CYBER SECURITY POLICY 2017

GOVERNMENT OF HARYANA

By
Haryana Information Security Management Office (ISMO)

PREAMBLE

The Cyberspace is complex environments with many fold increase in networks and devices connected to it and has become so integral to economic and national life that government, business and individual users are targets for ever more threatening and frequent attacks. The cyberspace of State depends on socio-political and technological domains with its unique characteristics, the balancing between fragmentation of Cyberspace and State sovereignty makes cyberspace governance quite complex.

The Haryana state government has been a key driver for increased adoption of IT-based products and IT enabled services in Public services (Government to Government (G to G) services, Government to Citizen (G to C) Services), Healthcare (telemedicine, remote consultation, and mobile clinics), Education (e- Learning, virtual classrooms, etc) and financial services (mobile banking/ payment gateways), etc. Such initiatives have enabled increased IT adoption in the state through sectorial reforms and adopt Digital India program which have led to creation of large scale IT infrastructure with corporate / private participation.

In the light of the growth of IT and Communication sector in the state as part of Digital India programme, ambitious plans for rapid social transformation & inclusive growth and Haryana State's prominent role in the IT global market, providing right kind of focus for creating secure computing environment and adequate trust & confidence in electronic transactions, software, services, devices and networks, has become one of the compelling priorities for both state and nation. Such a focus enables creation of a suitable cyber security eco-system in the state, in tune with national interest and globally networked environment.

Cyberspace is vulnerable to a wide variety of incidents and Large-scale cyber incidents (identity theft, phishing, social engineering, cyber terrorism, compound threats targeting mobile devices and smart phone, compromised digital certificates) may cause complications of a magnitude that may threaten lives, economy and national security. Rapid identification, information exchange, investigation and coordinated response and remediation can mitigate the damage caused by malicious cyberspace activity. The protection of information infrastructure and preservation of the confidentiality, integrity and availability of information in cyberspace is the essence of a secure cyber space.

To address the cyber security challenges various ongoing activities and programs of the Government have significantly contributed to the creation of a platform that is now capable of supporting and sustaining the efforts in securing the cyber space. Due to the dynamic nature of cyberspace, there is now a need for these actions to be unified under a State Cyber Security Policy Framework, as per National Cyber Security Policy with an integrated vision and a set of sustained & coordinated strategies for implementation.

The Haryana State Cyber Security Policy framework (HSCSPF) is an evolving framework and it caters to the whole spectrum of ICT users. It serves as an umbrella framework for defining and guiding the actions related to security of cyberspace. It also enables the individual sectors and organizations in designing appropriate cyber security policies to suit their needs. The policy provides an overview of what it takes to effectively protect ICT infrastructure, information, information systems & networks and also gives an insight into the Government's approach and strategy for protection of cyber space in the country. It also outlines some pointers to enable collaborative working of all key players in public & private to safeguard country's information and information systems. This policy, therefore, aims to create a cyber security framework, which leads to specific actions and programs to enhance the security posture of country's cyber space.

HARYANA STATE CYBER SECURITY POLICY FRAMEWORK

Cyberspace is an interdependent network of critical and non-critical national information infrastructures, convergence of interconnected information and communication resources through the use of information and communication technologies. Haryana

Purpose

The Haryana Cyber Security Policy to ensure about security policy with respect to information flow that:

- Critical IT/ICT information is protected from unauthorized access, use, disclosure, modification, and disposal, whether intentional or unintentional
- The confidentiality, integrity and availability of such information, whether acquired permanently or in transit, provided or created, are ensured at all times, as appropriate.
- Any security incidents and infringement of the Policy, actual or suspected reported are investigated by the designated Chief Information Security Officer and appropriate corrective and preventive action initiated
- Awareness programs on Information Security are available to all Employees and wherever applicable to third party viz. Subcontractors, Consultants, Vendors etc and regular training imparted to them
- Business Continuity Plan is maintained and tested
- All legal and contractual requirements with regard to information security are met wherever applicable
- The policy will be reviewed at periodic intervals to check for its effectiveness, changes in technology, legal and contractual requirements, and business efficiency.
- The designated Chief Information Security Officer is directly responsible for maintaining and for providing advice and guidance on the policy implementation. The Security Apex Forum is responsible for reviewing the policy according to the defined review process.
- All Managers and Heads of departments are directly responsible for implementing the policy within their business areas and adherence by their staff.

It is the responsibility of all employees to adhere to this policy and the Management has all rights to take action in case of its violation in accordance with defined process. The Management commits itself to supporting implementation and maintaining compliance.

VISION

To build and augment a secure and resilient cyberspace for citizens, businesses and Government of Haryana

MISSION

To determine, analyze, address and build capabilities to prevent and respond to cyber threats posed on Haryana State's information, Information Infrastructure in Cyber Space through a combination of institutional structures, people, processes, technology and cooperation.

OBJECTIVES

- To create a safe cyber society of Haryana state by generating adequate trust and confidence in IT/ICT/ Information process systems in Haryana cyberspace and thereby enhance adoption of secured IT and ICT infrastructure in all sectors of economy.
- To create a Cyber Security Policy Framework for design of security policies and promotions for enabling actions for compliance to national and international standards for strengthen the regulatory framework for ensuring safe cyber ecosystem or safe cyber society of Haryana
- To develop suitable indigenous security technologies by supporting research, solution oriented research, proof of concept, pilot developments and encouraging business growth for synchronizing with the emerging global digital economy / network society
- To enable visibility of the integrity of IT/ICT trusted products and services by establishing secured infrastructure for ensuring the Security / confidentiality of data and to protect privacy in information and communication infrastructure without unduly affecting public safety and National Security.
- To encourage wider usage of IT/ICT infrastructure by all entities including Government for trusted communication, transactions and authentication.
- To establish and create Haryana State CERT (HS-CERT) for obtaining strategic information regarding incidents, threats towards Haryana State IT/ICT infrastructure for creating incident response, crisis management through effective predictive, preventive, protective, response and recovery actions and support to protection and resilience of state IT/ICT and other critical infrastructures
- To support capacity building activities by enabling Education, Training and Awareness activities for creating skilled manpower and spreading cyber security awareness among public.
- To provide fiscal benefits to businesses in Haryana for adoption of standard security practices and processes
- To encourage the adoption of information security best practices by all entities and Stakeholders in the Government, public & private sector and citizens that are consistent with industry practice.
- To enable effective prevention, investigation and prosecution of cyber crime and enhancement of law enforcement capabilities through appropriate support to establish capacity building activities for LEAs
- To enhance global cooperation by promoting shared understanding and leveraging relationships by creating culture of cyber security and privacy enabling responsible user behavior and actions through an effective communication and promotion strategy for safer cyberspace of Haryana.

SECURING CYBERSPACE OF HARYANA

As part of establishing secured cyber space or society in Haryana state, there is a need to create a secure cyber ecosystem across all organizations including departments, institutes, and industry from both private and public in Haryana State

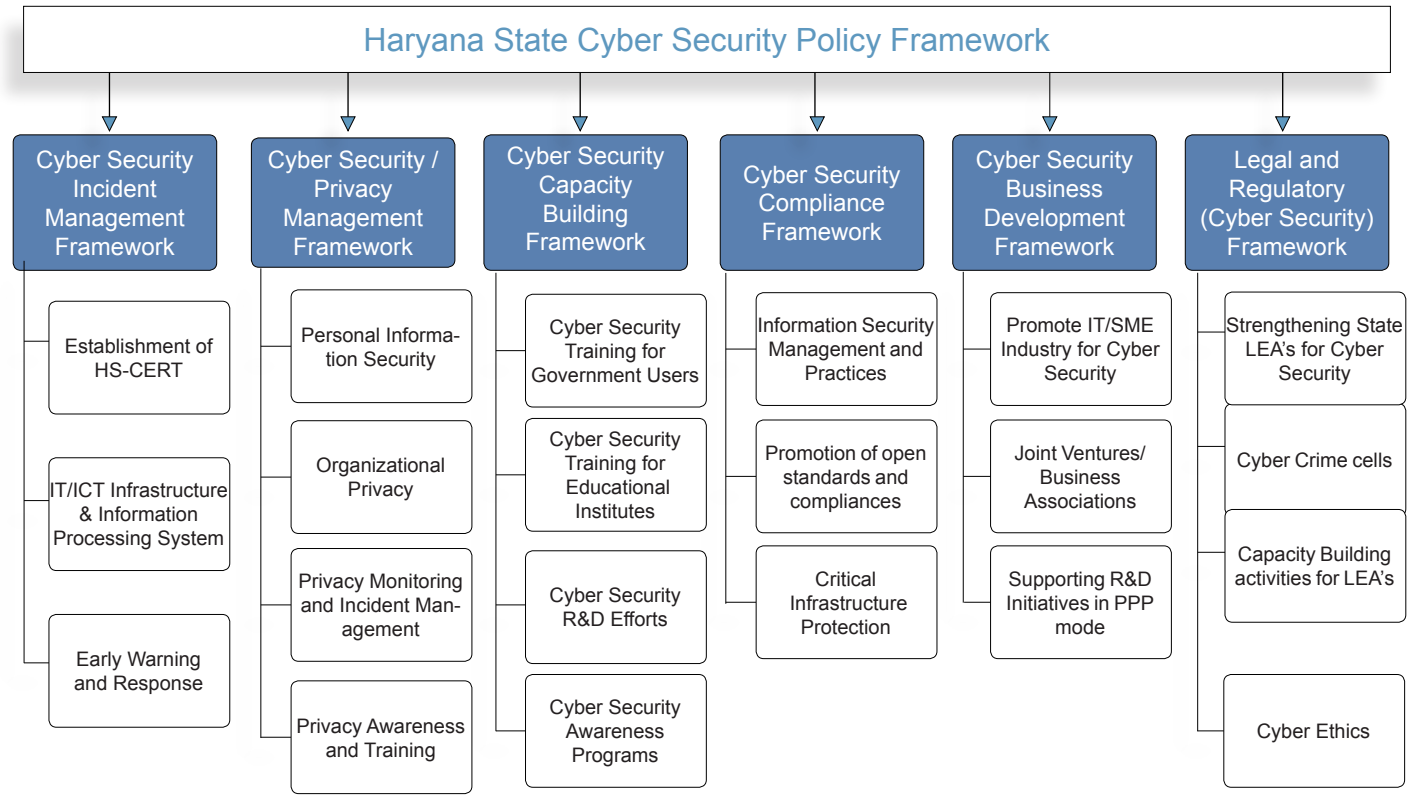
- To designate State nodal agency ISMO, E&IT Department for coordination of entire activities related to cyber security in the state of Haryana
- To encourage all organizations, private and public to designate a senior management member as state level chief information security officer (CISO) responsible for cyber security efforts and initiatives
- To encourage all stakeholders in the state including both internal and external, to interact with the cyberspace of Haryana to develop information security policies duly integrated with their business plans and implement such policies based on Haryana State Cyber Security Policy framework
- To ensure that all organizations earmark a specific budget other than IT Budget for implementing cyber security initiatives for encouraging to adopt guidelines, standards for procurement of trustworthy IT/ICT products and also supporting indigenously manufactured IT/ICT products that have security implications.

Creating Framework for Haryana State Cyber Security Policy

The Government of Haryana shall create a Haryana State Cyber Security Policy Framework (HSCSPF) with coordination of different departments under Government of Haryana and also by considering forum from private Industry and enterprises for better secured environment in Haryana State.
The Haryana State Cyber Security Policy Framework (HSCSPF) is a living document that will evolve with time and get enhanced with emergence of new technologies and, alongside new threats. It may include provisions for incident reporting and disclosure norms with respect to Cyber Security, to be adopted on a voluntary basis by all organizations dealing in IT.

The Government assures in building an enterprise security architecture/framework to design, develop a common platform to support all security services online (haryanaismo.gov.in) in an integrated platform for preventive, live, post analysis of security incidents which entails significant responsibility to all departments, system integrators and service providers to conform to the national and international standards to combat cyber attacks towards Haryana Government. The Government of Haryana shall coordinate with all the ISPs operating in the State to ensure that they establish and enforce appropriate cyber security plans in line with this policy framework.

The framework shall have the following objectives and features:



CYBER SECURITY INCIDENT MANAGEMENT FRAMEWORK

The purpose of the CIMF is to provide a consolidated whole approach to the management and coordination of potential or occurring cyber threats or incidents. It sets out the roles and responsibilities of all levels of government, critical infrastructure owners and operators and other public and private sector partners, in the coordinated prevention and mitigation of, preparedness for, response to and recovery from incidents affecting Haryana's portion of cyberspace. The CIMF is intended to enable each organization to fully and effectively participate in a coordinated national cyber incident response.

Protection of IT/ICT and Information System Processes in Haryana

- The Government of Haryana shall create an IT/ ICT, Information control systems Protection Plan in collaboration with the public, private sectors by adopting a risk based management approach for infrastructure protection.
- ISMO to serve as central point in the state for responding to cyber security incidents on occurrence and initiate proactive measures to increase awareness and understanding of cyber security issues for further report to CERT-In/I-CERT. ISMO shall create trustworthy in all ICT and Electronic environments in the state by implementing crisis management plan for the state.
- The detection of various incidents in live, post incident management and prevention and mitigation standards and practices needs to be implemented

Establishing Computer Emergency Response Team (HS-CERT)

The Government of Haryana shall establish Haryana State – Computer Emergency Response Team (HS-CERT) under ISMO, E&IT Department of Haryana state to coordinate with all organizations and Industry in both public and private in the state of Haryana for safer cyber society of Haryana. HS-CERT could function as sectoral CERT in support with Indian Computer Emergency Response Team (In-CERT) to respond to cyber security threats rapidly and effectively.

A dedicated Officer as Chief Information Security Officer (CISO) at state level shall coordinate Government, Organizations, Departments etc and Nodal agency/ ISMO for round the clock and shall continuously monitor the cyber situation of the state to support for emergency and response and crisis management system.

VA/ PT/ SOC Services:

Establishing a Security Operations Centre (SOC) as part of HS-CERT to act as a central point for identifying and correcting vulnerabilities in ICT systems through a reliable, trusted, 24-hour, single point of contact for emergencies.

As part of preventive maintenance and the security of applications hosted in Haryana state, shall be audited well in advance and conformity with CERT-In empanelment and international standards established before hosting in various data centres in Haryana.

To this effect, Government of Haryana designates a State nodal agency ISMO to coordinate all auditing activities related to cyber security auditing, penetration testing activities of all websites, applications and apps for in the state of Haryana. The nodal agency may become as regional CERT-In empanelment agency or associate with any CERT-In empanelled agency in Government to cater the needs of VA/PT services in Haryana

The Government of Haryana shall provide awareness, through a dedicated website/ portal for the stakeholders of Haryana with access to information on cyber threats, vulnerabilities in their systems and information on how to better protect them through *www.haryanaismo.gov.in*

Early Warning and Response System

Understanding of the importance of business continuity in case of incident, accident or disaster, the Government shall mandate ISMO, the nodal agency to design and develop a business continuity plan which needs to establish early warning and response system by establishing security operations centre (SOC) under HS-CERT for continuously monitoring the threats towards all government web sites and infrastructure.

- To facilitate cooperation and collaboration with all stake holders (ISPs, Departments, Organizations etc. of Haryana state) against cyber threats at highest level,
- To create cyber security forum with relevant stakeholders for policy
- CISO (Designated by state) shall coordinate forums of cyber security at highest level through establishing dedicated responsible members across respective departments by coordinating security efforts and incident response for cyber security issues at the state level and tune with the national and international norms.
- The HS-CERT shall also oversee the implementation of crisis management plan including cyber exercises and shall have collaborated with In-CERT and other supported organizations to operate cohesively towards the mission.

CYBER SECURITY PRIVACY MANAGEMENT FRAMEWORK

The State of Haryana empowers its security policy framework to succeed by integrating privacy protections from the outset. Privacy is also about public trust and confidence. It's about how the government acts responsibly and transparently in the way it collects, maintains, and uses personally identifiable information and employs a layered approach to privacy oversight for the state's cyber security activities.

Government also has a special responsibility to the citizen, Industry and organisations operating in the state of Haryana, and further to national and international allies & partners and able to assure them that every effort made has been to render our systems safe and to protect data and networks from cyber attacks or any other interference.

Personal Information Security

Individual data is of utmost important in terms of cyber security and individual privacy. The individual data includes information like name, date of birth, passwords, online account information, financial information, etc. Any data breach of an individual's financial account losing money or sending unwanted mails using identity theft from his personal account to harm others may have severe implications in both economical and public affairs.

Organizational Privacy

Designing and developing a security policy for an organization is essential to include about the privacy of individual, information and organization for avoiding information leakage where the basic information is initial source for attackers/ Cyber Criminals. The Haryana government insists all organizations shall clearly specify the objectives of various security controls and addresses the various security concerns for the privacy issues of employees, users, customers and information.

CYBER SECURITY CAPACITY BUILDING FRAMEWORK FOR HARYANA STATE

Cyberspace is an intrinsic part of the development of any state and a strong cyber capacity building is crucial for states to progress and develop in economic, political and social spheres. The rapid growth of and global access to ICT, combined with economic growth, has resulted in a great many first-time users in developing states in India. Capacity Building for managing the cyber security have to be built at various levels, considering the increasing sophistication of cyber threats and crime and the burgeoning size of user base of digital equipment and devices. The following steps shall be taken to address the capacity needs at various levels and in various areas of cyber security.

Capacity Building activities with respect to National requirements

The Government of Haryana ensures 6,000 Cyber Security professionals will be trained over the next 5 years in all sections – including 600 at Masters level, 4000 at the Graduate level, 1800 from among the employees of the State Government including LEAs by associating with Information Security Education and Awareness (ISEA) of Government of India and skill India programme. This program shall be formulated and implemented in close association with the ongoing Phase II of the ISEA (Information Security Education and Awareness) Program of the Ministry of Electronics and IT, Government of India.

Cyber Security Curriculums for Educational Institutes

The Haryana Government ensures in updating with Cyber Security curriculum in schools, colleges and Universities so as to provide education about cyber security among students by introducing courses of ISEA at graduate/ master graduate courses in state colleges/ universities and also recommend to all private institutes/ universities. Students to be encouraged to enroll recommended security certification courses from both state and central governments for all students from 10+2 onwards for better opportunities in cyber security. Faculty Advanced Training programs in Information Security to be introduced for faculty to mark them as Master trainers.

Cyber Security Awareness Programs in Haryana

The Government of Haryana shall take the following steps for enhancing the awareness amongst the citizen

- **By launching a citizen portal in association with www.haryana-ismo.gov.in in association with ISEA Phase-II program of Ministry of Electronics and Information Technology.**
- **Establishment of a Cyber Security Call Centre with a toll free number to support on security incidents**
- **To undertake an awareness campaign on cyber security through workshops, advertisements in print and electronic media and through short videos published on all frequently-visited web-sites**
- **A web-site www.hs-cert.gov.in can be initiated, for providing up-to-date advisories to the citizens and small business on safe practices while transacting online and to provide the registered members alerts on guarding against the anticipated threats.**
- **To launch awareness programs for all sections including LEAs, Government Users and General public.**
- **The Government shall promote holding of an Annual Conference on Cyber Security for all stakeholders in a PPP mode, to reinforce its commitment to cyber security and provide an impetus to the multiple initiatives in this area.**
- **Government of Haryana establishes an independent cyber security capacity building department under ISMO to coordinate for implementing Capacity Building activities by ensuring the safety and security of IT assets of the organization, along with ensuring the Safety and Security of data, controls, etc.**

The state CISO is the nodal officer to interact with department for feedback, trainings, and advisories, breach reporting etc. HR/ Training and Policy are responsible for manpower and their trainings etc. This group will also help in devising the IS policy specific to organization in coordination with the other groups.

R&D efforts for Cyber Security

The Government of Haryana to ensure the need for enhancing the efforts in R&D and innovation in this area and intends to establish a strong eco-system for Academia-Industry-Government collaboration.

- Establishment of Cyber Security Labs in different areas of cyber security and building a Cyber Range for suitable training of Government Officers and LEAs
- Secure Software Development initiatives for designing and developing various applications within IT department and other stakeholders of IT department shall be established with the motto “Secure by Design Program”
- Encourages all students of IT/ICT for the design and development of indigenous products as per national interest

CYBER SECURITY COMPLIANCE AND MANAGEMENT FRAMEWORK

The Government of Haryana shall encourage the implementation of standards and best practices of Information Security Management System as per national and International standards across all organizations in the state.

Information Security Management Practices

As part of their continuing efforts to establish effective information security management (ISM) practices, The nodal agency of Haryana state needs to design, develop, build and establish its own ISMS framework with available standards and guidelines for all organizations in state can be implemented to protect their assets.

This framework may be derived from the development of an a priori set of objectives and practices as suggested national and international standards by associating with cyber security forum of state, government and Academia

Promotion of open standards in Compliances

Information Security Compliance deals with the proper checks and balances for properly and effectively implementing the risk assessment and management model. This parameter also deals with the checks and balances for preventing any violation in implementing the model because the purpose for risk assessment and management will be defeated without proper compliance. The Government of Haryana ensures about various standards and compliances as based on business criticality as determined by the entity owner and nodal agency in all departments of state government and implements the respective standards, best practices and compliances.

Critical Infrastructure Protection

The Government of Haryana ensures about the inter section categorization is based on business criticality as determined by the entity owner. The underlying criticality of the CII is thereby determined based on the criticality of the supported business functions. This categorization is required as per IT Act 70 A and includes identification of all resources, assets (hardware and software) etc.

CYBER SECURITY BUSINESS DEVELOPMENT FRAMEWORK

As per the national security policy, importance is laid on design and development of indigenous products in national interest to secure cyber space of India. Government of Haryana assures to promote Haryana State as business destination for enhance activities of cyber security R&D in Government for indigenous products, encourage startups, SMEs and firms to design and develop security products for global requirements

Promote Local Cyber Security Industry

The Government of Haryana has an IT-Hub at Gurgaon and encourages the various start-ups, SMEs and other local bodies/Industry in the state and prepares for probable growth opportunities in cyber security industry for designing and developing information/ cyber security products in the state.

Government of Haryana shall ensure promoting local industry such as start-ups, SMEs by providing special incentives.

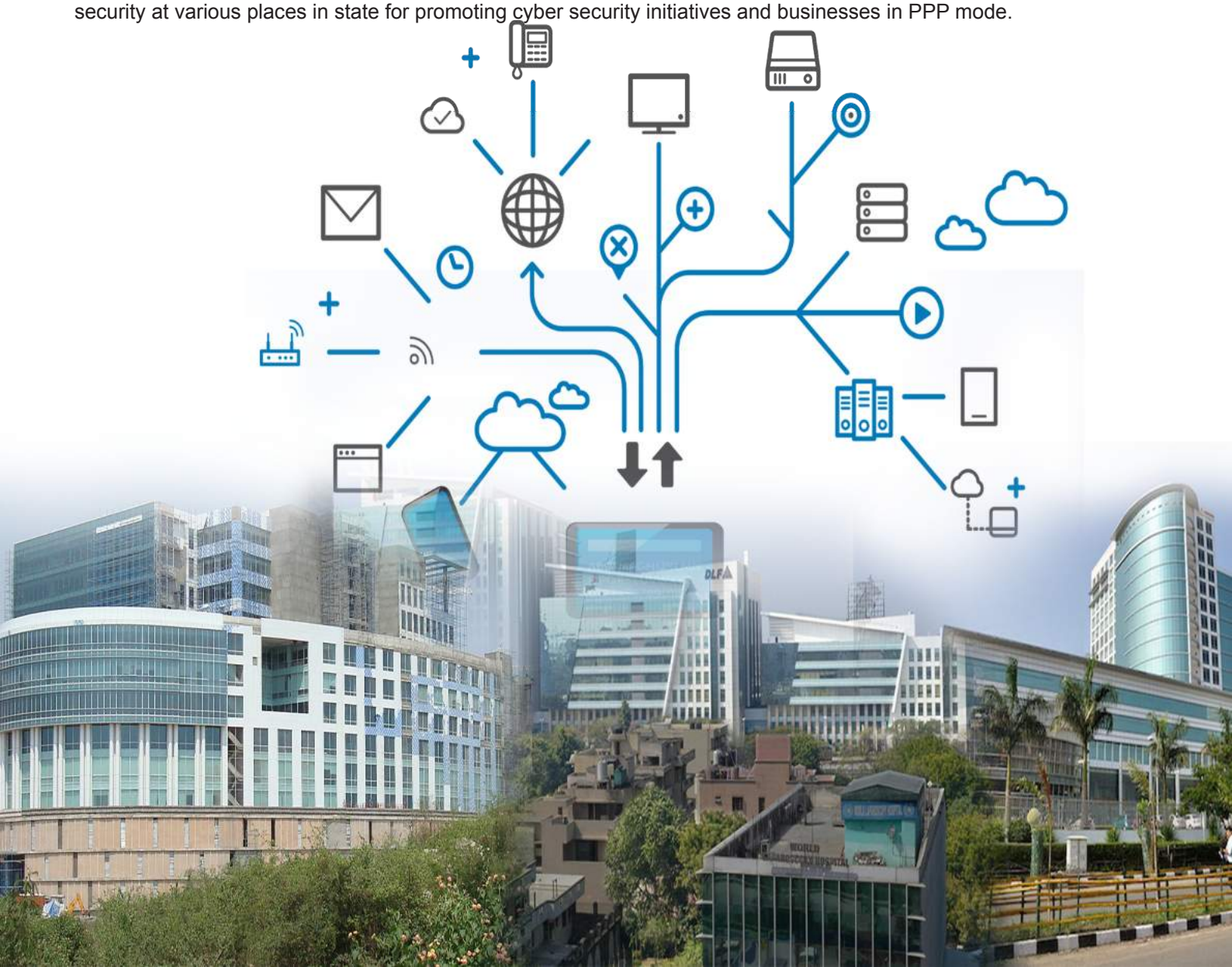
Joint Ventures /Alliances /Partnership for supporting R&D

Start-ups industries in Haryana 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.

Govt. of Haryana will encourage all existing IT/ITES companies already located in the state to expand and grow within the state, and also motivate and incentivize new companies to come and establish their units in the State.

Alliances with Private Sector and International Agencies

The Haryana Government assures strategic alliances by partnering with government organizations, Industry and International Agencies for integrating information security processes for various business processes in the state for safe and secured business architectures. Further, Haryana Government works on the possibility of establishing hubs in cyber security at various places in state for promoting cyber security initiatives and businesses in PPP mode.



LEGAL AND REGULATORY (CYBER SECURITY) FRAMEWORK

The Haryana Government is looking forward to address specific legislation governing cyber space activity for securing cyber space and control and counter cyber crimes by collaborating with various national and international agencies

The state collaborate with Digital Investigation Training and Analysis (DITAC) amd other available Legal expertise with respect to cyber security in the state to study existing frame works with respect to child, women security and privacy along with Cyber Security legal compliances. Further state needs to collaborate with non specific legislation of cyberspace such as copyrights, defamation, national security etc.

Strengthening State LEA's for Cyber Security

The Government of Haryana ensures to establish State Level Cyber Security investigation Lab for LEAs to combat various security crimes in the state of Haryana and the following initiatives shall be taken by the Law Enforcement Agencies in the State over a 5-year period:

- Establish digital, mobile, forensic labs along with social media analytical labs by associating the respective national agencies
- Police Officers of the rank of Sub-Inspector and above, shall be imparted training in Cyber security, through courses ranging from 2-weeks to 3-weeks, depending upon the needs of different categories of police functionaries, with focus on the areas of prevention, investigation and prosecution of cybercrimes.
- Since combating cybercrime is an ever-changing challenge, the training programs will be planned on a continuing basis and an appropriate institutional mechanism will be established for undertaking these training programs in a structured manner.
- The Law Enforcement agencies will be permitted to retain the services of Cyber Security Professionals in both private and public sectors, to assist and advise them in tackling organized crime and handling complex cases involving cyber forensics.
- Create master Trainer programs for both Police and judiciary Officers in cyber security who thereafter shall be posted in the security establishments of LEAs
- Cyber Police Stations and Basic Cyber Forensics Labs will be established in all the major cities of the State
- Police and judiciary Officers specializing in cyber security will be encouraged to participate in global conferences on cyber security and serve as Master Trainers to train subordinates in departments

Cyber Crime Cells

Haryana State assures in establishing Cyber crime cells to control and counter various cyber crimes in the state by establishing regional Cyber crime cells and state level cyber crime cell at nodal agency for both supporting investigation and capacity building activities.

Capacity Building Activities for LEAs

Haryana State shall ensure to establish a framework for training and awareness programs for Police, Judiciary and other LEAs by associating both private and Government organization or PPP mode to enhance skilled manpower in LEAs for cyber hygiene of Haryana state under Cyber Security Capacity Building Framework

The Government shall create a strategy among ISPs and Legal Enforcement Agencies (LEAs) to cooperate in data sharing for faster investigations in preventing Cyber Crimes

Authentication, Authorization and Accountancy Policy: The Government of Haryana shall put in place appropriate strategy mechanisms to prevent digital impersonation and identity theft and establish strong authentication, authorization and accounting mechanisms in all ICT online/ offline applications, systems, apps etc. as per national and international standards.

BUDGET ALLOCATIONS FOR VARIOUS FRAMEWORKS

Haryana State assures setting up of state level CERT named as Haryana State Computer Emergency Response System(Incident management framework) with an initial budget of Rs 27.65 Crore for the next 3 years.

Budget of Cyber Security Incident Management Framework

The Budget Allocations for Security over ICT: All departments, organizations, agencies in Government whomever implementing IT and ICT Projects shall earmark 10% of the annual IT Budget towards compliance as per IT Act 2000/2008, National Security Policy 2013 and this Policy framework, and with the security requirements to utilize the same for meeting the cost associated with the preparation and implementation of cyber security plans and Information Security Management System (ISMS); procuring products required to provide cyber security for the information and assets; conducting of training programs on cyber security and for conducting security audit of systems required under this policy.

The following budget is granted by Haryana for Cyber Security Incident management framework tentatively as below:
Government of Haryana (GoH) assuring for implementing Cyber Security includes under laws and forensics, for the following Activities:

- HS-CERT
- SOC As Service
- Incident Management and Forensics
- Capacity Building Activities/Training

- The state of Haryana is to ensure Fiscal Incentives for promoting Cyber Security Business opportunities in Haryana. Relevant incentives mentioned in the GO on Incentives for set up or Expansion of IT, ICT or IT enabled Services (ITeS) shall be applicable for cyber security firms.
- Establishing the Cyber Security firms, by virtue of being IT units, are serving global customers on 24x7x365 basis. Cyber Security firms are exempt from inspections under the following Acts and the Rules framed there under, barring inspections arising out of specific complaints.
- Additional preference shall be given to SMEs who would like to be part for cyber security related procurements and part of CERT-In empanelment services in the state. Separate guidelines will be issued for the same.
    - Subsidy on Lease Rentals: 30% Subsidy on Lease Rentals up to INR 600,000 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.
- Budget estimation to cater to the needs of cyber security capacity building activities
    - Academic (Teacher Training -Master Trainers)
    - Training (Certifications Scheme)
    - Awareness (Cyber Security Workshops)
- The Haryana Government allocates various budgets for cyber security privacy management and compliances and legal & Regulatory frameworks based on requirements of various critical IT/ICT and ITeS of Haryana Government agencies including departments, organizations etc.
    - Privacy Management:
      Government of Haryana encourages all agencies of Haryana Government to identify all activities, functions and operations attributed to the individual and organizational privacy and should be compliant to national and international standards. Further Government of Haryana recommends 5% of total budget for both privacy and security standards compliances.
    - Compliance Management:
      Government of Haryana insists all critical IT/ICT/ITeS infrastructures of Haryana Government need to comply with ISMS and other national/ International standards as per their business activities.
    - Legal and Regulatory Framework:
      Haryana State Government is planning to establish region based labs for legal and Forensic digital evidences to control the digital crime in state.

Haryana Information Security Management Office (ISMO)