http://it.telangana.gov.in

Jayesh Ranjan IAS
Secretary to Government

Information Technology, Electronics
& Communications Department
Government of Telangana
D - Block 2nd Floor Room No. 315A
Telangana Secretariat Hyderabad-500 022
P. +91 40 2345 6401 F. +91 40 2345 0103
secy_itc@telangana.gov.in
jayesh_ranjan@hotmail.com

ramakantadvertising.com

CYBER SECURITY POLICY 2016

Information Technology, Electronics & Communications Department
Government of Telangana

Sri K. Taraka Rama Rao

Hon'ble Minister for IT, Panchayat Raj, MA&UD
Government of Telangana

MESSAGE

In the IT Policy released by the Telangana Government in April 2016, we have identified a number of emerging technologies where opportunities beckon both Government and private industries to create new products and services, to innovate, and to position India on the global map as a leader.

When the Prime Minister launched the Digital India program in July 2015, he mentioned about a new kind of warfare going on in the world. He described cyber wars as bloodless wars that have the potential of creating untold damages in the world. At the same time, he also exhorted that while India should stay sufficiently guarded to protect itself, we should see this as an opportunity to raise a force strong enough to protect the rest of the world.

About a year ago, I got a chance to interact with the CEO of MasterCard who mentioned to me that thousands of attempts are made to hack their databases on a daily basis. Many other large companies face similar attacks. However, not much of Cyber Security work is coming India's way due to a variety of reasons. While everyone is speaking about it, no Government has really made an organized effort to support this vertical. There is a serious dearth of training and skilled manpower who can act as 'cyber warriors.' Our legal framework is also not robust enough to promote data sharing, maintain data confidentiality etc.

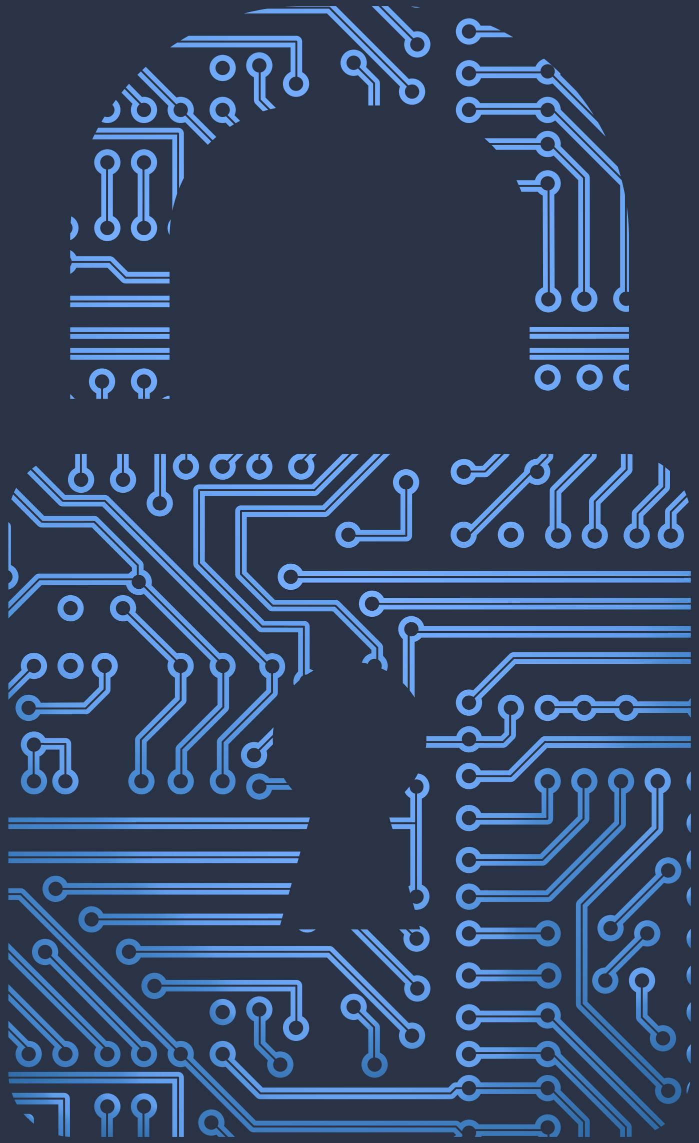
Our aim in Telangana is no different from capitalizing on the opportunities the Prime Minister has pointed out and in sync with the solutions the private industry is looking for. Not only will we ensure that vital databases of the Government are secure and protected, we will also take the lead in supporting the security requirements of the industry.

By announcing a separate policy on Cyber Security, we are making a strong statement of our intent to become the go-to hub where all stakeholders work on developing new products, test them, and eventually deploy them the world over. Telangana will offer the best quality manpower equipped to do so. We will also provide a legal framework which raises the confidence of the private sector in sourcing their cyber security related services from the State. A comprehensive architecture of institutions promoted by the Government will be in position.

Just as India is becoming more and more sensitive to the growing cyber threats, there are a few other countries / regions that have developed a strong reputation of being the leaders in cyber security. Israel and The Hague Security Delta are two such best examples. In the Government, our effort will be to also partner with such international agencies and learn and replicate the good practices that they have rolled out.

Moreover, the common public is a crucial stakeholder. While the Governments, private companies and institutions do their bit to ward off cyber security threats, every citizen of Telangana who is digitally connected must become aware of the cyber threats and conduct his cyber behavior with responsibility.

I am confident that the first-of-its-kind policy on cyber security being brought out by the Government of Telangana will earn the appreciation of all the stakeholders. The cyber war is indeed a faceless enemy threatening the advancement of the global economy further into the digital era. Such an obscure threat can only be countered by collective efforts from all the stakeholders, and I believe this policy on cyber security creates a collaborative environment to do so.



CYBER SECURITY POLICY

INDEX

PREAMBLE 06

CYBER SECURITY IN INDIA 07

VISION 08

DEFINITIONS 09

LEGAL AND REGULATORY FRAMEWORK 10
I. CYBERLAW AND RELATED LEGISLATION 10
Collaboration to Establish Robust Legal Framework 10

II. CYBER CRIME CELL 10
Cyber Grievance Redressal Efforts 10
Efforts against Pornography, Cyber Bullying, and Sexual Harassment 10

III. CYBER FORENSICS 10

COMPLIANCE AND ENFORCEMENT FRAMEWORK 11
I. PROTECTION OF CII 11
Risk Based Approach in Protecting Critical Information Infrastructure (CII) 11
Think Tank for Policy and Decision Inputs 11

II. EMERGENCY RESPONSE 11
Apex Agency for State-wide Coordination 11
Business Continuity 11

III. STANDARDS AND PRACTICES 12
Information Sharing and Analysis Centre 12
Promotion of Open Standards 12
Procurement of Safe ICT Products by the State 12

IV. ISMS IMPLEMENTATION 12

V. ICT SECURITY CERTIFICATION 12
Certification of Cyber Security Products and Services 12

CAPACITY BUILDING AND CYBERSECURE ACCULTURATION FRAMEWORK 14
I. INFORMATION SECURITY WORKFORCE CAPACITY BUILDING 14
Certification Programs through TASK 14
Collaboration with Academic and Research Institutions 14
Cyber Warriors 14
Customized Training Programs 14

II. CYBER SECURITY ACCULTURATION 15
Multi-Channel Awareness Campaign 15
School Level Cyber Security Education 15
Guidelines for Safe Practices 15
Cyber Security Challenge 15

BUSINESS DEVELOPMENT FRAMEWORK 16
I. PROMOTE LOCAL CYBER SECURITY INDUSTRY 16
Dedicated Incubator for Cyber Security Startups 16
Annual Cyber Security Expo 16
Promoting SMEs in Cyber Security 16
Fiscal and Non-Fiscal Incentives 16

II. STRATEGIC PARTNERSHIPS 16
Collaboration with Private Sector for R&D 16
Partnering with Service Providers 16
Partnering with Private Sector 16
Partnerships with International Agencies 17

STAKEHOLDERS' RESPONSIBILITIES 18
Citizens 18
Private Sector 18
Partners 18
Government 18
APPENDIX I 19

CONCLUDING NOTE 21

PREAMBLE

Cyber Security is among the leaders in emerging technologies in the world. Dealing with the security of Cyberspace, the virtual environment where people and software interact over a complex web of computer networks, Cyber Security is on the path towards gaining increasing prominence as we move towards a technology driven future. Currently, the size of the industry is estimated to be USD 100 Billion, and is projected to grow to USD 170 Billion by 2020.

Government and military organizations, and other businesses, store and process significant volumes confidential data, regularly transmitted across networks, thereby increasing the exposure to cyber threats. The potential damages can not only lead to monetary losses, but also put national security at stake if critical information infrastructure is targeted.

Two cyber incidents that stand out in the recent past are the 2016 heist of Bangladesh Bank and the 2015 power outage in Ukraine affecting over 225,000 citizens. The Ukraine attack was the first confirmed attack in the world to have taken down a power grid. Such incidents expose the vulnerabilities in a world where more and more data and processes are being shifted online. Hence, protection of data is gradually positioning itself as a priority of any 21st century Government.

Ensuring a safe cyberspace is of paramount importance to Telangana, whose growth story is driven primarily by Information and Communication Technology, one of the critical sectors that rides on and resides in the cyberspace. Hyderabad, which is home to the top 5 technology firms in the world, is next only to Bangalore in terms of IT exports and contributes to more than 10% of the total IT exports of the country. In the next 5 years, Telangana plans to establish 3 Tier II cities as IT Hubs and double the IT exports value by focusing on new-age technologies like cloud computing, Artificial Intelligence and Internet of Things, which are expected to increase automation and improve the quality of living. However, they also bring in a horde of other challenges pertaining to cyber security.

Within the next 20 years, these sectors will advance in incomprehensible ways, and it becomes the responsibility of every state to be at the crest of this change. It is extremely important to send out a strong and clear message in this direction. A robust cyber security policy will ensure that citizens are protected in the cyber space, the state is well equipped to meet the cyber security challenges, and a conducive atmosphere is created for investors.

CYBER SECURITY IN INDIA

India has taken its first step towards ensuring a safe cyberspace to all its stakeholders in 2000, when it passed the IT Act 2000. The act was later amended giving way to the IT (amendment) Act 2008, mainly to cover security related issues. Various other initiatives were simultaneously undertaken by the Government of India to address cyber security challenges. One such initiative was the Indian Computer Emergency Response Team, which has been functional since 2004 and is actively involved with mitigating cyber crime. To integrate all the initiatives in this area and tackle the fast-changing nature of cyber crimes, the Government has launched the National Cyber Security Policy in 2013. Initiatives such as setting up the NCCC, NCIIPC, creating sectoral CERTs under CERT-In to deal with sector specific security issues were taken up through this policy.

Although this is a step in the right direction, the destination lies far ahead. 2015 has witnessed a rise in cyber crime, with over 94% of organizations facing major threats. However, most firms have not started taking cyber crime seriously, with only 74% firms conducting a detailed annual IT and cyber risk assessment. Additionally, the number of cybercrime cases registered in India has been growing at a CAGR of over 100% in the last 5 years. Technology typically has an exponential growth rate. So is the case with cybercrime which goes hand in hand with technology.

Although the Government of India has passed laws and set up agencies, the onus is on the individual States to take up initiatives, drive on-ground implementation and ensure that a safe cyber space is created in the local environment. Hence, it becomes imperative for each state to adopt a dynamic approach to maintain a safe cyber space through effective and ever evolving policies.

VISION

The State of Telangana is committed to creating and sustaining a safe and resilient cyberspace to promote well-being of its citizens, protection and sustainability of its infrastructure, and creation of wealth through investment and growth in this sector. The following table summarizes the vision to achieve a safe and resilient cyber space for Citizens, Businesses and Government:

1. Build awareness about cyber security and safe cyber practices among citizens
   Establish requisite Institutions and legal framework to counter cyber crime

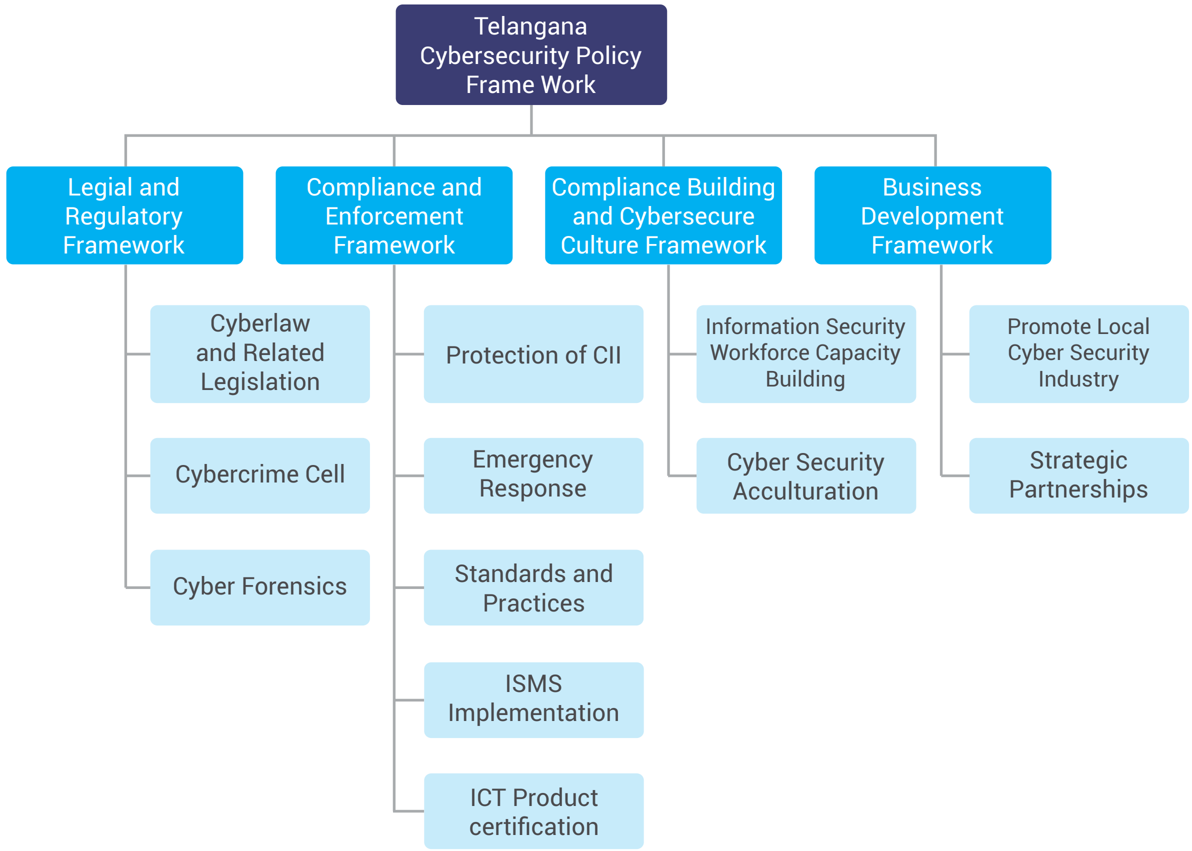
3. Build capacity and protect our Critical Information Infrastructure

4. Equip professionals with requisite cyber security skills and knowledge and establish a pool of "Cyber Warriors" to work with the State

5. Promote the state as an ideal destination for cyber security firms and startups to develop cyber security products

6. Encourage State-State and inter-institutional partnerships to promote data sharing and collaborative research efforts

The Cyber security Policy Framework holds several other frameworks that are intended to provide a holistic and complete solution the cyber security threat. The four pillars that hold up the State cyber security policy framework are as under:



Telangana Cybersecurity Policy Frame Work

Legal and Regulatory Framework
- Cyberlaw and Related Legislation
- Cybercrime Cell
- Cyber Forensics

Compliance and Enforcement Framework
- Protection of CII
- Emergency Response
- Standards and Practices
- ISMS Implementation
- ICT Product certification

Compliance Building and Cybersecure Culture Framework
- Information Security Workforce Capacity Building
- Cyber Security Acculturation

Business Development Framework
- Promote Local Cyber Security Industry
- Strategic Partnerships

DEFINITIONS

Cyber Space - Cyber space is a complex environment consisting of interactions between people, software, and services, supported by worldwide distribution of information and communication technology (ICT) devices and networks.

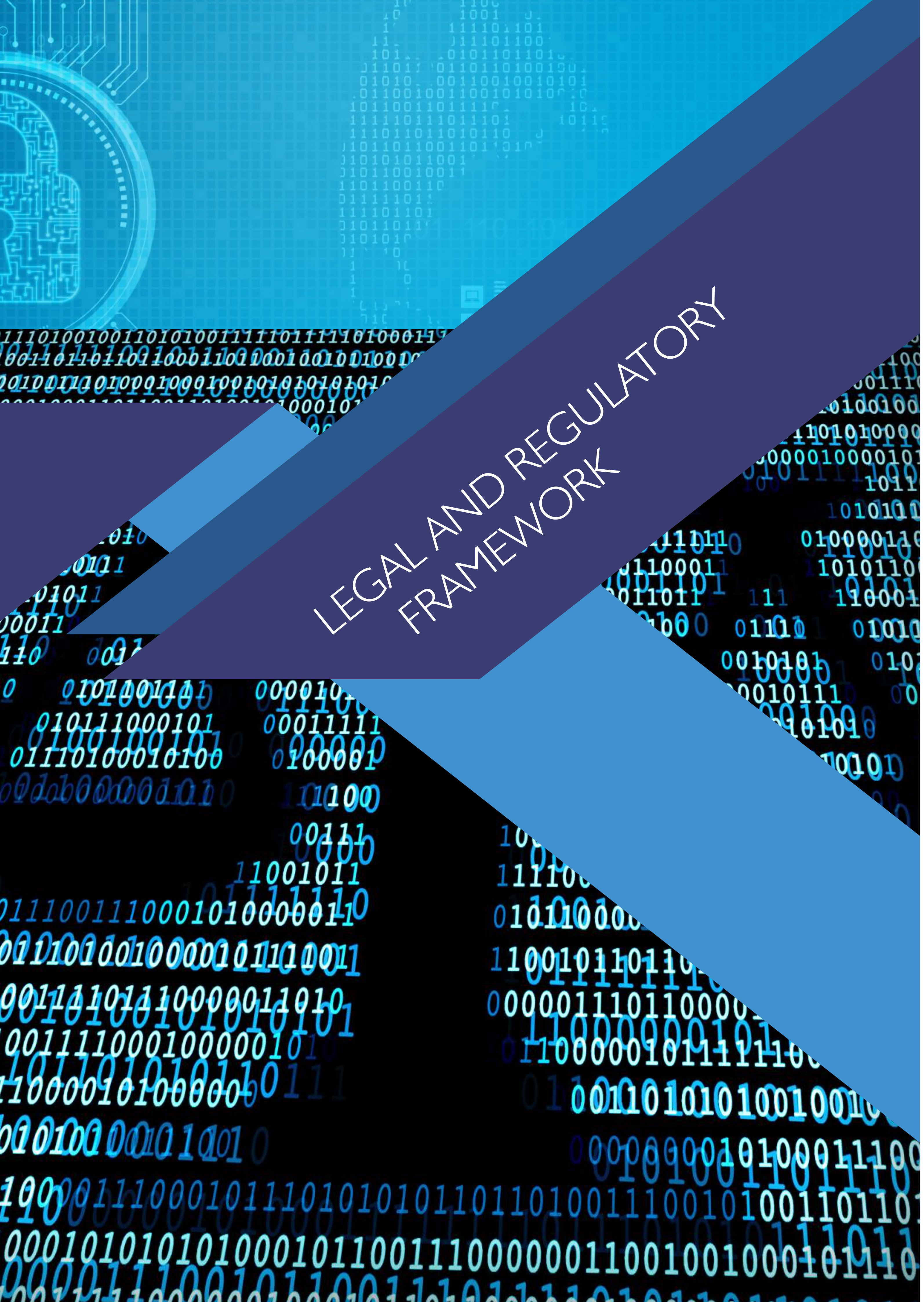
Cyber Security - The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.

Critical Information Infrastructure - Critical Information Infrastructure (CII) is defined as a computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety.

Cyber Crime - Cyber crime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes).

Cyber crimes range from basic crimes such as online harassment to calculated attacks such as fraud and financial crimes. A few broad categories of attacks are as follows:

- **Fraud and Financial Crimes:** Computer fraud is any dishonest misrepresentation of fact intended to let another to do or refrain from doing something which causes loss.
- **Cyber terrorism:** Any act of terrorism committed through the use of cyber space or computer resources can be categorized as cyber terrorism.
- **Cyber extortion:** Cyber extortion occurs when a website, e-mail server, or computer system is subjected to or threatened with repeated denial of service or other attacks by malicious hackers, who demand money in return for stopping the attacks and for offering protection.
- **Obscene or offensive content:** Delivering obscene and offensive content to users through the use of cyberspace or computer resources is considered an offense in many countries across the globe. The extent to which these communications are unlawful vary greatly based on the nation.
- **Cyber harassment:** Any form of harassment, such as directing obscenities and derogatory comments at specific individuals, committed through the use of computer resources can be categorized as cyber harassment.



LEGAL AND REGULATORY FRAMEWORK

I. CYBER LAW AND RELATED LEGISLATION

The objective of the legislative framework is to address specific legislation governing cyberspace activity through various collaborative initiatives

Collaboration to Establish Robust Legal Framework

The State shall collaborate with NALSAR, legal experts in the area of cyber security, The Hague Security Delta, Cyber Cell, TIPCU etc. to study the existing legal frameworks, identify problems and formulate advocacy laws to tackle real-time issues faced by these entities. This collaborative effort will be given the needed impetus to counter the ever evolving nature of cyber threats.

Non-Cyber Specific Legislation that may be relevant to regulate cyberspace activity whenever applicable such as protection of (a) copyrights (b) defamation (c) national security/sedition (d) anonymity etc. will also be addressed to protect information flow on the internet.Telangana has already established Telangana Intellectual Property Crime Unit (TIPCU) to bolster its efforts against Intellectual Property crime and piracy.

II. CYBER CRIME CELL

Cyber Grievance Redressal Efforts

The State of Telangana has a specialized Cyber Crime Cell for investigating into complaints pertaining to offences under the Information Technology Act. The Cyber Crime cell is headed by the Assistant Commissioner of Police, supported by a team of 4 Inspectors. The government shall further strengthen this unit to simplify reporting, tackling and tracking progress on cyber crimes. This unit will be empowered address issues pertaining to child pornography, woman harassment, etc.

Efforts against Pornography, Cyber Bullying, and Sexual Harassment

The State will strive to create a cyber space free of pornography, especially child pornography, cyber bullying, and sexual harassment. The cyber grievance system will be put in place to lay special emphasis on these crimes.

III. CYBER FORENSICS

The State will establish a digital forensics lab to analyze and investigate cybercrime to assist in the recovery and preservation of digital evidence. A data recovery lab will be established to recover corrupted and deleted data that are not available for intended use as a result of cyber crime. In line with capacity building efforts, there will be a provision for developing data experts who can handle forensic and related requirements. A digital evidence preservation facility will also be created to have a secure environment for retention of digital evidence.

COMPLIANCE AND ENFORCEMENT FRAMEWORK

I. PROTECTION OF CII

Risk-based Approach in Protecting Critical Information Infrastructure (CII)

Absolute security exists only as a concept but cannot be achieved practically, irrespective of the amount of resources focused on it. Hence, a risk-based approach, where response is prioritized based on the risk it poses, is the way forward. The Government shall formulate a Critical Information Infrastructure Protection Plan in collaboration with the private sector and by adopting a risk-based analysis approach.

Think Tank for Policy and Decision Inputs

To facilitate cooperation and collaboration against cyber threats at the highest level, the government shall create a think tank comprising of relevant stakeholders for policy and decision inputs.

II. EMERGENCY RESPONSE

Apex Agency for State-wide Coordination

The government shall set up T-CERT, a nodal agency for the state to coordinate with institutions, organizations and companies. T-CERT will contribute towards the State's efforts for a safer, stronger Internet for all citizens by responding to major incidents, analyzing threats, and exchanging critical cyber security information with trusted partners.

The primary mandate of T-CERT would be to:

- Provide cyber security related actionable information to the Government, critical infrastructure agencies, private industries and general public through advisories
- Provide cyber security protection through intrusion detection and prevention capabilities
- Develop state's crisis management plan and implement the same in coordination with CERT-In, offering the following services to critical infrastructure clients
- Assist the State in collaborative efforts to improve the cyber security posture of the State
- Initiate proactive measures to increase awareness and understanding of information security and computer security issues
- Act as a nodal agency to conduct security audits or assessments of government and constituent IT infrastructure in the state, evolving security policy for the state

A dedicated officer at the nodal agency shall coordinate with stakeholders and drive the State's efforts. Further, a round the clock support facility will be established for emergency response and crisis management. Through a network of dedicated officers in every department, the support team shall continuously monitor the cyber situation in the State.

Business Continuity

Understanding the importance of business continuity in case of an incident, accident, or disaster, the Government shall mandate an agency to develop a business continuity plan. In addition, Telangana shall strive to ensure a culture of issuing and procuring cyber insurance.

III. STANDARDS AND PRACTICES

Information Sharing and Analysis Centre

Through partnerships with private players, the government shall create the requisite infrastructure, and set up an Information Sharing and Analysis Center to share actionable information, develop capabilities, and analyze trends to identify latest opportunities and threats. These will include among others:

- Development and implementation of Information Security Standards
- Develop Information Security Guidelines and Best Practices
- Joint development of a State Cyber Crisis Management Plan to protect state information assets and critical infrastructure

Promotion of Open Standards

To ensure high levels of transparency and collaboration at various levels, the government shall promote use of open standards and data exchange.

Procurement of Safe ICT Products by the State

Weak ICT products will increase vulnerability of our information systems to external attacks and data leaks. The Government shall contact industry experts to frame guidelines for procurement of trustworthy products by the State.

IV. ISMS IMPLEMENTATION

The Government shall encourage the implementation of ISMS across organizations in the state. The Government will also explore the potential of having its own ISMS initiative to help local small and medium scale industries. This will be focused on the practical governance and organizational issues of securing information systems considering business and organizational challenges, and not address it merely as a technology problem.

V. ICT SECURITY CERTIFICATION

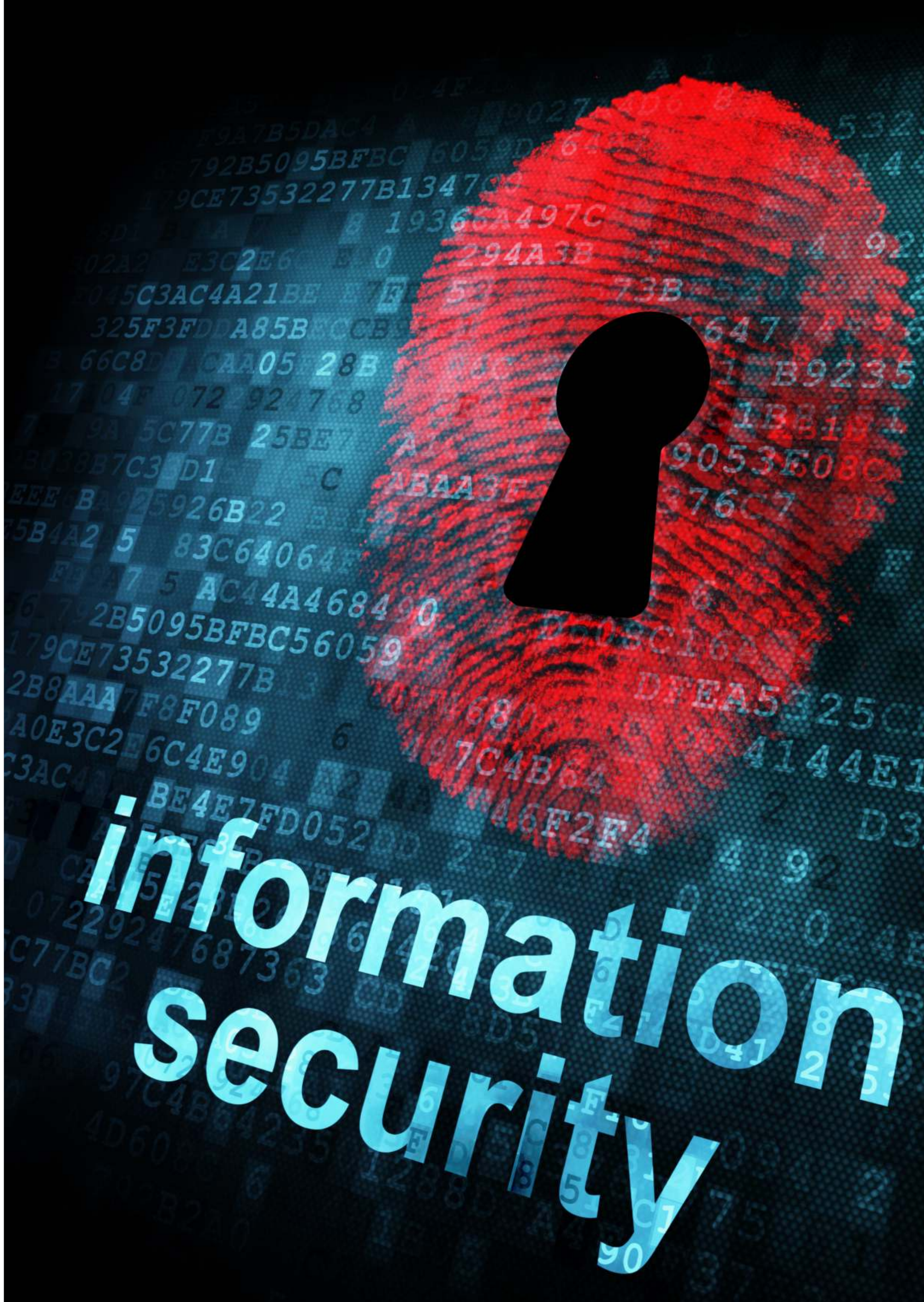
Certification of Cyber Security Products and Services

The Government shall establish Telangana State ICT Security Assessment Facility where product certifications and compliance assessment of all sensitive ICT products linked directly or indirectly to CII will be done. The facility will provide among other services

- Vulnerability Assessment and Penetration Testing Services for critical infrastructure sectors Security Assessment for control systems (SCADA/DCS)
- ICT Product Security Assessment and Certification service
- Common Criteria (CC) evaluation service and Protection Profiling

The Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria or CC) is an international standard (ISO/IEC 15408) for computer security certification. Common Criteria will be used as the basis for Government driven certification scheme and product testing and evaluations that will be conducted for Government agencies and critical infrastructure.

The Government shall also introduce security kite-marks to help individuals and companies identify trusted cyber security products for procurement at any level. Certifications for all cyber security products and critical ICT products will be made mandatory.



CAPACITY BUILDING AND CYBERSECURE ACCULTURATION FRAMEWORK

I. INFORMATION SECURITY WORKFORCE CAPACITY BUILDING

The government shall encourage, develop or impart training to increase cyber security awareness at all levels. The government will lay impetus on building a strong workforce of auditors, policy implementers, data management experts, forensic personnel to provide cybersecurity related services. This will also include creating a pool of penetration testers and cyber security experts who can provide advisory services to the government and statewide enterprises.

Certification Programs through TASK

The State shall develop certification programs through TASK and collaborate with academic institutions to encourage students to sign up for these programs. Additionally, TASK already provides recruitment assistance to the private sector, which will significantly reduce on-boarding costs for employers.

Collaboration with Academic and Research Institutions

The State shall set up Centers of Excellence (CoE) in association with a college of higher education to boost research in specific areas of cyber security. The State shall also launch specific R&D projects relevant to current day challenges that the Government faces, which will be addressed through these centers

The Government shall perform a comprehensive revamping of the curriculum in place for Master's Degree in cyber security domain. Specialized degree and diploma programs catering to various aspects such as auditing, forensics, data management will be launched.

In addition, the State shall enter into partnerships with leading institutions around the country by identifying win-win situations for furthering its interests in cyber security.Special scholarships shall be set up for students pursuing advanced academic degrees in cyber security fields.

Cyber Warriors

The State shall create a pool of 'cyber warriors' trained in cyber security, to work as part-time security consultants with the Government, advising the Government in procuring ICT and cyber security products, simulating cyber-attacks to help find security loopholes, and assisting T-CERT on ground in case of a cyber-security incident.

Customized Training Programs

The Government shall collaborate with the private sector to provide customized training programs for Police and Government Departments, PSUs, Banks, and other key Industries which are associated with critical infrastructure.

II. CYBER SECURITY ACCULTURATION

Multi-Channel Awareness Campaign

The government shall launch a state-wide multi-channel awareness campaign involving workshops, social, print and digital media etc. to create cyber security awareness among its citizens.

School Level Cyber Security Education

Having identified that cyber security is an important aspect of digital education, Telangana will modify curriculum for high schools to include aspects of cyber security relevant to children. This will be deployed along with the School Computer Literacy Program. The government will also launch a program that will be accessible to all children to deal with issues such as cyber bullying, cyber etiquette, identify theft, privacy etc.As more and more human interaction is being shifted online, the importance of good and acceptable behavior online shall be outlined and paralleled with that of offline behavior.

Guidelines for Safe Practices

By collaborating with the private sector, the State shall issue live document guidelines on best practices to help citizens and organizations stay aware of the latest developments in cybercrime and address them proactively

Cyber Security Challenge

The Government shall announce an annual competition, named the Cyber Security Challenge, which will help identify and nurture individual talent. This will be a statewide drive to increase awareness as well as build assurance in the community about government initiatives and efforts to secure the cyberspace with the help of its stakeholders. This challenge will have different levels of complexity to appeal to personnel of varying levels of cybersecurity skills and competency.

BUSINESS DEVELOPMENT FRAMEWORK

I. PROMOTE LOCAL CYBER SECURITY INDUSTRY

Dedicated Incubator for Cyber Security Startups

The Government of Telangana has launched T-Hub with a vision to boost the start-up ecosystem in the state. Under this umbrella, a dedicated incubator will be set up for cyber security related start-ups. The state shall also develop a venture capital model to provide assistance to first generation entrepreneurs, start-ups and SMEs operating in this field.

Annual Cyber Security Expo

The State shall conduct an Annual Cyber Security Expo to showcase the advantages of the State, primarilyindigenously developed products by SMEs and Startups. This will also ensure a platform for cyber security enthusiasts to interact and discuss the latest developments across the globe.

Promoting SMEs in Cyber Security

The Government shall award a certain number of cyber security contracts each year to SMEs incorporated in Telangana and devise a mechanism to ensure transparency in the allotment procedure. In addition, a separate area in the proposed SME towers will be earmarked for SMEs incorporated in Telangana operating in this area.

Fiscal and Non-Fiscal Incentives

To boost the local industry, special fiscal and non-fiscal incentives will be given to firms operating in Telangana as outlined in Appendix I.

II. STRATEGIC PARTNERSHIPS

Collaboration with Private Sector for R&D

In addition to collaborating with colleges for R&D projects, the State shall outsource relevant R&D projects of the Government to corporates incorporated in Telangana. Startups incorporated in Telangana will be provided access to Government Applications to showcase their product as proof of concept (PoC). These projects can be converted into full-scale Government contracts post performance reviews.

Partnering with Service Providers

To ensure safety at the supply end, the government shall work with ISPs to help individuals assess the existing security levels to protect them from future attacks. Further, to avoid fraudulent practices and identify service users, the government shall take up personal identity assurance and other measures.

Partnering with Private Sector

In addition, the Government will enter into strategic partnerships with the private sector to set up infrastructure such as cyber security training and development labs, which in turn will facilitate the development of new products.

Partnerships with International Agencies

Numerous international institutions and agencies, such as Israel National Cyber Bureau and The Hague Security Delta, have already established a name for themselves at the global level. Telangana shall strive to enter into strategic alliances with such organizations to benefit from their infrastructure, skillset and research capabilities.

STAKEHOLDERS' RESPONSIBILITIES

The stakeholders involved, namely citizens and the private sector, must work together with the Government and act responsibly to realize the vision of a safe cyber space for one and all. Since the cyberspace comprises of networks, the adage 'the chain is only as strong as its weakest link' is apt, and this demands every entity to assume basic responsibilities to secure themselves from cyber threats.

Citizens

Citizens, forming the building blocks of the society, have a key role to play in protecting the cyberspace. A responsible citizen shall be encouraged to:

- Follow cyber hygiene while interacting in the cyberspace
- Be responsible for their own behavior in cyberspace
- Be aware of the ever changing threat landscape and adopt safety measures
- Learn to identify and report threats in a safe and timely manner
- Know how to protect themselves from basic cyber attacks

Private Sector

A major chunk of the cyberspace is run by the private sector. The innovation required to keep pace with security challenges is also driven by them. Hence, businesses shall be encouraged to assume basic responsibility and:

- Be accountable for the products and services they provide and provide adequate guidance for the users
- Adopt 'security by design' and 'privacy by design' principles into their standards
- Maintain transparency in their security and data-handling mechanisms
- Invest in training and capacity building to meet future cyber security needs

Partners

Telangana shall partner with various Institutions for driving various initiatives. The potential partners include academic and research institutions, private players, other Government organizations etc. These partners shall:

- Participate in information sharing efforts driven by the State
- Assist the State in promoting it at the global stage
- Assist the State in its research efforts
- Tie up with the State to deploy/test new products developed

Government

Being the primary stakeholder, the Government shall spearhead the efforts to engage with citizens and businesses to help them fulfill their roles. The Government shall:

- Protect critical information infrastructure
- Develop safe and secure e-Governance products, applications and services
- Protect sensitive citizen data
- Strengthen laws to effectively handle cyber crimes
- Facilitate the development of secure ICT products
- Advise public on safe practices to improve awareness
- Collaborate with the private sector to grow the cadre of cyber security professionals

APPENDIX I

Fiscal Incentives

Relevant incentives mentioned in the GO on Incentives for Expansion of IT/ITeS shall be applicable for cyber security firms.

In addition to the IT/ITeS and Innovation Policy, the following incentives shall be provided:

- **Server Space:** Rack Space shall be provided from the State Data Centres to cyber security start ups incorporated in Telangana at a subsidized cost.In addition, the option of subsidizing cost of server space leased through third party vendors shall also be explored.
- Promoting SMEs:
  - **Procurement:** Additional preference shall be given to SMEs in the field of cyber security for procurement of cyber security services by the Government. Separate guidelines will be issued for the same.
  - **Subsidy on Lease Rentals:** 25% Subsidy on Lease Rentals up to INR 500,000 per annum for a period of 3 years will also be provided
  - **Exhibitions Costs:** 50% exhibition stall rental cost or INR 50,000, whichever is lower, will be reimbursed for participating in the notified national/international exhibitions limited to 9 sq.mts. of space.
- Promoting Start ups:
  - **Financial Assistance as Matching Grants:** The Government would match the funding raised by the Incubator from Government of India on a 1:1 basis as matching grants.
  - **Recruitment Assistance:** To promote idea stage companies, the government shall offer recruitment assistance of INR 10,000 per employee for the first year.

- **R&D grants:** The Government of Telangana will facilitate to provide specific R&D grants to cyber security companies in tune of 10% of overall R&D expenses of the company's Telangana operations or 2% of annual turnover of company's Telangana operations or INR 500,000, whichever is lesser.
- **Internet Costs:** Cyber Security Start ups shall be provided 25% reimbursement on internet charges up to a maximum of INR 2,50,000 per year for the first three years of operation
- **Patent Filing Costs:** The cost of filing and processing a patent application will be reimbursed to cyber security start ups subject to a limit of INR 2,00,000 per Indian patent awarded and INR 10,00,000 for foreign patent awarded
- **Recruitment Assistance:** Recruitment Assistance will be provided to start ups, SMEs and large organizations as per GO on Incentives for Expansion of IT/ITeS Units.

For projects of strategic importance, a tailor-made package of incentives shall be designed

Below, are given the general incentives available to the ICT industry, automatically. The Cyber Security firms, by virtue of being IT units, are serving global customers on 24x7x365 basis. Therefore, this industry is regarded as an essential services enjoying benefits mentioned below:

a. Cyber Security firms are exempt from the purview of the Telangana Pollution Control Act, except in respect of IT parks/IT SEZ campuses with built up area over 20,000 sqm, special permissions need to be taken from SEIAA under MoEF.

b. Cyber Security firms are exempt from the purview of statutory power cuts.

c. Cyber Security firms are exempt from inspections under the following Acts and the Rules framed thereunder, barring inspections arising out of specific complaints. These units are permitted to file self-certificates, in the prescribed formats.

   - The Factories Act 1948.
   - The Maternity Benefit Act 1961.
   - The Telangana Shops & Establishments Act 1988.
   - The Contract Labour (Regulation & Abolition) Act 1970.
   - The Payment of Wages Act 1936.
   - The Minimum Wages Act 1948.
   - The Employment Exchanges (Compulsory Notification of Vacancies) Act 1959.

d. General permission for three shift operations with women working in the night

e. Cyber Security Firms are declared as essential service under TS Essential Services Maintenance Act.

CONCLUDING NOTE

Technology can be a great enabler for a new state like Telangana which can propel it to greater heights of achievement and prominence among other states and in the nation. Given its strong foundation and talent in IT and ITeS, the State of Telangana can emerge as the leading state in India when it comes to IT related products and services. The Government strongly believes that growth should be managed in order to be sustained and nurtured. It is in this light that the Government proposes a Cyber Security Policy to address the challenges that come with the use of technology and cyberspace.

Telangana has been making significant advances in positioning itself proactively as a truly digital State. The Digital Telangana initiative is a holistic approach to promote the use of ICT in all spheres of life and manage it in a healthy manner. The cyber world is a world without boundaries, where opportunities are endless and possibilities limitless. Therefore, one of the most crucial strategies of the Digital Telangana initiative is its cyber security strategy. To ensure that a truly secure digital environment is made available to all the stakeholders, a collaborative effort is required from the Government, corporates, institutions and citizens alike.

Telangana, being one of the pioneering states in technology and related fields, has decided to come out with the Cyber Security Policy to facilitate this collaboration and give the State a roadmap to establish itself as the global leader in cyber security and emerge as the leader in the technology domain.