Annexure-'X'.

CYBER SECURITY POLICY 2017

ELECTRONICS & INFORMATION TECHNOLOGY DEPARTMENT

GOVERNMENT OF HARYANA

1.0 PREAMBLE

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

The economic security of the state depends on the reliable functioning of critical infrastructure. Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the State's security, economy, and public safety and health at risk. Similar to financial and reputational risk, cybersecurity risk affects a business's bottom line. It can drive up costs and impact revenue. It can harm state enterprises ability to innovate and to gain and maintain business confidence.

The Haryana state government has been a key driver for increased adoption of IT-based products and IT enabled services in Public like 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 sectoral 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 and also 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 individual lives, economy of the state 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. Cybersecurity is a critical part of digital government with its broader external ecosystem and new challenges in an open digital world.

The scope of cybersecurity is expanding and becoming digital security. Safety becomes an issue with the intersection of technology and the physical world including Internet of Things [IoT]). The policy addresses the digital risks and digital adversaries that will continue to challenge government eco-system. It serves as an umbrella framework for defining and guiding the actions related to security of cyberspace

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 state's cyber space.

The key aspect of the policy is also to consider between now and 2025, a future where the government department and businesses Chief Information Security Officer (CISO), ISMO & ISOs will develop a evidence-based security practices and this will be a core capability of successful security and risk management programs. Evidence-based decisions will happen at the speed of intuition and will not in any way hamper the speed of digital businesses.

2.0 HARYANA STATE CYBER SECURITY POLICY FRAMEWORK (HSCSPF)

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.

2.1 Purpose

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

- 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 Chief Information Security Officer (CISO) by utilizing the resources of the ISMO and Designated Information Security officers bytaking appropriate corrective and preventive actions. The Chief Information Security Officer shall keep the Information Security Steering Committee (ISSC) updated from time to time.
- Awareness programs on Information Security needs to be 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 tested and maintained
- 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.

- Preparation of Cyber Crisis Management Plan (CCMP) in line with national cyber crisis management plan may be included and should be established cyber crisis management committee for responding to crisis situation
- 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 (or equivalent) is responsible for reviewing the policy according to the defined review process.
- The policy objectives represents about the need to protect and safeguard of all Government and Critical infrastructure applications for the state of Haryana.
- The policy will also be Measuring and Demonstrating Cybersecurity to discuss correlation of business results to cybersecurity risk management metrics and measures.

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.

This policy applies to all State Government Organizations (Departments, Boards, and Corporations), employees including full-time, part-time, and temporary employees, contractors, interns, volunteers, or any other individual who operates or has access to Haryana Government information or information systems.

2.2 Vision

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

2.3 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.

The mission is the foundation based on FOUR Pillars:

1. Building a Resilient Cyber Security Infrastructure
2. Creating a Safer Cyberspace for all in the State of Haryana
3. Developing a Vibrant Cybersecurity Eco-system
4. Building international partnership on cybersecurity

2.4 Objectives

"Cybersecurity" is a team effort, everyone has a part to play, and everyone has to play their part. The Government will take the lead to spearhead initiatives to enhance Haryana State's cybersecurity stance, and we will need everyone's cooperation to reap long term benefits for the cyber ecosystem. We aim to build a Smart State – one that will be enabled by trustworthy infrastructure and technology."

- To create a safe cyber society in 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 promotion 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 of information and communication infrastructure to ensure 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 is consistent with industry standards.
- 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
- Establish a Cybersecurity Fortification Initiative

3.0 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.

- To designate State nodal agency ISMO, E&IT Department for coordination of entire activities related to cyber security in the state of Haryana.
- A Chief Information Security Officer and ISMO shall be responsible for cyber security efforts and initiatives in the respective organizations by effectively utilizing the Infrastructure and resources in Haryana
- To encourage Departments, Districts, Boards/ Corporations and all other private and public organizations, to designatean officer as Information Security Officer (ISO) to coordinate with Chief Information Security Officer (CISO) & ISMO for cyber security efforts and initiatives in the respective organizations for securing infrastructure and management in state.
- 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 to adopt guidelines, standards for procurement

of trustworthy IT/ICT products and also supporting indigenously manufactured IT/ICT products security products.

- To encourage all individual stakeholders in the state by practicing cyber security practices to be part of cyber aware society of Haryana

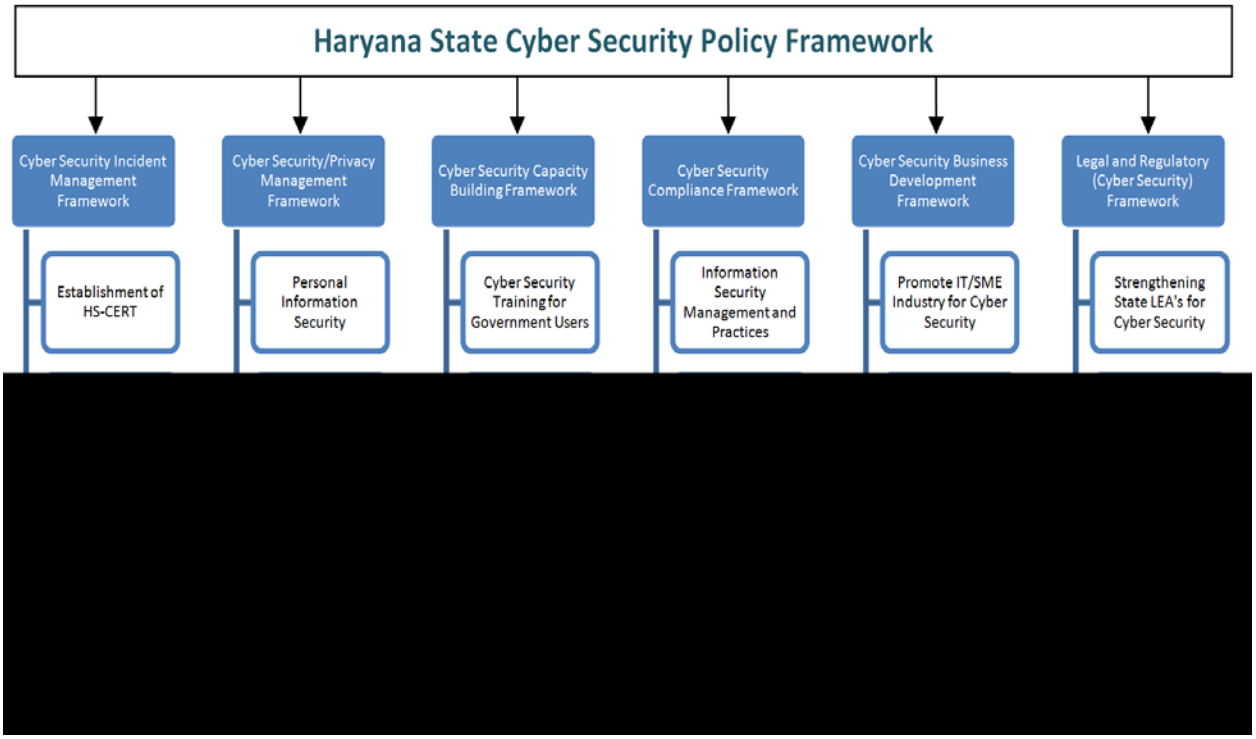
3.1 Creating Framework for Haryana State Cyber Security Policy

The Government of Haryana shall create a Haryana State Cyber Security Policy Framework (HSCSPF) with coordination with different departments under Government of Haryana and also from private Industry and enterprises by considering as forum 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 along side with an updated latest threat modelling. It includes provisions for incident reporting and disclosure norms with respect to Cyber Security, which needs to be adopted on a voluntary basis by all organizations dealing in IT/ICT infrastructure.

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:



4.0 CYBER SECURITY INCIDENT MANAGEMENT FRAMEWORK (CIMF)

The purpose of the CIMF is to provide a consolidated approach to the management and coordination of potential 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.

4.1 Establishing Responsible Owners for Haryana State – Computer Emergency Response Team (HS-CERT) and Chief Information Security Officer

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 shall function as sectorial CERT in support with Indian Computer Emergency Response Team (In-CERT) to respond to cyber security threats rapidly and effectively

An officer to be designated as Chief Information Security Officer (CISO) at state level shall coordinate with Government Organizations, Departments and Nodal agencies, etc. He shall be responsible for continuously monitor the cyber situation of the state to support for emergency and response and crisis management system utilising the resources of ISMO.

4.2 Protection of IT/ICT and Information System Processes in Haryana

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

To encourage all stakeholders in the state including both internal and external, to practice secured communications by using secure channels, whitelisting software, isolation of critical infrastructure etc.

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, thorough security audit will be done in advance with 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 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 to the needs of VA/PT services in Haryana. Being a nodal agency, ISMO may collect/obtain system logs for incident response/intrusion detection. ISMO may also scan Govt. IT infrastructure to find vulnerabilities for timely remediation.

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 systems and information on how to better protect them through www.haryanaismo.gov.in

4.3 Early Warning and Response System for IT/ICT and Information System Processes

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 updates and analysis.
- 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 collaborated with CERT-In and other supported organizations to operate cohesively towards achieve the mission.

5.0 CYBER SECURITY PRIVACY MANAGEMENT FRAMEWORK

The State of Haryana empowers its security policy framework to succeed by integrating privacy protections which implies public trust and confidence. The Framework defines 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 towards the citizens, 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 systems safety and to protect data and networks from cyber attacks or any other unauthorized interference.

5.1 Personal Information Security

Individual data is of utmost important in terms of cyber security and individual privacy. 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.

5.2 Organizational Privacy

Designing and developing a security policy for an organization is essential which include about the privacy of individual and organizations information to avoid 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 addressing the various security concerns for the privacy issues of employees, users, customers and information.

6.0 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 and global access to ICT, combined with economic growth, has resulted in creating 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 different areas of cyber security. ISMO envisages being CERT-In empanelled office/ entity by sufficiently building the in-house capacities and expertise.

6.1 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, 1400 from among theemployees of the State Government including LEAs by associating with Information Security Education and Awareness (ISEA), 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.

6.2 Cyber Security Curriculum for Educational Institutes

The Haryana Government ensures updating 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 pursuing 10+2 onwards shall be encouraged to enroll recommended for security certification courses from both state and central governments schools for better opportunities in cyber security. Faculty Advanced Training programs in Information Security to be introduced for faculty to mark them as Master trainers.

6.3 Cyber Security Awareness Programs in Haryana

The Government of Haryana shall take the following steps for enhancing the awareness among citizens

- By launching a citizen portal in association with www.haryanaismo.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 citizens 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 shall be initiated for Haryana State - CERT, 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 shall be the nodal officer to interact with department for feedback, trainings, and advisories, breach reporting etc by utilising the resources of the ISMO. 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.

6.4 R&D efforts for Cyber Security

The Government of Haryana ensures 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
- The R&D effort will be complemented by Cyber Intelligence Sharing Platform
- Cyber intelligence could be used by AIs to proactively strengthen their cyber resilience posture to better prepare for any potential cyber threats, and to take timely actions to strengthen the preventive, detective and recovery processes.
- To help improve the capability of AIs in cyber intelligence sharing and the Government will be working with global agencies to implement a cyber intelligence sharing platform.
- Relevant cyber intelligence sourced from different reliable channels will be collected, analyzed and shared on this platform together with detailed cyber-threat analysis report advisories and recommendations. Through this platform, all agencies and industry will be able to tap the latest threat scenarios and get prepared accordingly.

7.0 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.

7.1 Information Security Management Practices

As part of their continuous 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 to protect their assets.

This framework may be derived through the development of set of objectives and practices as suggested by national and international standards and also by associating with cyber security forums of state, government and Academia.

To encourage all stakeholders in the state including both internal and external to do initial risk assessment of all infrastructure before implementation.

7.2 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.

7.3 Critical Infrastructure Protection

All the identified critical assets/resources under various CIIs of the state of Haryana need to be gazette notified as "Protected System" under section 70 of IT Act 2000. Any attack on a "Protected System" with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people, shall be treated as Cyber Terrorism. (Section 66F of IT Act 2000). Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment, which may extend to imprisonment for life.

The Government of Haryana shall plan the establishment of **Cyber Crisis Management Plan (CCMP) as per international standard compliances** to reduce the risk of disruption and improve the security posture**.**

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.

8.0 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 in-house as well as global requirements.

8.1 Promote Local Cyber Security Industry

The Government of Haryana has an IT-Hub at Gurugram 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 as provisioned in the State policies applicable to IT/ ITES, ESDM, Start-up Industry.

8.2 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.

Government 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 provide incentives to new companies, Start-Ups to come and establish their units in the State.

8.3 Alliances with Private Sector and International Agencies

The Haryana Government assures strategic alliances by partnering with private 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.

8.4 International engagements

Strong international partnerships enable countries to deal with cybercrime more effectively.Haryana will actively foster regional and global cooperation, partner INTERPOL and other countries in capacity building initiatives, and bring global experts and thought leaders together to discuss the latest threats, trends and solutions in the cyber domain, and share best practices and solutions

(i) Fostering regional and global cooperation

Haryana is at the forefront of working with foreign countries to enhance our operational cooperation against cybercrime. At the ASEAN regional level, Haryana will participate with ASEAN that provides a platform for the ASEAN Member States (AMS) to coordinate the regional approach to cybercrime, and work together on capacity building, training and the sharing of information.

At the international level, Haryana will participate at the INTERPOL Global Complex for Innovation (IGCI), INTERPOL's global hub on cybercrime. Haryana will leverage INTERPOL's resources to strengthen our global operational networks and build new capabilities to tackle cybercrime.

ii) Building capacities and capabilities through collaboration at the regional, National and global levels

Haryana will roll out programs with partner countries and INTERPOL. The involvement of key Asian partners, AMS and INTERPOL facilitates a conducive environment for collaboration on cybercrime issues and sharing of best practices, and forging of effective operational links between countries and across the regions.

(iii) Bringing global experts and thought leaders together

Government of Haryana will be supporting thought leadership platforms that bring together public sector and industry partners on cybercrime.

9.0 LEGAL AND REGULATORY (CYBER SECURITY) FRAMEWORK

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

The state collaborate with Digital Investigation Training and Analysis (DITAC) and 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 will collaborate with non specific legislation of cyberspace such as copyrights, defamation, national security etc.

9.1 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 in 3 years:

- Establish digital, mobile, forensic labs along with social media analytical labs by associating with 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 continuous 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

9.2 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.

9.3 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, applications/apps etc. as per national and international standards.

10.0 IMPLEMENTATION OF HSCS POLICY FRAMEWORK

The Implementation of the HSCS policy framework shall be the responsibility of the State E&IT Department, Government of Haryana. The Nodal office for the implementation shall be the ISMO headed by CISO which shall be working in close coordination with all the Stakeholders (internal, Inter Department and other agencies of Government of India like CERT IN, NCIIPC, MeitY, etc.

10.1 Implementation of Cyber Security Incident Management Framework of Haryana State:

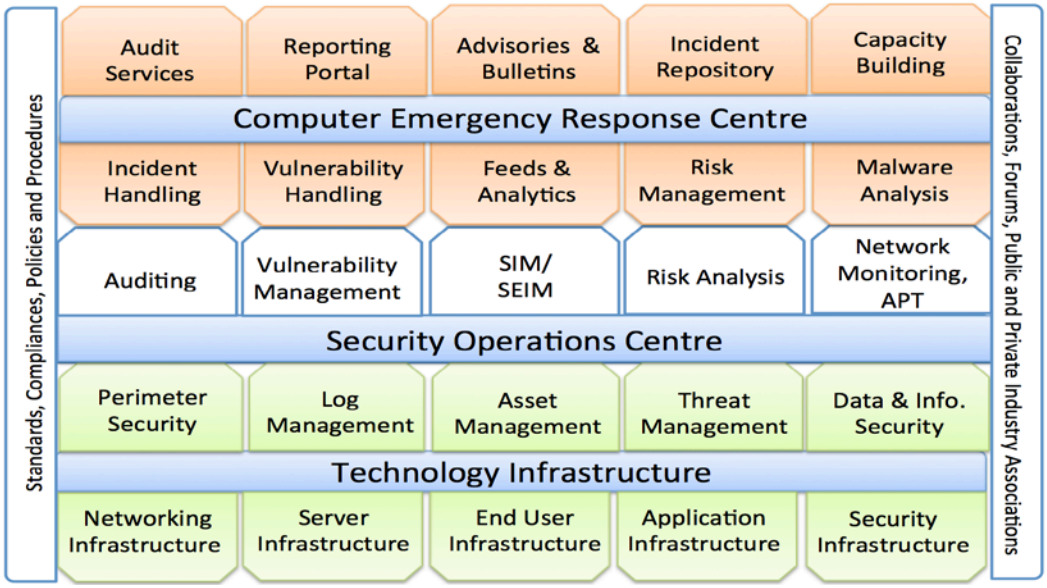
Haryana State CERT (HS-CERT) is setup with an objective to respond to incidents towards IT/ICT infrastructure of Haryana and also provides the necessary services to government departments, public sector undertakings, critical infrastructures, corporate and business institutions and other institutions in Haryana to handle security incidents and also helps to recover such incidents. HS-CERT will also act as extended arm of CERT-In, Government of India for the purpose of coordination and responding emerging threats.

Key Objectives of HS-CERT are:

- Incident response including coordination, resolution, recovery & subsequent prevention of incidents and respective attacks
- Audit, Vulnerability Assessment and Penetration Testing Services
- Security Operations Centre at State Data Centre
- Establishing Cyber Crisis Management Plan (CCMP) in line with National Crisis Management Plan
- Design and Development of threat intelligence of Haryana state infrastructures by collecting respective data, data aggregation for threat information, correlation and dissemination of actionable intelligence.
- Security Advisory Services
- Education, Training & Awareness and Capacity Building
- Coordination with CERT-In and other organizations to handle security incidents for providing advisories to citizens of Haryana and public, private entities including OEMs
- Incident Detection, Analysis and Response with a database of reported cyber security incidents for constituents
- Security Operations and Analytics for all IT/ICT infrastructure
- Monitoring Cyber Security Posture and reports deficiencies and providing regular reporting to authorities, IT Security officials and cyber incident responders
- Providing alerts and notifications to general and specific threats
- Capacity building activities
- Academic and Industry connect through by conducting security forums, annual workshops

Architecture of Cyber Security Incident Management Framework

The following architecture shows about high level diagram of cyber security incident framework that will be performed by HS-CERT and list of indicative activities which will be provided as part of framework



Implementation of Security Operations Centre for State Data Centre

Security Operations Centre "SOC" is required to be established for monitoring internal and external threats to the HS-CERT organization and will provide the required protection.

- Infrastructure Security including perimeter/boundary protection
- End Point Protection including desktops/mobiles/ end point applications
- Internal Vulnerability Assessment and Penetration Testing environment
- Internal threat management
- Forensic Team
- Data and application analysis for protection through logging mechanisms
- Deployment of infrastructure with Tools and Techniques

Security Advisory Services

One of key component of CERT activities are creating alerts, warnings and announcements to send them out to all stakeholders as part of dissemination along with synthesis, summarization and redistribution of threat intelligence reports and news related information security to all participating members. Potential stakeholders are:

- Departments/organizations
- Law enforcement / Polices
- Customers/Constituents

Dissemination channels which will be actively used by CERT will include

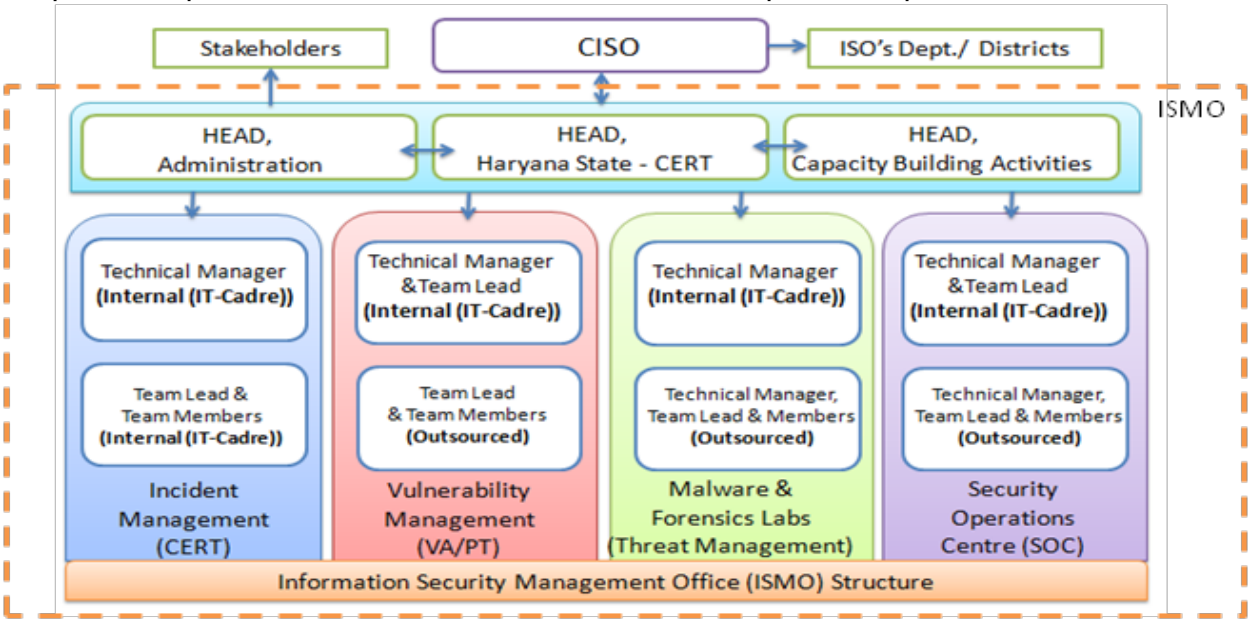
- Web site
- Service Desk Support/Telephonic
- Mailing lists
- Social Media

Education, Training and Awareness

As part of HS-CERT program, it is one of main function is to train members of CERT as per their functional activity and also train the respective members of various government department who would be part of information security for both functional and dissemination programs

- To train members of technical and administration teams at HS-CERT
- To train master trainers to disseminate education, training and awareness program for all stakeholders

Manpower Requirements: Technical and Administrative Expertise required is as under:



In the above organogram, It is suggested to allocate members dedicatedly towards Incident Management, vulnerability management, threat management and SOC services, The

heads and leads can be taken from the IT Cadre or if not found suitable then recruited directly as part of ISMO and where suitable technical team members can be considered from Out Source/ Third Party members. Industry expertise can be considered as short services/consultancy basis by ISMO as continuous forum of experts to support various activities of HS-CERT.

Roles and Responsibilities:

#	Role	Responsibilities	Experience	Additional Requirements
1.	CISO	Overall head of ISMO, interface with State Government Departments & Districts, Centre Government Agencies (CERT IN, NCIIPC, Meity, etc) and other collaboration with respect to cyber security issues in State	18+ years experience in information technology	Govt Appointed
2.	Head - HS CERT	Would be overall in-charge for Haryana State CERT activities Coordination with National CERT and Global CERTs Coordinate day to day work of infrastructure and technology operations and decide how to act in problems in situations Ensures seamless CERT technology operations and provide confidentiality, integrity and availability data Propose improvements for technology infrastructure & Maintain management and operations of IT infrastructure	15+ years experience in information technology related exposure and last 5 years in information security specifically in management	Should have experience in leading 20-25 security experts Advanced IT operations & technical knowledge communication and PR skills Strong analytic Skills Appropriate Certification/s
3	Head – Administration (based on requirements)	Would be overall in-charge for dissemination of reports/ advisories for all stakeholders including administration of HR, FINANCE and purchase activities of HS-CERT Ensures efficient operations of facility and support functions Maintain management and operations of support functions and organized periodic meetings for discussions about support functions	15+ years experience in the areas of administration in IT/ ITES Industry	Experience /exposure in finance and HR/Purchase activities
4	Head –Capacity Building Activities (based on requirements)	Would be overall in-charge for capacity building activities in state in terms of Information security activities	15 + years experience in education, training activities	Exposure in designing and developing courseware in IT/ITES courseware
5	Technical Manager –	Would be overall in-charge for Incident management activities for state and	10-12 years experience in	Preferably certification in

	Incident Management	lead & govern the entire program	managing security incidents	incident management
6	Team Lead – Incident Management	Would provide expert guidance to the team members for continuous support to HS-CERT activities	8-10 years experience in managing security incidents	Relevant certification
7	Technical Manager – Threat Intelligence	Would be overall in-charge for Malware reverse engineering/analysis and threat intelligence management activities for state and lead & govern the entire program	10-12 years experience in managing security incidents	Preferably certification in incident management
8	Team Lead – Threat Intelligence and Malware Reverse Engg.	Would provide expert guidance to the team members of Malware reverse engineering/analysis and threat intelligence management for continuous support to HS-CERT activities	8-10 years experience in managing security incidents	Relevant certification
9	Technical Manager – VA/PT Services	Would be overall in-charge for VA/PT Services and management activities for state and lead & govern the entire program	10-12 years experience in managing security incidents	Preferably certification in incident management
10	Team Lead – VA/PT Services Reverse Engg.	Would provide expert guidance to the team members of VA/PT Services and management activities for continuous support to HS-CERT activities	8-10 years experience in managing security incidents	Relevant certification
11	Technical Manager – SOC Services	Would be overall in-charge for SOC Services where we can integrate both VA/PT and Threat intelligences for state and lead & govern the entire program	10-12 years experience in managing security incidents	Preferably certification in incident management
12	Team Lead – SOC Services	Would provide expert guidance to the team members of SOC Services where we can integrate both VA/PT and Threat intelligences to HS-CERT activities	8-10 years experience in managing security incidents	Relevant certification
13	Team Member-HS-CERT/ SOC/ VAPT / Threat Intelligences (4 members each)	The member would be having experience in design and development capabilities in the areas of incident management/ VA/ PT/ Malware Reverse Engineering / SOC Services/ Capacity Building in Information Security	2-5 years relevant experience with strong network management/ log management / security programming skills as per job function	Relevant Certifications

The following Software/ Hardware infrastructure would be implemented as part of Cyber Security Incident Management Framework :

- SIM/SIEM Solution
- DLP/DRM Tool
- Net Flow/ Network Analysis Tools
- Honey Pots
- Vulnerability & Penetration Testing Tools
- Firewall/ Proxies/WAFs & IDS/IPS
- Identity Management & Inventory Tools
- Threat Intelligence Tools
- Security Analytics Tools
- DDOS protection Tools
- Threat Assessment Tools
- End Point Product Testing Tools
- Forensic imaging and Analysis Tools
- Network Telescopic and Encryption Tools
- Hardware Infrastructure like Server Farm, Network Infrastructure
- Malware Isolation technologies/ tools

The Budget allocations for security over ICT: All departments, organizations, agencies in Government who ever 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.

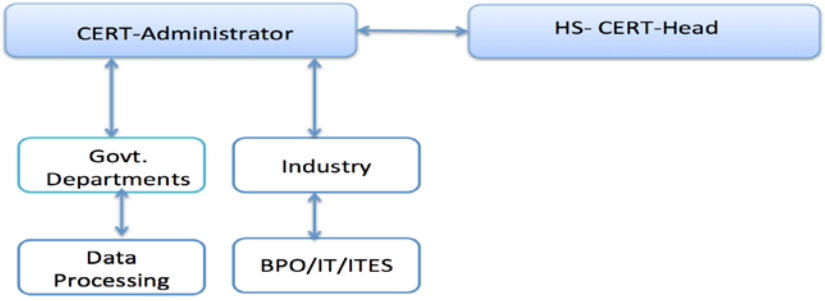
Government of Haryana (GoH) assuring for implementing Cyber Security includes under laws and forensics, for the following Activities:

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

It is also understood that suitable manpower/ resources (infra/ software) may not be available initially with ISMO for successfully implementation of HSCS Policy Framework however, the same shall be built in due course time to slowly move towards building capacity in-house. Meanwhile, the specialised resources & expertise in order to successfully implement the HSCS Policy Framework may be taken on outsources model with Third Party agencies from Govt / Private on need basis.

10.2 Implementation of Cyber Security Privacy Management Framework

The State of Haryana empowers its security policy framework to succeed by integrating privacy protections which implies public trust and confidence. The Framework defines 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.



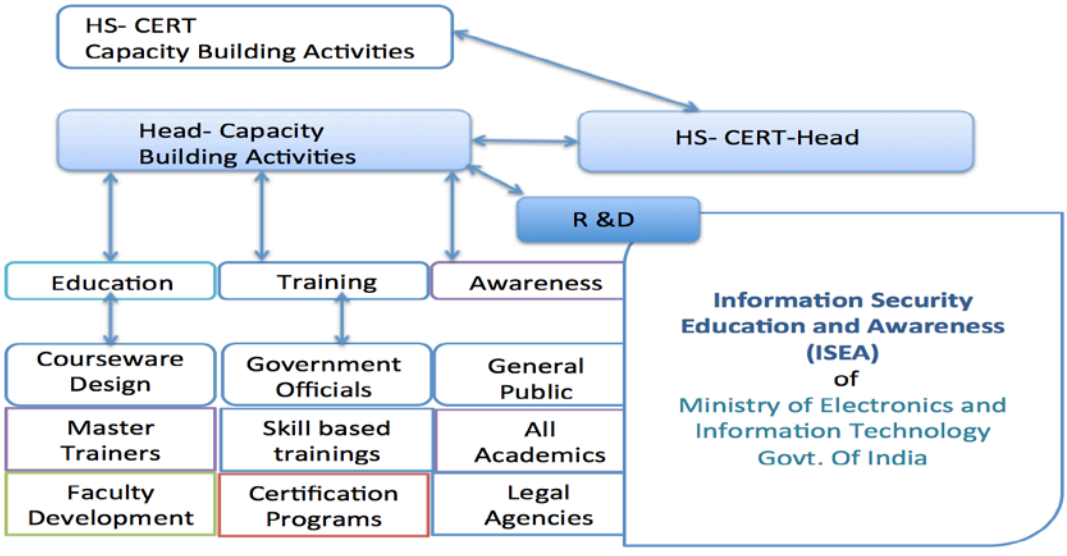
The CERT-Administrator coordinates about the implementation of Cyber Security policy framework, by issuing a separate policy, guidelines and procedures to the departments, industry and general public. As part of the policy, the CERT administrator coordinates with industry and Government for suitable guidelines for data, information and personal privacy with respect to Industry and Government for securing an individual privacy in Haryana state.

Further, they coordinate through HSCERT-HEAD, about privacy monitoring and capacity building activities in implementation of privacy management framework.

There are 70 awareness programs of 3-6 hour programs for all Government agencies and industry, national/ international seminar/ workshops on privacy for data/ information/ governance are planned in Haryana.

10.3 Implementation of Cyber Security Capacity Building Framework

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 and global access to ICT, combined with economic growth, has resulted in creating 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 different areas of cyber security.



Capacity Building activities with respect to National requirements

The Government of Haryana ensures the target of Government of India's Information Security Education and Awareness Program (ISEA), Phase-II target of 1.1 lakh cyber security capacity building activities and from Haryana State an around 6,000 Cyber Security professionals will be trained over the next 5 years in all sections – including 600 at Masters level at both teachers and Faculty level, where 4000 at the Graduate level, 1400 from among the employees of the State Government including LEAs by associating with Information Security Education and Awareness (ISEA), 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 Curriculum for Educational Institutes

The Haryana Government ensures and supports by considering resources of cyber security curriculum at school level to graduation level of Information Security Education and Awareness Program of the Ministry of Electronics and IT, Government of India for implementing in Haryana State

Cyber Security Awareness Programs in Haryana

With support of ISEA Phase-II resources, Haryana Government ensures through head, capacity building activities of HS-CERT, conducts awareness programs in Haryana State in the form of cyber security awareness programs for academics, Government and general public about 100 workshops in Haryana in next 5 years, an around 15 awareness weeks could be planned for across all major cities in Haryana and 20 Training programs (2/3/5 days) for Government department with respect to cyber security and related technologies.

R&D efforts for Cyber Security

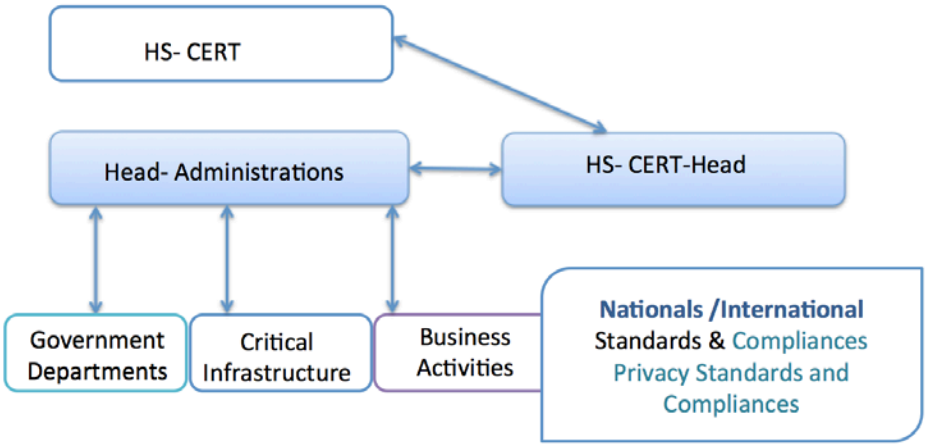
The Government of Haryana ensures the need for enhancing the efforts in R&D and innovation in this area and intends to establish a strong eco-system for Academia-Industry-Government collaboration for indigenous solutions for Haryana state.

10.4 Implementation of 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.

As part of their continuous 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 to protect their assets.

This framework may be derived through the development of set of objectives and practices as suggested by national and international standards and also by associating with cyber security forums of state, government and Academia.



HS-CERT- Administration department under ISMO implements national/ international compliances/ standards by promoting a cyber security forum and crisis management committees in coordination with Government for implementing cyber security compliance and management framework with the following components

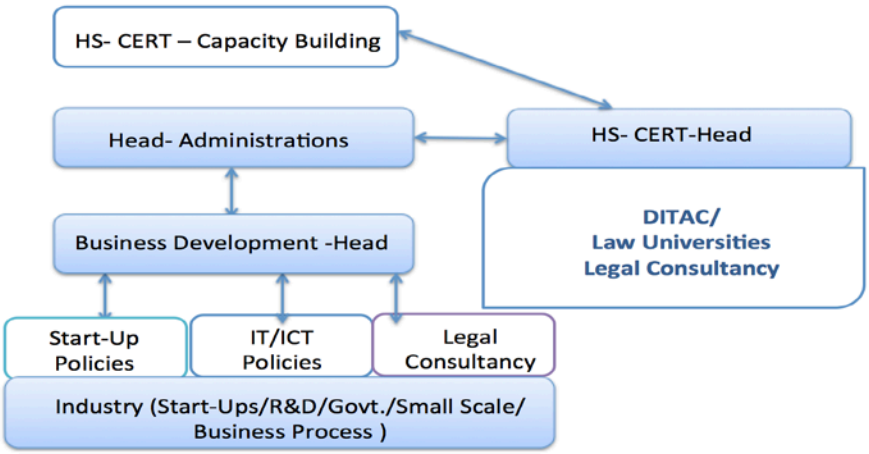
- Promotion of open standards in Compliances
- Haryana State Critical Infrastructure (IT/ICT/Information Process and other key industries) Protection

All the identified critical assets/ resources under various CIIs of the State of Haryana need to be gazette notified as "**Protected System**" under section 70 of IT Act 2000. Any attack on a "Protected System" with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people, shall be treated as **Cyber Terrorism**. (Section 66F of IT Act 2000). Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment, which may extend to imprisonment for life.

The Government of Haryana shall plan the establishment of **Cyber Crisis Management Plan (CCMP)** as per international standard compliances to reduce the risk of disruption and improve the security posture.

Government of Haryana insists all critical IT/ICT/ITeS infrastructures (SDC, SWAN, CCTNS, etc) of Haryana Government need to comply with ISMS and other national/ International standards as per their business activities.

10.5 Implementation of Haryana Cyber Security Business Development Framework



The implementation of business development framework by taking consultancy or recruiting business head to encourage business prospects in cyber security in Haryana state.

The State of Haryana is to ensure Fiscal Incentives for promoting Cyber Security Business opportunities in Haryana. The incentives for establishing cyber security organizations as part of business development would be considered as per the approved policy of the State as applicable to incentives for IT/ ESDM & Start-up Industry.The fiscal incentives shall be applicable to all cyber security firms as part of business development in which supports indigenous security products/ security services / global emerged products in cyber security area.

10.6 Implementation of Legal and Regulatory (Cyber Security) Framework

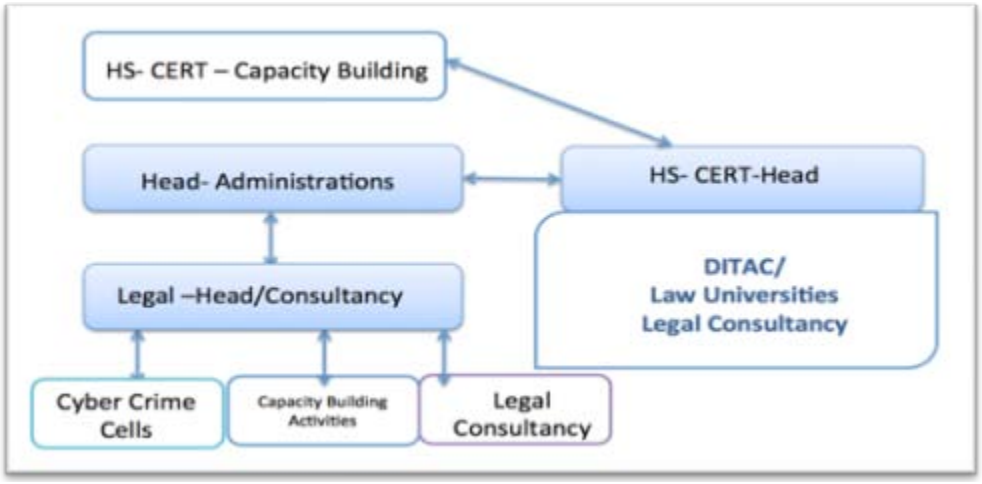
The Haryana Government is looking forward to address specific legislation governing cyber space activity for securing cyber space will control & counter cyber crimes by collaborating with various national and international agencies

The state may collaborate with **Digital Investigation Training and Analysis (DITAC)** and other available Legal expertise in the state to study existing frame works with respect to child, women security and privacy along with Cyber Security legal compliances.

Further, state will collaborate with non specific legislation of cyberspace such as copyrights, defamation, national security etc. with the following activities:

- Strengthening State LEA's for Cyber Security
- Cyber Crime Cells
- Capacity Building Activities for LEAs

The funding support for the setting up



Head, Administration coordinates implementation of legal framework by taking consultancy support with legal head and also various organizations such as DITAC, Law universities etc through HS-CERT/ISMO.

The capacity building activities for LEA's including judiciaries would be taken care. It is expected at least minimum 20 trainings would be conducted for LEAs including master trainers for 400 members in Haryana State.

Haryana State Government is planning to establish region based labs for legal and Forensic digital evidences to control the digital crime in State.

Budget allocation for Implementation of Haryana State Cyber Security Policy Framework:

Haryana State assures for implementing Haryana State Cyber Security Policy Framework by setting up of State level CERT, SOC, Threat intelligence services, Privacy Framework, Capacity Building activities, Legal compliances and business development activities etc.

The tentative budget required to implement the policy shall be approximately Rs 47 Crore for next 5 years.

This excludes the cost of Manpower which shall be available for the implementation and support through the IT Cadre of the State for which the budget provision has already been made in the IT Cadre Policy.