዊ የግንኙነት መረቦች" ማለት በአገር ወይም በተቋማት ውስጥ ብቻ ተግባራዊ የሚደረጉ እንደ ኢንትራኔት፣ የቁልፍ መሰረተ ልማቶች መቆጣጠሪያ ስርዓት፣ የኤሌክትሮኒክስ አስተዳ ደር፣ ኤሌክትሮኒክስ ንግድን እና የመሳሰሉትን የሚያጠቃልል ነው።

"ቁልፍ መሰረተ ልማት ወይም ተቋም " ማለት ለኢንፎርሜሽን መረብ ደህንነት አደጋ የተጋለጠና በሚፈጠረው አደጋም በሃገራቱ

and electromagnetic communication systems and public key infrastructure;

5. "Cyberspace" means a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded procedures and controllers;
6. "Information warfare" means warfare against the national interest, constitutional order and nation's psychology by using cyber and electromagnetic technologies and systems;
7. "Cryptography" means a science of coding message so that they cannot be read or altered by anyone other than the intended recipient;

...

ማህበራዊ፣ ኢኮኖሚያዊ ወይም ፖለቲካዊ ጥቅሞች ላይ ከፍተኛ ጉዳት ሊያደርስ የሚችል መሰረተ ልማት ወይም ተቋም ነው።

"የኮምፒውተር አደጋዎች መከላከል ግብረ ሃይል" ማለት ከኢንፎርሜሽን ደህንነት ጋር በተያያዘ የሚከሰቱ ለውጦችን፣ አደጋዎችንና የአደጋ ምልክቶችን እንዲሁም መከላከያ መንገዶችን በተመለከተ የመረጃ ልውውጥ ነቁጥ ሆኖ የሚያገለግል ብሄራዊ ግብረ ሃይል ነው።

አሕፅሮተ ቃላት

- ኢኮቴ የኢንፎርሜሽን ኮሙኒኬሽን ቴክኖሎጂ
- ኢመደኤ የኢንፎርሜሽን መረብ ደህንነት ኤጀንሲ

8. "Critical infrastructure" means a critical infrastructure that will have considerable damage on the national interest and public safety if its information and information infrastructure security become vulnerable to a threat;
9. "Computer emergence response team" means a team of dedicated information security specialists that prepares for and responds to information security incidents.

Acronyms

1. ICT	Information Communication Technology.
2. CERT	Computer Emergence Response Team.
3. NCERT	National Computer Emergence Response Team.
4. R&D	Research and Development.
5. INSA	Information Network Security Agency.
6. FDRE	Federal Democratic Republic Of Ethiopia

መግቢያ

በአሁኑ ወቅት የኢንፎርሜሽንና የኢንፎርሜሽን መሰረተ ልማት ዋጋ ከምንም ጊዜ በላይ ከፍ ብሏል። ለዚህም የግሎባላይዜሽን እውን መሆን፣ የኢኮቴ ፈጣን እድገት፣ የሳይበር ክልል መፈጠርና የአካባቢያዊ የግንኙነት መረቦች መስፋፋት የማይተካ ሚና የተጫወቱ ሲሆን ኢንፎርሜሽን ከማስፈፀሚያነት አልፎ ቁልፍ ሃብትና እሴት እየሆነ በመምጣቱ፣ ያለ ኢንፎርሜሽን ሰላምን፣ ልማትን፣ ዲሞክራሲንና መልካም አስተዳደርን ማስፈን የማይታሰብ ሆኗል። በሌላ በኩል ደግሞ ኢንፎርሜሽንና የኢንፎርሜሽን መሰረተ ልማት ቁልፍ የኢንፎርሜሽን ጥቃቶች ማስፈጸሚያም ኢላማም በመሆናቸው በአገራችንም የኢንፎርሜሽን ደህንነት ስጋት አሳሳቢ ደረጃ ላይ ከደረሰ ውሎ አድሯል። በተለይም ሃገሪቱ የአለም አቀፍ ሽብርተኞች ኢላማ ከመሆኗና ሽብርተኞቹም እኩይ ዓላማቸውን ለማስፈፀም ኢንፎርሜሽንና የኢንፎርሜሽን መሰረተ ልማትን በማስፈፀሚያነትና በኢላማነት ተመራጭ ስትራቴጂ እያደረጉት በመምጣታቸው ሃገሪቱ ለደህንነት ስጋቶች ምን ያህል ቅርብ እንደሆነች እና እነዚህን ችግሮች ለመፍታት በሚደረጉ ጥረቶችም የኢንፎርሜሽን ደህንነት ፖሊሲን ወሳኝነት መንግስት ይገነዘባል። በአጠቃላይ የዚህ ፖሊሲ መውጣት መሰረታዊ መነሻዎች በርካታ ቢሆኑም ዋና ዋናዎቹ፡-

ሀ/ ኢንፎርሜሽን ውድ ሃብት በመሆኑ ሃገሪቱ ለቀየሰቻቸው የሰላም፣ የልማት፣ የዲሞክራሲና የመልካም አስተዳደር መርሃ ግብሮች መሳካት ቁልፍ ግብአትና ማስፈፀሚያ እንዲሆን ደህንነቱን ማረጋገጥ አስፈላጊ መሆኑ፣

ለ/ ኢንፎርሜሽን የሚከማችበት፣ የሚተነተንበትና የሚሰራጭበት ቁልፍ መሰረተ ልማት ደህንነቱን ማረጋገጥ አስፈላጊ መሆኑ፣

ሐ/ ኢንፎርሜሽን አለም አቀፋዊ የኢንፎርሜሽን ጦርነት ዋንኛ ኢላማና መሳሪያ ሲሆን ከዚህ ጦርነት ራስን ለመከላከል የኢንፎርሜሽን ደህንነት ማረጋገጥ የግድ መሆኑና

INTRODUCTION

The information revolution has dramatically increased the value and importance of information and information infrastructures in the contemporary world. This is due to, among other things, the reality of globalization, rapidly changing ICT and growing dependence on technology, the veracity of cyberspace and the expansion of local networking and interaction. As the value of information is increasing dramatically, it becomes difficult to ensure peace, democratization and development without it.

However, with ever-increasing use of, and reliance on, information and information infrastructure comes increased exposure, and vulnerability, to more advanced and sophisticated information security threats- state sponsored information security attacks, information warfare, cyber terrorism, organized crimes, individual hackers/crackers, and so on.

Ethiopia is not immune from the above mentioned information security threats and attacks. The country is vulnerable not just in general terms, but also in its full detail. The government is therefore, convinced that devising a coherent and comprehensive national information security policy is one step to reduce these threats and vulnerabilities. Although the push factors for the development of this policy cannot be listed exhaustively, they can be summarized in the following points.

A. Information is a valuable asset. This valuable asset can be used for the implementation of national peace, democratization and development programs only if it is protected from any threat;
B. It is essential to ensure the security of information infrastructures in which information is stored, processed and transmitted;
C. Information is a weapon and target of information warfare. To protect oneself from such warfare, safeguarding information and information infrastructure is a prerequisite;

መ/ ሃገራችን ወደ ኢንፎርሜሽን ዘመን በመቀላቀል ላይ በመሆኗ ምክንያት በርካታ መልካም አጋጣሚዎችና ውስብስብ ስጋቶች የተፈጠሩ ሲሆን መልካም አጋጣሚውን በላቀ ለመጠቀምና ስጋቱን ለመቀነስ መፈጠር የሚገባውን አገራዊ ቅንጅት አቅጣጫ ማስያዝ አስፈላጊ መሆኑ ናቸው።

ምዕራፍ አንድ
አጠቃላይ

1.1 የፖሊሲው አስፈላጊነትና መሰረታዊ እሳቤዎች

ሀ/ የኢንፎርሜሽን ደህንነት ከኢኮቴ ደህንነት በላይ በመሆኑ ፖሊሲው ማንኛውም የኢንፎርሜሽን ሃብትና ይህ ሃብት የሚከማችበት፣ የሚተነተንበትና የሚሰራጭበት መሰረተ ልማትን ደህንነት መጠበቅ የሚያስችል ስርዓት ነው።

ለ/ የኢንፎርሜሽን ደህንነት የማረጋገጥ ጉዳይ የብሄራዊ ደህንነትን፣ ተቋማዊ ደህንነትን፣ የዜጎች መሰረታዊ መብቶችና ነፃነቶችን እንዲሁም የህዝብ ሰላም፣ ልማትና ዲሞክራሲያዊ ስርዓት ግንባታ ለማረጋገጥ የሚደረገው ጥረት አካል ነው።

ሐ/ ፖሊሲው የኢንፎርሜሽንን ሚስጢራዊነት፣ ተአማኒነት፣ ተደራሽነትና እውነተኛነትን ከማረጋገጥ እንዲሁም የኢንፎርሜሽን ላኪና ተቀባይ ማረጋገጫ ስርአት ከመዘርጋት ባሻገር ስጋቶችን የመለየት፣ የመከላከል፣ አፀፋዊ ምላሽ የመስጠትና መልሶ የማቋቋም እርምጃዎችን መውሰድና ስጋቶችን ለመግታት የሚያስችሉ ህጋዊ ስርዓቶችንና ቴክኒካዊ አቅሞችን ያጠቃልላል።

መ/ ፖሊሲው በዋናነት በመንግስት ተቋማት ላይ የሚያተኩር ሲሆን ይህም የሃገራችን ቁልፍ ተቋማትና መሰረተ ልማቶች በዋናነት በመንግስት የሚንቀሳቀሱ በመሆ ናቸው ነው።

D. Ethiopia is becoming part of the international information society. This comes with both opportunities and security perils. Therefore, there is a sense of urgency to utilize the opportunities and reduce the threats and vulnerabilities.

PART ONE
GENERAL

1.1. The Need for and Basic Assumptions of the Policy

A. Information security is beyond ICT security. It addresses all the issues involving the protection of information or data in whatever format or medium it exists, the related technologies and infrastructures used for information processing, storage and communications.

B. Information security is an integral part of national security, organizational security, public peace and security and the protection of basic rights and freedoms of citizens.

C. In addition to ensuring the confidentiality, integrity, availability, authenticity and non-repudability of information, the policy encompasses the detection, prevention, response, deterrence and recovery measures and legal and technical capabilities.

D. The policy focuses mainly on governmental institutions and infrastructures for most of the country's critical infrastructures are currently operated by the government.

ሠ/ ሃገራችን ወደ አለም አቀፍ የኢንፎርሜሽን ስርዓቱ በፍጥነት በመቀላቀል ላይ የምትገኝ በመሆኗና የኢንፎርሜሽን ደህንነት ስጋት ምንጭ ድንበር የለሽ በመሆኑ ፣ ስጋቱን ለመከላከል አለም የደረሰበትን ቴክኖሎጂ ማወቅና መጠቀም መቻልን፣ አለም አቀፍ ተቀባይነት ያላቸው ስታንዳርዶችና መለኪያዎችን ተግባራዊ ማድረግን፣ ከስነ ምህዳሩ ጋር አብሮ መራመድ የሚያስችል የጥናትና ምርምር አቅም መገንባትን፣ በዘርፉ የሰለጠነና ብቁ የሰው ሃይልን ማፍራትን፣ የኢንፎርሜሽን ደህንነት ንቃተ ህሊና ማሳደግን፣ ስጋቶቹን በብቃት ማስተናገድ የሚችል የህግና ፖሊሲ ማዕቀፎች መዘርጋትንና የመሳሰሉ ተግባራት በራስ አቅም ማከናወን የግድ ይሆናል።

ረ/ የኢንፎርሜሽን ደህንነት ማረጋገጥ ጉዳይ በዋናነት በሪስክ ማኔጅመንት ስርዓት ላይ የተመሰረተ ነው። ስለሆነም የኢንፎርሜሽን ደህንነት ማኔጅመንት ስርዓት የመልካም አስተዳደር አካል ሲሆን የአመራሮችን በቂ ግንዛቤና ቁርጠኝነትን እንዲሁም የአሰራር ስርዓትና የስራ ሂደቶችን አካል እንዲሆን ማድረግ ያስፈልጋል።

ሰ/ የኢንፎርሜሽን ደህንነት የማረጋገጥ ጉዳይ የኢንፎርሜሽን ቴክኖሎጂ መሰረተ ልማትን የማስፋፋት ፕሮግራም ውህድ አካል ነው።

ሸ/ የኢንፎርሜሽን ደህንነት በቴክኒካዊ እውቀት ብቻ የሚረጋገጥ አይደለም። የኢንፎርሜሽን ደህንነት በርካታ ገፅታዎች ያሉት ሲሆን በዋናነትም ፖለቲካዊ፣ ህጋዊ፣ ኢኮኖሚያዊ፣ ማህበራዊ፣ ቴክኖሎጂያዊና አስተዳደራዊ ገፅታዎች ያሉት በመሆኑ ይህ ፖሊሲ እነዚህን እሳቤዎች ከግምት ባስገባና ሁሉም አቀፍ በሆነ መልኩ ተዘጋጅቷል።

E. As Ethiopia is becoming part of the international information society, it is also exposed and vulnerable to the global information security threats. This fundamentally challenging and dynamic issue requires, therefore, to build technological capabilities, research and development capabilities, implement international standards and best practices, develop and implement robust policy and legal frameworks, raise information security awareness of the public, and develop skilled manpower to the extent and advancement of the security threats.

F. Information security is an integral part of risk management system and business process which requires management awareness and commitment.

G. Information security is an integral part of ICT infrastructure development plan.

H. Information security cannot be handled only from its technological dimension. It should be understood as a systematic security framework including the political, economical, social, legal, technical and administrative dimensions. The policy is, therefore, developed in a holistic approach taking these basic assumptions in to account.

1.5 አጠቃላይ ግቦች

ሀ/ የሃገሪቱን የኢንፎርሜሽን ሃብትና የኢንፎርሜሽን መሰረተ ልማትን ከደህንነት ስጋት መከላከል የሚችል ጠንካራ የህግና የቁጥጥር ስርዓት መዘርጋት፣

ለ/ ሁሉም የህብረተሰብ ክፍሎችና ተቋማት በሃገራዊ፣ ተቋማዊና ግለሰባዊ የኢንፎርሜሽን ሃብትና የኢንፎርሜሽን መሰረተ ልማት የደህንነት ስጋቶች፣ ተጋላጭነቶችና መከላከያ መንገዶች ላይ ያላቸውን የግንዛቤ ደረጃ በማሳደግ የነቃ ተሳትፎ እንዲኖራቸው ማድረግ፣

ሐ/ የኢንፎርሜሽን ደህንነት ትምህርትንና ስልጠናን በማስፋትና በዘርፉ የሚከናወኑ የጥናትና ምርምር ስራዎችን በመደገፍና በማጠናከር የሰለጠነ የሰው ሃይልን ማፍራትና ሃገራዊ አቅምን መገንባት፣

መ/ ሃገራዊ፣ አህጉራዊና አለም አቀፋዊ ቅንጅትንና ትብብርን በማጠናከር የሃገሪቱ የኢንፎርሜሽን ደህንነት ስጋቶች፣ የኢንፎርሜሽን ጦርነቶችና የሳይበር ሽብርተኝነት የመከላከል አቅምን መገንባት፣

ሠ/ በምርምርና ስርፀት ላይ የተመሰረቱ ሃገራዊ የኢንፎርሜሽን ሴኩሪቲ ምርቶችንና አገልግሎቶችን ማቅረብ ማስቻል።

1.6 መርሆች

ሀ/ ለፖሊሲው የተሳካ አፈፃፀም መንግስት ስትራቴጂያዊ አመራር ይሰጣል፣

ለ/ ፖሊሲው የዜጎችን ህገ መንግስታዊ መብቶችና ነፃነቶች ማስጠበቂያ መንገድ ነው፣

ሐ/ የኢንፎርሜሽን ደህንነት የብሄራዊ ደህንነት ፖሊሲ፣ ስትራቴጂና ሌሎች የእለት ተእለት ተግባራት ውህድ አካል ነው፣

መ/ ኢንፎርሜሽን ቁልፍ ሃብት ነው፣

1.5. Strategic Objectives

The Strategic objectives of the national information security policy are to:

A. Establish a robust legal and regulatory frameworks that can facilitate the security of Ethiopia's information asset and information infrastructures;

B. Increase the awareness of all citizens regarding the value and importance of information assets (individual, organizational and national), the threats and vulnerabilities on information and information infrastructures so as to actively participate in applying security measures;

C. Promote information security education and training, foster research and development so as to produce skilled manpower and develop national capability on information security;

D. Develop national capability to prevent information security threats, information warfare and cyber terrorism through the promotion and strengthening of national, regional and international cooperation and coordination; and

E. Provide information security products and services based on research and development.

1.6. Guiding Principles

Implementation of this policy will be guided by the following general principles:

A. The Government shall provide strategic leadership and facilitate implementation of the policy;

B. The policy is a safeguarding mechanism of constitutional rights and freedom of citizens;

C. The policy is an integral part of the national security policies and strategies and other operational activities of the country;

D. Information is a valuable asset,

ሠ/ ማንኛውም የኢንፎርሜሽን ደህንነት ፕሮግራም በሪስክ ማኔጅመንትና በቀደምትነት መርህ ላይ ይመሰረታል፣

ረ/ የፖሊሲው አፈፃፀም ሂደት በህብረተሰቡ የነቃ ተሳትፎና በሁሉም ባለድርሻ አካላት ቅንጅት ላይ የተመሰረተ ይሆናል።

1.7 የመንግስት የኢንፎርሜሽን ደህንነት አቋም

የኢፌዲሪ መንግስት የኢንፎርሜሽን ደህንነት የሃገራዊ ሰላም፣ ልማት፣ ዲሞክራሲ ስርአት ግንባታና በአጠቃላይ የብሄራዊ ደህንነት አካል ነው ብሎ የምናል።

1.8 የፖሊሲው አድማስ

ፖሊሲው በሰነዶች፣ በሰዎች አስተሳሰብ፣ በኤሌክትሮኒክስ መሳሪያዎች፣ በዲጂታል ቅርጽ፣ በሲግናል፣ በጂኦ ስፓሻል ምስሎች፣ ካርታዎች፣ ስእሎች፣ ምልክቶች፣ በድምጽና ተንቀሳቃሽ ምስሎች መልክ ወዘተ በሚገኙ ዳታ፣ የተተነተኑና ያልተተነተኑ መረጃዎች፣ የአካላዊና ምናባዊ (virtual) የኢንፎርሜሽን መሰረተ ልማቶች ላይ ተፈፃሚ ይሆናል።

ምዕራፍ ሁለት
የኢንፎርሜሽን ደህንነት ፖሊሲ ስትራቴጂያዊ ትኩረት

2.1. የህግና የቁጥጥር ማእቀፎች

2.1.1. አጠቃላይ ምልከታ

የኢንፎርሜሽንና የኢንፎርሜሽን መሰረተ ልማት አጠቃቀም ተገቢ ጥንቃቄና ጥበቃ ካልተደረገለት በሃገር ደህንነት፣ በአእምሮአዊና ቁሳዊ ንብረቶች፣ በሰዎች ህይወትና ነፃነትና ብሄራዊ ጥቅም ላይ ጥቃትን ለሚሰነዝሩ የተለያዩ መንግስታት፣ ተቋማት፣ ቡድኖች፣ አሸባሪዎችና ግለሰቦች መጠቀሚያና የጥቃት ኢላማ

E. All information security programs and measures are based on risk management and priority principles; and
F. The implementation of the policy depends on the cooperation and coordination of all stakeholders, and the active participation of the whole society.

1.7. Government Information Security Stance

The Ethiopian government strongly believes that information security is an integral part of national peace, democratization, development and national security programs.

1.8. Scope of the Policy

This policy covers all data, processed and not processed information (individual, organizational or national) regardless of the medium used and the form they exist (be people, documents, electronic or digital devices, signals, maps, symbols, geospatial maps, voice, or in any other form and any other device) and all physical and virtual information infrastructures whereby information is collected, stored, processed and transmitted. It applies to both physical and virtual information security measures.

PART TWO
THE STRATEGIC FOCUS OF THE INFORMATION SECURITY POLICY

2.1 Adopt Appropriate Legal and Regulatory Frameworks

2.1.1. Overview

Information resources and information infrastructures of the country are highly vulnerable to various and complicated information threats. Unless adequate protection and security measures are taken, the national security, intellectual property rights, individual privacy, government and public interests would be at stake, and open a door for state- sponsored threat

ይሆናል። ስለሆነም መንግስት ይህንን ፈታኝ ሁኔታ በተሟላ መልኩ ማስተናገድ የሚችሉና እንደ አስፈላጊነቱም ከዘርፉ መለዋወጥ ጋር አብረው መራመድ የሚችሉ የህግና የቁጥጥር ስርዓቶች ለመዘርጋትና ለመተግበር ከዚህ በታች የተዘረዘሩት ግቦችና የአፈፃፀም ስትራቴጂዎች ነድፎ ይንቀሳቀሳል።

2.1.2. የፖሊሲ መግለጫ

የኢንፎርሜሽንና የኢንፎርሜሽን መሰረተ ልማት ደህንነትን ለማረጋገጥና ጥቃቶች ለመከላከል እንዲሁም አጥፊዎችን ተጠያቂ በማድረግ የክልከላ ሁኔታ (detternce) ለመፍጠር የሚያስችሉ አዋጆች፣ ደንቦችና መመሪያዎች ይወጣሉ፣ የቁጥጥር ስርአትም ይዘረጋል።

2.1.3. የህጋዊ ማዕቀፉ ግቦች

ሀ/ ህገ ወጥ ድርጊቶችን ተከታትሎ ለህግ በማቅረብ በዘርፉ የሚፈጸሙ የወንጀል ድርጊቶችን በመቀነስ የኢንፎርሜሽንን ተደራሽነት፣ ሚስጢራዊነትንና ተአማኒነትን ለማረጋገጥ የሚደረገውን ሂደት ማገዝ፣

ለ/ በኢንፎርሜሽንና የኢንፎርሜሽን መሰረተ ልማት ላይ ማንኛውም አይነት ጥቃት ማድረስ ወንጀል መሆኑ ግንዛቤ እንዲፈጠር ማድረግ፣

ሐ/ አጥፊዎችን ወደ ህግ በማቅረብ ማረምና ለሌሎች ማስተማሪያ በማድረግ፣ ሌሎች በወንጀል ድርጊቱ እንዳይሰማሩ በመከላከል የኢንፎርሜሽን ደህንነትን ለማረጋገጥ የሚደረገውን ሂደት ማገዝ፣

መ/ በኢንፎርሜሽን አሰባሰብ፣ ክምችት ፣ ትንተናና አጠቃቀም ዙሪያ በህዝቡ ዘንድ አመኔታንና መተማመንን በማሳደር የአገር ውስጥና የውጭ ኢንቨስትመንትን ማበረታታት።

actors, ideological and political extremists, organized criminals, cyber terrorists and individuals who can exploit our vulnerability.

Having taken this in mind, the government of Ethiopia has determined himself to enact laws and formulate appropriate regulatory frameworks pertinent to the complicated and dynamic nature of information security issues. The Government is therefore committed to the following legal and regulatory framework objectives and implementing strategies.

2.1.2. Policy Statement

Laws will be enacted and regulatory procedures adopted so as to secure information and information infrastructures and enforce appropriate legal measures that can deter information security threat actors.

2.1.3. Objectives of Legal Framework

A. To prevent, deter, respond to and prosecute acts of crime against information and information infrastructures and thereby help the process of ensuring confidentiality, integrity, availability and authenticity of information;

B. To criminalize any kind of attack against information and information infrastructures so as to raise public awareness on information security issues;

C. To take appropriate legal actions against information security offenders in order to reform, deter them from committing another crime and make them a lesson to others; and

D. To create conducive legal and regulatory environment in the collection, storage, process and transmission of information so as to build confidence and trust in the use of information and facilitate domestic and foreign investment.

2.1.3.1. የማስፈጸሚያ ስልቶች

ሀ/ በአለም አቀፍ ምርጥ ተሞክሮና ነባራዊ ሃገራዊ ሁኔታዎች ላይ መሰረት ያደረጉ፣ በበቂ ጥናት የተደገፉ፣ የሚመለከታቸውን አካላት ያሳተፉና ወቅታዊነታቸውን የጠበቁ መሰረታዊና የስነ-ስርአት ህጎች ይዘጋጃሉ።

ለ/ የኢንፎርሜሽን ደህንነት ህጎችን ለማስፈጸም አስፈላጊ ሆኖ ከተገኘ በዚህ ጉዳይ ላይ ስፔሻላይዝ ያደረጉ የፖሊስና የዓቃቤ ህግ ክፍሎች ሊቋቋሙ ይችላሉ።

ሐ/ በኢንፎርሜሽን ደህንነት ዙሪያ የሚከሰቱ አዳዲስ ለውጦችንና አዝማሚያዎችን በመከታተል የህግ ሽፋን እንዲኖራቸው በማድረግ፣ ህጎቹ ከስነ ምህዳሩ እድገት ጋር አብረው መራመድ በሚያስችል መልኩ በየጊዜው ይከለሳሉ።

መ/ በሚወጡ ህጎች ዙሪያ ለሚመለከታቸው የፍትህ አካላት በቂ የግንዛቤ ማስጨበጫ ስልጠናዎች በየጊዜው ይሰጣሉ።

ሠ/ የዜጎች ግላዊ መረጃዎችን ደህንነት ለመጠበቅ የሚያስችሉ ህጎች ይወጣሉ፣ የአሰራር ስርዓቶች ይዘረጋሉ።

2.1.4. የቁጥጥር ማዕቀፍ ግቦች

ሀ/ በሁሉም የኢንፎርሜሽን ደህንነት ትግበራዎች ዓለም አቀፍና ብሄራዊ ደረጃቸውን የጠበቁ የቁጥጥርና ክትትል ስርዓቶችን በመዘርጋት የኢንፎርሜሽን ደህንነት የማረጋገጥ ሂደቱን ማገዝ፣

ለ/ በሃገር ውስጥ የሚመረቱም ሆነ ወደ ሃገር ውስጥ የሚገቡ የኢንፎርሜሽን ደህንነት ምርቶችና አገልግሎቶች አለም አቀፋዊና ሃገራዊ የደህንነት ደረጃዎችን ያሟሉ መሆናቸውን ለማረጋገጥ የሚያስችል ስርዓት በመዘርጋት ደረጃቸውን ባልጠበቁ ወይም ለብሄራዊ

2.1.3.1. Implementing Strategies

A. Enact and enforce a comprehensive, well researched and participatory set of substantive and procedural laws relating to information security which are complementary to and in harmony with national and international laws, treaties and conventions;

B. Develop the capabilities of courts, the police and public prosecutors and establish specialized public prosecutor and police units as and when the need arises to facilitate implementation of the policy;

C. Drafting new legislations that are in tune with the technological changes and international developments in the area of information security to cover new trends or threats and periodically review them in order to keep abreast of the dynamic nature of information security threats;

D. Establish progressive training and capacity building programs for national law enforcement agencies, judges, prosecutors, police officers, investigators and intelligence officers to assist them in keeping track with new developments and threats; and

E. Adopt and implement data protection laws and procedures

2.1.4. Objectives of Regulatory Framework

A. To develop appropriate regulatory and monitoring frameworks in compliance with national and international security standards and best practices and apply in all information security measures so as to help the information security process; and

B. To ensure that all information security products and services produced domestically or imported from abroad are in compliance with national and international quality standards and security tests.

ደህንነት ስጋት ሊሆኑ በሚችሉ የቴክኖሎጂ ምርቶችና አገልግሎቶች ምክንያት ሊከሰቱ የሚችሉ የኢንፎር ሜሽን ደህንነት ስጋቶችን መከላከል።

2.1.4.1. የማስፈጸሚያ ስልቶች

ሀ/ ከኢንፎርሜሽን ደህንነት ጋር ተያያዥነት ያላቸውን ምርቶችና አገልግሎቶች ከማቅረብ ጋር የተያያዙ የጥራትና ቁጥጥር ደረጃዎችና መለኪያዎች በስራ ላይ ይውላሉ፣

ለ/ በአገር አቀፍ ፣ በክልሎች ደረጃና በየተቋማቱ ተግባራዊ የሚሆኑ የደህንነት ፖሊሲዎች፣ የደህንነት ደረጃዎች፣ ስታንዳርዶችና የአሰራር ስርዓቶች ይዘረጋሉ፣ ተግባራዊ ይደረጋሉ፣

ሐ/ አለም አቀፍ የኢንፎርሜሽን ደህንነት ምርጥ ተሞክሮዎችና ስታንዳርዶች ተቀምረው ከሀገራችን ሁኔታ ጋር እንዲጣጣሙ ይደረጋል፣

መ/ በዘርፉ የተሰማሩ ተቆጣጣሪና አስፈጻሚ አካላት በቂ አቅምና ግንዛቤ እንዲያገኙ ይደረጋል።

2.2. የኢንፎርሜሽን ደህንነት ንቃተ ህሊና

2.2.1. አጠቃላይ ምልከታ

የኢንፎርሜሽን ደህንነት የቴክኖሎጂ፣ የስራ ሂደት እና የሰው ልጅ መስተጋብር ውጤት ሲሆን፣ የሰው ልጅ ዋነኛው የኢንፎርሜሽን ቋትና የደህንነት ስጋት የተጋላጭነት ምንጭ ነው። ለዚህም የግንዛቤ ማነስ ዋነኛው ምክንያት ሲሆን፣ የአገራችንን ተጨባጭ ሁኔታ ስንመለከትም የኢንፎርሜሽን ደህንነት ጉዳይ የኢንፎር ሜሽን መሰረተ ልማት እድገትንና የኢንፎርሜሽን ተጠቃሚነትን ያህል በቂ ትኩረት ያልተሰጠውና በዘርፉ ያለው የግንዛቤ ደረጃም እጅግ አናሳ ነው። በመሆኑም በአገሪቱ የኢንፎርሜሽን ሃብትና መሰረተ ልማት ላይ

2.1.4.1. Implementing Strategies

A. Applying quality standards and security tests in all activities relating to the provision of information security products and services;

B. Enhance information and information infrastructure security policies, standards and procedures in the federal government, regional governments and in all critical infrastructures;

C. Adopt and implement international information security best practices and standards;

D. Build the capacity of concerned regulatory and enforcement bodies.

2.2. Raise Public Awareness

2.2.1. Overview

Information security is the combination of technological, process and human factors. As such, people are often the weakest link in the security chain and many information security vulnerabilities exist because of the lack of awareness. Therefore, it can be said that lack of awareness is the biggest vulnerability and open the door for security threats posed on the information assets and information infrastructures. To reduce such vulnerabilities and prevent information security

ከተጋረጡ ስጋቶች አንዱ የግንዛቤ እጥረት መሆኑ መረዳት ይቻላል። ስለዚህም መንግስት የሚከተሉትን ስልቶችና ግቦች በመከተል የኢንፎርሜሽን ደህንነት ንቃተ ህሊናና ባህል እንዲያድግ ይሰራል።

2.2.2. የፖሊሲ መግለጫ

በኢንፎርሜሽን ተዋንያኑ የህብረተሰብ ክፍሎች ዘንድ የኢንፎርሜሽን ደህንነት ስጋቶችና ተጋላጭነቶች ንቃተ ህሊና ከፍ በማድረግ፣ የኢንፎርሜሽን ዋጋና የኢንፎር ሜሽን ደህንነት አደጋዎች አስመልክቶ የመረጃ ልውውጥ ባህል እንዲጎለብትና የባህሪ ለውጥ እንዲመጣ ይደረጋል።

2.2.3. ግቦች

ሀ/ የመንግስት ተቋማትና ዜጎች በኢንፎርሜሽን ሚና እና ዋጋ ላይ ያላቸውን አመለካከት ማዳበር፣

ለ/ የኢንፎርሜሽን ደህንነት ቁልፍ ተዋናዮች ግንዛቤ ማሳደግ ፣ አቅም መገንባትና

ሐ/ በጥንቃቄ ጉድለትና ካለማወቅ የሚደርሱ ጥቃቶችን በማስወገድ የኢንፎርሜሽን ደህንነት የማረጋገጥ ሂደቱን ማገዝ።

2.2.4. የማስፈጸሚያ ስልቶች

ሀ/ በዋናነት የመንግስት ሚዲያዎች የኢንፎርሜሽን ዋጋና፣ መሰረታዊ የሆኑ ኢንፎርሜሽን ደህንነት ባህሪያትና የማስጠበቂያ መንገዶች ማስገንዘቢያ ፕሮግራሞች እንዲኖሯቸው ይደረጋል።

ለ/ የመንግስት ተቋማት (በተለይ ቁልፍ ተቋማት) በኢንፎርሜሽን ደህንነት ዙሪያ በየጊዜው የምክክር መድረኮች፣ ፓናሎች፣ ውይይቶች እና የመሳሰሉ የግንዛቤ ማስጨበጫ መድረኮች ያዘጋጃሉ፣

ሐ/ በኢንፎርሜሽን ደህንነት ዙሪያ የተሰማሩ ተቋማት ተደራሽነታቸውን በማስፋትና በማጠናከር ለህብረ

threats, the government is highly convinced that security awareness program is a critical component of the information security program. Considering all these issues, government will pursue the following objectives and strategies so as to improve information security awareness and develop security culture.

2.2.2. Policy Statement

Comprehensive national information security awareness program will be promoted so as to develop information security and information sharing culture among all stake holders.

2.2.3. Objectives

A. To increase and reinforce awareness of all citizens and government institutions about the value of information and information security, including the risks and threats associated;

B. To build the capacity of key information security actors and operators; and

C. To minimize information security threats that emanate from ignorance and negligence.

2.2.4. Implementing Strategies

A. Conducting targeted media programs on the value of information, importance of information security, the growing threats presented by vulnerabilities in and threats to information and information infrastructures, and the mechanisms necessary for self-protection;

B. Promote information security awareness-raising forums, panel discussions, debates, etc and facilitate active participation of all organizations, particularly critical infrastructures;

C. Expand and reinforce information security organizations outreach so that they can create and maintain situational

ተሰቡ ወቅታዊ የኢንፎርሜሽን ደህንነት ማስገንዘቢ ያዎችን እንዲሰጡ ይደረጋል።

2.3. ትምህርትና ስልጠና

2.3.1. አጠቃላይ ምልከታ

ለኢንፎርሜሽን ደህንነት ስጋት ከሚያጋልጡ ነገሮች ዋነኛው የሰለጠነ የሰው ሃይል አለመኖር ነው። በመሆኑም ደረጃው የጠበቀ የኢንፎርሜሽን ደህንነት ትምህርትና ስልጠና በአገራችን ተግባራዊ መደረግ እንዳለበት መንግስት በፅኑ ያምናል። ስለሆነም መንግስት የሚከተሉትን ስልቶችና ግቦች በመከተል በሃገሪቱ የኢንፎርሜሽን ደህንነት ትምህርትና ስልጠና ለማስፋፋት ይሰራል።

2.3.2. የፖሊሲ መግለጫ

በኢንፎርሜሽን ደህንነት የሰለጠነ የሰው ሃይል በማፍራት የሃገሪቱን የኢንፎርሜሽን ሃብትና የኢንፎርሜሽን መሰረተ ልማት አጠቃቀምና የኢንፎርሜሽን ደህንነት ስጋትንና ተጋላጭነትን የመከላከልና የመለየት አቅም ይገነባል።

2.3.3. ግቦች

ሀ/ በኢንፎርሜሽን ደህንነት ዘርፍ የሰለጠነ የሰው ሃይል በቀጣይነት በማፍራት በዘርፉ ሀገራዊ አቅም እንዲጎለብት ማድረግ፣

ለ/ በኢንፎርሜሽን ደህንነት ጥናትና ምርምር ተቋማት የሚፈለገውን የሰለጠነ የሰው ሃይል ማቅረብ፣

2.3.4. የማስፈጸሚያ ስልቶች

ሀ/ ከመዋእለ ህጻናት እስከ መካከለኛ ደረጃ ባሉ የትምህርት ተቋማት ለሚማሩ ተማሪዎች ቢያንስ ራሳቸውን ከጥቃት የሚከላከሉበት ስርአት ይዘረጋል፣ እውቀት እንዲያገኙም ይደረጋል።

awareness concerning information security vulnerabilities, threats, incidents and self protection measures.

2.3. Promote Information Security Education and Training

2.3.1. Overview

Lack of trained human power on information security is considered as one of the loop holes which make information and information infrastructure more vulnerable. Thus, the government of Ethiopia believes that information security education and training program shall be enforced.

The information security training and education program strives to produce relevant and needed security knowledge and skills within the workforce.

To this end, it is essential to make information security an integral part of the country's educational curriculum, and needs to revise the existing one. Therefore, the government is ready to follow the following objectives and strategies to extend information security education and training program.

2.3.2. Policy Statement

Adequate training and education programs will be fostered to develop skilled information security human resource and thereby support the country's information security needs and build security capabilities.

2.3.3. Objective

A. To build national capability in a way that can ensure information security in a strategic way through the proliferation of information security professionals in the country; and

B. To provide research and development organizations with adequately trained information security professionals

2.3.4. Implementing Strategies

A. Formulate a strategy to educate students at all levels of the school system so that they will develop basic information security literacy and skill for self protection;

ለ/ በሀገራቱ የሚገኙ የሁለተኛ ደረጃና ከፍተኛ የትምህርት ተቋማት በኢንፎርሜሽን ደህንነት ዙሪያ የትምህርትና ስልጠና ካሪኩለሞች እንዲቀረፁ ይደረጋል።

ሐ/ በኢንፎርሜሽን ደህንነት ዙሪያ ስልጠና የሚሰጡ ተቋማት እንዲጠናከሩ ይደረጋል።

መ/ ሁሉም የመንግስትና የግል ተቋማት የኢንፎርሜሽን ደህንነትን የስራ ሂደታቸው አካል እንዲያደርጉትና ስርዓት እንዲዘረጉ ይደረጋል።

2.4. ሃገራዊ ቅንጅት

2.4.1. አጠቃላይ ምልከታ

የኢንፎርሜሽን ደህንነት ስጋት እጅግ ውስብስብ፣ ኢተገማች፣ ተለዋዋጭና አለም አቀፋዊ በመሆኑ በተወሰኑ ተቋማት የተናጠል ጥረት እንዲሁም በመንግስት ጥረት ብቻ የሚፈታ ጉዳይ አይደለም። በመሆኑም መንግስት በሃገራቱ የኢንፎርሜሽን ደህንነት ላይ የተጋረጡ ስጋቶች የጋራ ስጋቶች በመሆናቸው የጋራ ሃላፊነትና የጋራ ርብርብ የሚጠይቅ ነው ብሎ ስለሚያምን የሚከተሉትን ግቦችና ስልቶችን በመከተል የኢንፎርሜሽን ደህንነት የሚያረጋግጥ ሃገራዊ ቅንጅት የማጠናከር ሰፊ ስራ ለመስራት ይንቀሳቀሳል።

2.4.2. የፖሊሲ መግለጫ

የኢንፎርሜሽን ደህንነት ስጋቶችን የመከላከልና ተጋላጭነቶችን የመቀነስ እንዲሁም ጥቃቶች ሲደርሱ የስራ ሂደቶች ሳይስተጓጎሉ፣ በአነስተኛ ወጪና በአጭር ጊዜ ወደ ነበረበት መመለስ እንዲቻል፣ ሃገራዊ አቅሞችን አስተባብሮ ለመጠቀም የሚያስችል ቅንጅት ይፈጠራል።

2.4.3. ግቦች

ሀ/ ሁሉም የመንግስት አካላት የመረጃ፣ የተሞክሮና ክህሎት ልውውጥ ባህልን በማጎልበት የኢንፎርሜሽን

B. Develop information security education and training curricula to secondary school and higher institutions;

C. Encourage and support private and governmental educational institutions and industrial establishments, to introduce and strengthen information security training; and

D. Create a conducive environment and procedure to make sure that information security is a built -in and integral part of all business processes, strategies and policies in all governmental and private organization.

2.4. Foster National cooperation and coordination

2.4.1. Overview

As information security has international, dynamic, sophisticate and challenging in nature, it cannot be solved by the separate efforts of certain organizations or the government alone. On the other hand, information security threats are shared perils of all stake holders. The government is therefore, strongly convinced that protecting information and critical information infrastructure is a shared responsibility that can best be accomplished through collaboration and synergy between government at all levels and the private sector. Therefore, the government will follow the following objectives and strategies to ensure national cooperation and synergy.

2.4.2. Policy Statement

Government-private collaborative relationships will be established so as to effectively manage information security risks and build national capability to prevent, detect, deter, respond to, and recover from information security incidents.

2.4.3. Objectives

A. To promote information, best practices and knowledge sharing culture among governmental organizations and institutions so as to support the information security process;

D. To define roles and responsibilities of all stakeholders and

እነዚህን ችግሮች ለመፍታትና አለም አቀፍዊ ይዘት ያለውን የኢንፎርሜሽን ደህንነት ስጋት ለመከላከል የአለም አቀፍ ማህበረሰብን ትብብር ይጠይቃል። መንግስትም ይህንን እውነታ በመገንዘብ የሚከተሉትን ግቦችና ስትራቴጂዎች ነድፎ አለም አቀፍ ትብብርን ለማጠናከር ይሰራል።

2.5.2. የፖሊሲ መግለጫ

በኢንፎርሜሽን ደህንነት ዙሪያ የእውቀትና የቴክኖሎጂ ሽግግር እንዲኖር ሁኔታዎች ማመቻቸትና የተደራጀ ወንጀልና የሳይበር ሽብርተኝነት የመሳሰሉ ብሄራዊ፣ አህጉራዊና አለም አቀፋዊ የሳይበር ወንጀሎችን ለመመከት የሚያስችል አለም አቀፍ ቅንጅት ይጠናከራል።

2.5.3. ግቦች

ሀ/ የሳይበር ወንጀልና መሰል አለም አቀፍ ይዘት ያላቸው የኢንፎርሜሽን ደህንነት ስጋቶች በመከላከል ዙሪያ የሚፈጠሩ የህግ ግዛት ጥያቄዎችን መፍታት፣

ለ/ አለም አቀፍ የልምድ ልውውጥና የእውቀት ሽግግርን የሚያፋጥን ስርአት መዘርጋት፣

ሐ/ የሁለትዮሽ ስምምነትና ጥረትን ማበረታታት።

2.5.4. የማስፈጸሚያ ስልቶች

ሀ/ በሃገሪቱ ውስጥ የሚቀረፁ የኢንፎርሜሽን ደህንነት ህጎችና ፖሊሲዎችን ከአለም አቀፍ ደረጃዎችና ስታንዳርዶች ጋር የተጣጣሙ እንዲሆኑ ይደረጋል፣

ለ/ አለም አቀፍ በሆኑ የኢንፎርሜሽን ደህንነት መድረኮች ላይ ንቁ ተሳትፎ ይደረጋል፣

ሐ/በኢንፎርሜሽን ደህንነት ዙሪያ የሚኖሩ አህጉራዊና አለም አቀፋዊ የትብብርና የአጋርነት ስምምነቶች አስፈላጊነታቸው እየታየ ይፈረማሉ።

Therefore the fighting against information security threats will require international cooperation to raise awareness, increase information sharing, promote security standards, investigate and prosecute those who engage in information security threats, and facilitate direct foreign investment. The Ethiopian government is committed to working with nations and international organizations to ensure the integrity of the global information networks that support critical economic and security infrastructure. To promote and strengthen this international cooperation government is determined to following objectives and strategies.

2.5.2. Policy Statement

Recognizing the need for global collaboration on technical and legal matters in order to curb national, regional and international cybercrimes, organized crime, cyber terrorism and other information security threats, Ethiopia will promote bilateral and multilateral cooperative endeavors.

2.5.3. Objectives

A. To resolve jurisdictional issues so that prevent international cyber crime, cyber terrorism and other related threats;

B. To facilitate international best practice and knowledge sharing; and

C. To promote bilateral agreements and efforts.

2.5.4. Implementing Strategies

A. Ensure that all local information security policies, laws and regulations are complementary to and in harmony with international laws, standards and best practices;

B. Participate actively in all relevant international information security bodies, panels, forums, conferences and multi-national agencies to promote national prevention of,

C. Adopt and ratify regional and international cooperative agreements on information security issues based on their merits.

2.6. ምርምርና ስርፀት

2.6.1. አጠቃላይ ምልከታ

በኢንፎርሜሽን ደህንነት ቴክኖሎጂዎች ላይ የሚደረገው ምርምርና ስርፀት አስተማማኝና ጥራታቸውን የጠበቁ ምርቶችንና አገልግሎቶችን በአገር ውስጥ እንዲመረቱ፣ አዳዲስ የኢንፎርሜሽን ጥቃቶችን በመለየት እና መፍትሄን በማበጀት እንዲሁም ጥሩ የአገራት ተሞክሮችን ወደ አገር ውስጥ በማምጣት ረገድ ከፍተኛ የሆነ ድርሻ የሚጫወት ሲሆን፤ መንግስት በዘርፉ ለሚካሄዱ ጥናትና ምርምሮች ልዩ ትኩረት ይሰጣል።

2.6.2. የፖሊሲ መግለጫ

በምርምርና ስርፀት ላይ የተመሰረቱ የኢንፎርሜሽን ደህንነት ምርቶችን እና አገልግሎቶችን በማቅረብ የመከላከል፣ ተጋላጭነትን የመቀነስና ምላሽ የመስጠት ሃገራዊ አቅም ይገነባል።

2.6.3. ግቦች

ሀ/ የእውቀት፣ የቴክኖሎጂና የተሞክሮ ሽግግር ላይ ያተኮረ የምርምርና ስርፀት አቅም በመገንባት የኢንፎርሜሽንና የኢንፎርሜሽን መሰረተ ልማት ደህንነትን ለማረጋገጥ የሚያስችሉ ሀገራዊ አገልግሎቶችንና ምርቶችን ማቅረብ፣

ለ/ ሃገራዊ የኢንፎርሜሽን ደህንነት ማኔጅሜንት ስርአቶችን በውስጥ አቅም ማበልጽግ፣ መዘርጋት።

2.6.4. የማስፈጸሚያ ስልቶች

ሀ/ በኢንፎርሜሽን ደህንነት ዙሪያ የተፈጠሩትን ሃገራዊ አቅሞችና ተሞክሮዎች እንዲጠናከሩና የቀጣይ እድገት መሰረት እንዲሆኑ ይደረጋል።

2.6. Enhance R & D towards Self Reliance

2.6.1. Overview

The dynamic nature of information security requires the continuous development of research and development capabilities in order to develop knowledge and expertise to face new and emerging security challenges, to produce cost-effective, indigenous security solutions. In recognition of the important role that R&D plays in information security the Government, therefore, commits itself to the following specific objectives and strategies.

2.6.2. Policy Statement

Information security products and services based on R&D will be enhanced so as to build prevention, detection, deterrence, response, and recovery national capabilities

2.6.3. Objectives

A. To provide national information and information infrastructure security services and products; and
B. To develop and implement national information security management system through internal capability.

2.6.4. Implementing Strategies

A. Strengthen and utilize the existing national information security capabilities and use them as foundation for further self-reliance R&D capabilities;

ለ/ በኢንፎርሜሽን ደህንነት ላይ ምርምር ከሚያከናውኑ አለም አቀፍ ተቋማት ጋር የቅርብ ትስስር ይፈጠራል።

ሐ/ ተግባራዊ የምርምር ስራዎች እንዲጠናከሩ ይደረጋል።

መ/ በመንግስትም ሆነ በግል ተቋማት፣ ቤተ ሙከራዎችና መሰል የምርምር ማዕከላት ውስጥ ለሚደረጉ የምር ምርና የቴክኖሎጂ ሽግግር ስራዎችን በመደገፍ ሃገር በቀል የኢንፎርሜሽን ደህንነት ቴክኖሎጂና አገልግሎ ቶች አምራችነት አቅም እንዲጎለብት ይደረጋል።

ሠ/ በክሪፕቶግራፊ ምርት፣ ዝውውርና አጠቃቀም ሂደቶች ላይ የማኔጅመንት ስርአት ይዘረጋል።

ረ/ ከአምራቾች ጋር ቀጥተኛ የአጋርነት ግንኙነት ይመሰረ ታል።

2.7. የቁልፍ የኢንፎርሜሽን መሰረተ ልማቶች ልዩ ጥበቃ ማጠናከር

2.7.1. አጠቃላይ ምልከታ

የሃገራቱ ቁልፍ ተቋማትና መሰረተ ልማቶች የኢኮቴን እድገት ተከትሎ አውቶሜትድ እየሆኑና በኢንፎርሜሽን መሰረተ ልማቶች አማካኝነት እርስበርሳቸው እየተሳሰሩ በመምጣታቸው ለ24/7 የደህንነት ስጋት የተጋለጡ እና የ24/7 አካላዊና ምናባዊ (አካላዊ ያልሆነ) ጥበቃ የሚያስ ፈልጋቸው ዘርፎች ሆኗል። በእነዚህ ተቋማትና መሰረተ ልማቶች ላይ ሊደርስ የሚችለውን የኢንፎርሜሽን ደህንነት አደጋ የሃገራችን ብሄራዊ ደህንነት ስጋት ላይ የሚጥል፣ ከፍተኛ ፖለቲካዊ፣ ኢኮኖሚያዊና ማህበራዊ ውድቀት የሚያስከትል መሆኑን በመገንዘብ መንግስት የሚከተሉትን ግቦችና ስትራቴጂዎች በመንደፍ ደህንነታቸውን ለማረጋገጥ ይሰራል።

B. Establish closer ties with the international research community in the scientific fields which underpin information security;

C. Support and encourage applied research activities;

D. Support government and private institutions and laboratories which involve in R&D and technology transfer activities aimed at increasing domestic competence on information security;

E. Develop and implement appropriate management system of cryptography products; and

F. Establish collaborative and direct partner[illegible] with producers and service providers.

2.7. Protection of Critical Information Infrastructures

2.7.1. Overview

Infrastructures considered critical are those physical and information-based facilities, networks and assets, which are vital to the nation that if damaged would have a devastating impact on well-being of citizens, national economic strength, national image, national defense and security, government capabilities to function, and public health and safety.

Technological progress has lead to more automation in the operation and control of these critical infrastructures and the creation of a special information infrastructure. Critical information infrastructure is the nervous system of all critical infrastructures and hence vulnerable to 24/7 security threats requiring 24/7 physical and virtual protection. Therefore, the government articulates the following objectives and strategies to protect key information infrastructure of a country.

2.7.2. የፖሊሲ መግለጫ

በአገራቱ ቁልፍ የኢንፎርሜሽን መሰረተ ልማቶች ላይ የሚደርሰውን የኢንፎርሜሽን ደህንነት ስጋትን መከላከልና ተጋላጭነቶችን የመቀነስ ተግባር ቀዳሚነትን ያገኛል፣ ልዩ ጥበቃም ይደረጋል።

2.7.3. ግቦች

ሀ/ በቁልፍ ተቋማትና መሰረተ ልማቶች ላይ ሊደርሱ የሚችሉ ውድመቶችን መከላከል፣

ለ/ ውስን ሃገራዊ አቅምን በተገቢና ቁልፍ ሃብት ላይ እንዲውል ማድረግ፣

ሐ/ የሁሉም ሃይሎች ጥረትን ማቀናጀት፣

2.7.4. የማስፈጸሚያ ስልቶች

ሀ/ ቁልፍ የኢንፎርሜሽን መሰረተ ልማቶችና ሃብቶች ተለይተው በየደረጃው ይመደባሉ።

ለ/ የኢንፎርሜሽን ደህንነት ስጋት አስተዳደር ስርዓት ይዘረጋል።

ሐ/ ተከታታይ የኢንፎርሜሽን ደህንነት ስጋት ተጋላጭነት ዳሰሳ ጥናቶች ይከናወናሉ።

መ/ ቁልፍ ተቋማት ከዚህ ፖሊሲና ከአለም አቀፍ ምርጥ ልምዶች፣ ስታንዳርዶችና የአሰራር ስርዓቶች ጋር የተጣጣመ የኢንፎርሜሽን ደህንነት ፕሮግራም እንዲቀርፁና የስራ ሂደቶቻቸው አካል እንዲያደርጉት ይደረጋል።

ሠ/ ደህንነታቸው የተረጋገጡ ምርቶች፣ አገልግሎቶች፣ ፕሮቶኮሎችና የመገናኛ ዘዴዎች፣ አስተማማኝ ኔትዎርኮችና ዲጂታል የቁጥጥር ስርዓቶች ተግባራዊ ይደረጋሉ።

ረ/ በማንኛውም ጊዜ የተጋላጭነት ፍተሻና የኢንፎርሜሽንና የኢንፎርሜሽን መሰረተ ልማት ሴኩሪቲ አዲት

2.7.2. Policy Statement

Security measures will focused on and priority will be given to prevent information security attacks against critical infrastructures, reduce national vulnerabilities to cyber attacks; minimize damage and recovery time from cyber attacks that do occur.

2.7.3. Objectives

A. To protect critical organizations and infrastructures form information security threats.

B. To apply national capabilities and resources on appropriate and critical national assets protection; and

C. To coordinate and integrate efforts of all information security actors.

2.7.4. Implementing Strategies

A. Classify and prioritize critical information infrastructures and assets;

B. Develop information security management system;

C. Undertake continuous risk assessment studies and testing activities to evaluate reliability and vulnerability of the information security systems of critical infrastructures;

D. Make sure that all critical infrastructures have formulated organizational information security policies, standards and procedures in conformity with the national information security policy, international best practices, standards and procedures and make an integral part of their business process;

E. Ensure that secured and reliable products, services, networks, cryptography algorism standards, communication systems, and digital controlling systems are applied in critical information infrastructures;

F. Undertake periodic and accidental penetration tests and information security audit to evaluate the security strength

እንዲካሄዱና ፈጣን የማስተካከያ አርምዳምቱን አንዲወ ሰዱ ይደረጋል።

ሰ/ በሁሉም ቁልፍ ተቋማት የኢንፎርሜሽን ደህንነት አደጋ ዎች መከላከል ግብረ ሃይል ይቋቋማል።

ሸ/ ቁልፍ የኢንፎርሜሽን መሰረተ ልማቶች የ24/7 አካላዊ ጥበቃ ይጠናከራል።

ምዕራፍ ሶስት

የፖሊሲው የአፈፃፀም ማዕቀፍ

3.1. ተቋማዊ አወቃቀር

የኢንፎርሜሽንና ኢንፎርሜሽን መሰረተ ልማቶች ደህንነት ለማረጋገጥ ጠንካራ አቋም ያላቸው ተቋማት መፍጠርና ማጠናከር ያስፈልጋል። መንግስትም ይህንን እውነታ በመገንዘብ እንደ ኢመደኤ ያሉ የኢንፎርሜሽን ደህንነት ተቋማዊ የማእዘን ድንጋዮችን ማስቀመጥ ጀምሯል። ከዚህም በተጨማሪ በሃገርና በቁልፍ ተቋማት ደረጃ ከኢንፎርሜሽን ደህንነት ጋር በተያያዘ የሚከሰቱ ለውጦች፣ አደጋዎችና የአደጋ ምልክቶች የመረጃ ልውውጥ አገናኝ ድልድይ ሆነው የሚያገለግሉ የኮምፒውተር አደጋዎች መከላከል ግብረ ሃይሎች (CERTs) ይቋቋማሉ። እንደአስ ፈላጊነቱም መንግስት ለፖሊሲው አፈፃፀም በሚያመች ሁኔታ አዳዲስ ተቋማትን ሊያቋቁም ወይም ባሉት ተቋማት ላይ ሃላፊነትን ሊጨምር ይችላል።

3.2. የተቋማት ድርሻና ሃላፊነት

ሁሉም የመንግስት ተቋማት ይህንን ፖሊሲ የመተግበርና ከፖሊሲው አፈፃፀም ጋር በተያያዘ ተልእኳቸውን መሰረት ያደረጉ ሌሎች ስራዎችን የማከናወን ግዴታ አለባቸው። በተጨማሪም ከዚህ ፖሊሲና አለም አቀፍ ስታንዳርዶች የሚጣጣም የኢንፎርሜሽን ደህንነት ጥበቃ ፕሮግራም የመንደፍና የመተግበር ሃላፊነት ያለባቸው ሲሆን

networks, cryptography algorism standards, communication systems, and digital controlling systems are applied in critical information infrastructures;

F. Undertake periodic and accidental penetration tests and information security audit to evaluate the security strength and preparedness of critical infrastructures, and take appropriate corrective measures;

G. Establish CERTs in all critical institutions and infrastructures; and

H. Ensure 24/7 virtual and physical protection of critical information infrastructures.

PART THREE

A FRAMEWORK FOR POLICY IMPLEMENTATION

3.1. Institutional Arrangements

In recognition of the dynamic, unpredictable and complex nature of information security threats, the Government has put in place the necessary institutional building blocks. Amongst the measures taken so far is the establishment of the Ethiopian Information Network Security Agency.

In addition to this CERT will also be established at the national level, in all critical infrastructures and government agencies that will serve as single point of contact for coordination of incident information security issues.

The Government will further commit itself to make the necessary changes to the existing institutions as well as make new arrangements as and when the need arises to facilitate implementation of the policy

3.2. Role and Responsibilities

All government institutions and agencies have the duty to implement this policy and to perform other activities in relation to the implementation of this policy based on their mission. In addition to this, they have the duty to formulate and implement

በፕሮግራሞቻቸውም የሚከተሉትን ቁልፍ የደህንነት ጥበቃ አሃዶችን ማካተት ይኖርባቸዋል።

1. ተቋማዊ የኢንፎርሜሽን ደህንነት ፖሊሲ ማእቀፎች ማዘጋጀት፣
2. የግንኙነትና ኦፕሬሽን ማኔጅመንት ስርአት መዘርጋት፣
3. የተደራሽነት ጥበቃ ስርአት መዘረጋት፣
4. የኢንፎርሜሽን ደህንነት ስርዓቱን ለማስጠበቅ የሚያስችል የሰው ሃይል አስተዳደር ስርዓት ማበጀት፣
5. የደህንነት ስጋት ማኔጅሜንት ስርአት መዘርጋት፣
6. አካላዊና ከባቢያዊ ደህንነት ጥበቃ ስርአት መዘርጋት፣
7. የሃብት ምደባና ጥበቃ ስርአት መዘርጋት፣
8. የግዥ ሂደቶች፣ የማበልጸግ ሂደቶች፣ የትግበራና ጥገና ሂደቶች ደህንነት ቁጥጥር ስርዓት መዘርጋት፣
9. የስራ ሂደት ቀጣይነት ማኔጅመንት ስርዓት መዘርጋት፣
10. የድንገተኛ ክስተቶች ማኔጅመንት ስርአት መዘርጋት፣
11. የኢንፎርሜሽን ደህንነት ማኔጅመንት ስርአት መዘርጋትና
12. ከተዛማጅ ሕጎችና ፖሊሲዎች ጋር ያለውን መጣጣም ማረጋገጥ።

information security policies and programs inconformity with this policy and international standards. While the priority and focus of the programs may differ based on the specific needs and missions of each institution, the following security components should be considered as minimum requirements.

- Organizational information security policy,
- Communication and operation management system,
- Access control (logical, physical and administrative),
- Develop human resource management system in the way to ensure information security,
- Risk management system,
- Physical and Environmental Security,
- Asset classification and control,
- Systems acquisition, Development, Purchasing and Maintenance,
- Business continuity management,
- Information Security Incident Management and disaster recovery system,
- Information Security Management, and
- Compliance with laws and regulations.