



## Madhya Pradesh Agency for Promotion of Information Technology

(A Regd. Society of Govt. of M.P. Under Department of Science & Technology)


Ref. No./MAP-IT/2017/1656

Bhopal, Dated. 02/11/17

### OPEN FOR SUGGESTIONS

MAP\_IT, on behalf of department of Science & Technology has come up with the first draft of state cyber security policy and inviting suggestions on the same.

All are requested to please go through the policy and write back to us at [cyber.security@mapit.gov.in](mailto:cyber.security@mapit.gov.in) for any suggestions.



Additional CEO

MAP IT



# CYBER SECURITY POLICY 2017

GOVERNMENT OF MADHYA PRADESH



**PREPARED BY:**  
**MADHYA PRADESH AGENCY FOR PROMOTION OF INFORMATION**  
**TECHNOLOGY (MAP\_IT)**

## TABLE OF CONTENTS

<b>1. INTRODUCTION .....</b>	<b>4</b>
<b>2. BACKGROUND .....</b>	<b>4</b>
<b>3. DEFINITIONS .....</b>	<b>5</b>
<b>4. VISION .....</b>	<b>6</b>
<b>5. CYBER SECURITY FRAMEWORK .....</b>	<b>8</b>
5.1 LEGAL AND REGULATORY FRAMEWORK .....	9
5.1.1 <i>Cyber Law and Related Legislation .....</i>	<i>9</i>
5.1.2 <i>Cyber Crime Cell .....</i>	<i>9</i>
5.1.3 <i>Cyber Forensics .....</i>	<i>10</i>
5.2 COMPLIANCE AND ENFORCEMENT FRAMEWORK .....	10
5.2.1 <i>Protection of CII .....</i>	<i>10</i>
5.2.2 <i>Emergency Response (MP-CERT) .....</i>	<i>10</i>
5.2.3 <i>Standards and Practices.....</i>	<i>11</i>
5.2.4 <i>Information Security Management System (ISMS) Implementation .....</i>	<i>12</i>
5.2.5 <i>Information and Communication Technology (ICT) Security Certification.....</i>	<i>12</i>
5.3 CAPACITY BUILDING AND CYBER SECURE ACCULTURATION FRAMEWORK .....	13
5.3.1 <i>Information Security Workforce Capacity Building.....</i>	<i>13</i>
5.3.2 <i>Cyber Security Acculturation.....</i>	<i>14</i>
5.3.3 <i>Promotion of Cyber Ethics.....</i>	<i>15</i>
5.4 BUSINESS DEVELOPMENT FRAMEWORK.....	15
5.4.1 <i>Promote Local Cyber Security Industry .....</i>	<i>15</i>
5.4.2 <i>Strategic Partnerships.....</i>	<i>16</i>
<b>6. STAKEHOLDERS' RESPONSIBILITIES.....</b>	<b>17</b>
6.1 CITIZENS .....	17
6.2 PRIVATE SECTOR.....	17
6.3 PARTNERS.....	18
6.4 GOVERNMENT .....	18
<b>7. Institutional Arrangement .....</b>	<b>19</b>
<b>8. APPENDIX I.....</b>	<b>22</b>
8.1 FISCAL INCENTIVES.....	22

# ABBREVIATIONS

GoMP	Government of Madhya Pradesh
Gol	Government of India
MAP_IT	Madhya Pradesh Agency for Promotion of Information Technology
CERT	Computer Emergency Response Team
ICT	Information and Communication Technology
CII	Critical Information Infrastructure
NCCC	National Cyber Coordination Centre
NCIIPC	National Critical Information Infrastructure Protection Centre
ISMS	Information Security Management System
I.T Act	Information Technology Act
SCSC	State Cyber Security Committee
ITes	Information Technology Enabled Services
SME	Small and Medium Enterprise
R&D	Research and Development
SLBC	State Level Bankers Committee
SCADA	Supervisory Control and Data Acquisition
DCS	Distributed Control System

## 1. INTRODUCTION

Today computers have pervaded every aspect of human existence – health care, communication, business and education. Even personal relationships develop over the internet. The internet has opened the doors to a flood of information. More and more activities are taking place in the cyber space, including business deals and monetary transactions. Security to citizens doing their interactions in the cyber space is of growing importance. The state of Madhya Pradesh has been continuously working to augment the facilitation of citizens through providing services through use of information security. The growing technological space also brings in more and more interactions of citizens on to the cyber space where in a clear delineation of the state policy in this regard is sought to be done in the “M.P State Cyber Security Policy”.

## 2. BACKGROUND

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

Technology typically has an exponential growth rate. So is the case with cybercrime which goes hand in hand with technology. Although the Government of India has passed laws and set up agencies, the onus is on the individual states to take up initiatives, drive on-ground implementation and ensure that a safe cyber space is created in the local environment. Hence, it becomes imperative for the state to adopt a dynamic approach to maintain a safe cyber space through effective and ever evolving policies.

### 3. DEFINITIONS

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

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

**Critical Information Infrastructure – As per Section 70 of Information Technology (Amendment) Act, 2008** Critical Information Infrastructure (CII) is defined as a computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety.

**Cyber Crime** – Any illegal activity in relation with computers or internet or rather cyberspace can be loosely termed as cybercrime.

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

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

- **Cyber harassment:** Any form of harassment, such as directing obscenities and derogatory comments at specific individuals, committed through the use of computer resources can be categorized as cyber harassment.

**ISMS-** An information security management system (ISMS) is a set of policies and procedures for systematically managing an organization's sensitive data. The goal of an ISMS is to minimize risk and ensure business continuity by pro-actively limiting the impact of a security breach.

**Cyber Ethics-** Cyber ethics is the philosophic study of ethics pertaining to computers, encompassing user behavior and what computers are programmed to do, and how this affects individuals and society.

**Cyber warrior-** A computer expert engaged in the defense of information systems against outside attack.

**Adjudicating Officer-** means an adjudicating officer appointed under sub-section (1) of section 46 of I.T Act 2000.

#### **4. VISION**

The State of Madhya Pradesh is committed to create and sustain a safe and resilient cyberspace to promote well-being of its citizens, protection and sustainability of its infrastructure in cyber security sector. The following summarizes the vision to achieve a safe and resilient cyber space for Citizens, Businesses and Government:

1. Build awareness about cyber security and safe cyber practices among citizens.
2. Establish requisite Institutions and legal framework to counter cybercrime.
3. Build capacity and protect our Critical Information Infrastructure.
4. Equip professionals with requisite cyber security skills and knowledge and establish a pool of "Cyber Warriors" to work with the State.
5. Promote the state as an ideal destination for cyber security firms and startups to develop cyber security products.
6. Encourage State-State and inter-institutional partnerships to promote collaborative research efforts.

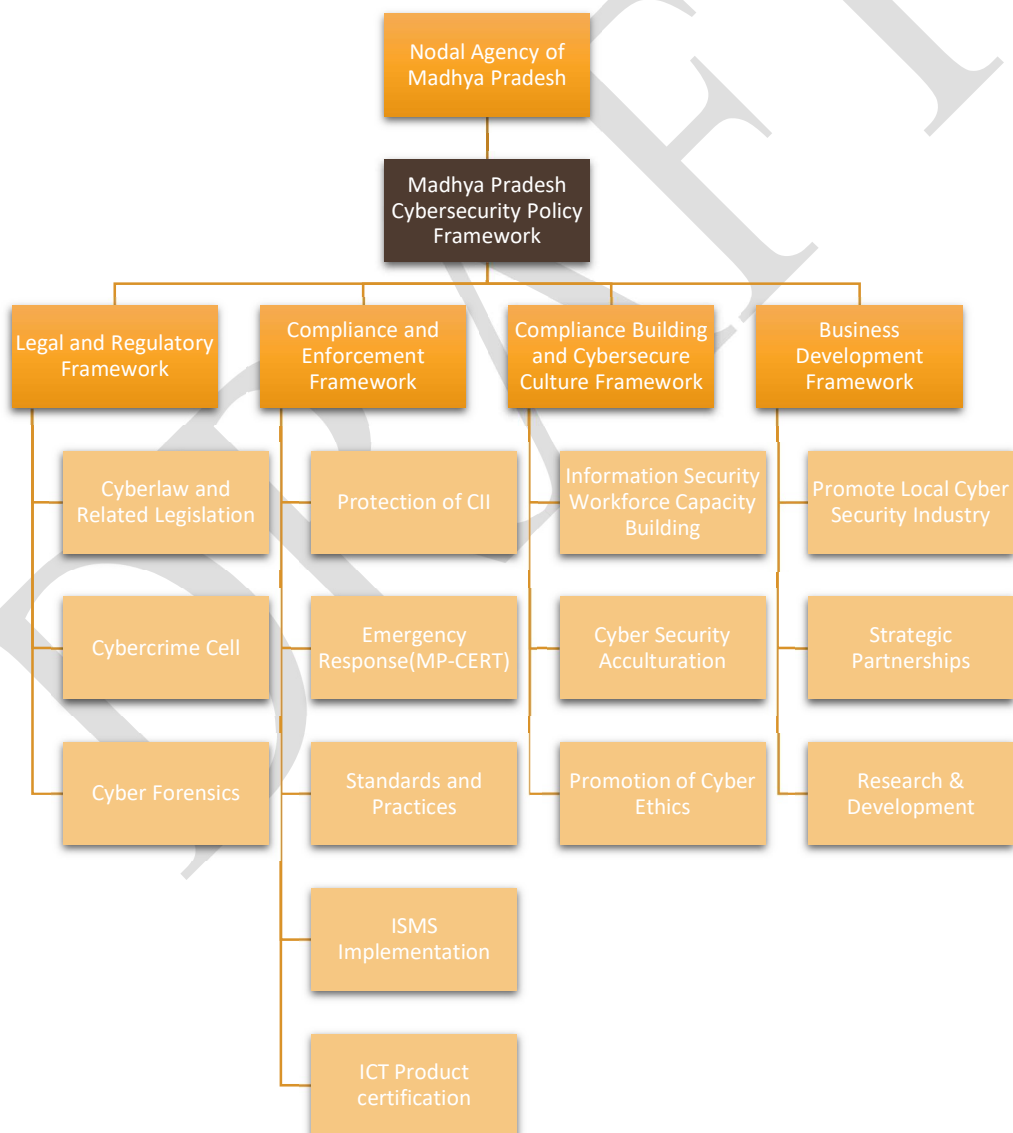
# FRAMEWORK

FRAMEWORK

## 5. CYBER SECURITY FRAMEWORK

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

1. Legal and Regulatory Framework
2. Compliance and Enforcement Framework
3. Compliance Building and Cyber Secure Culture Framework
4. Business Development Framework



## **5.1 LEGAL AND REGULATORY FRAMEWORK**

### **5.1.1 Cyber Law and Related Legislation**

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

#### *5.1.1.1 COLLABORATION TO ESTABLISH ROBUST LEGAL FRAMEWORK*

The state shall collaborate with law academies, legal experts in the area of cyber security, NCIIPC and CERT-In etc. to study the existing legal frameworks, identify problems and formulate advocacy laws to tackle real-time issues faced by these entities. The collaborative effort will be given the needed impetus to counter the ever evolving nature of cyber threats.

Non-Cyber specific legislation that may be relevant to regulate cyberspace activity whenever applicable such as protection of (a) copyrights (b) defamation (c) national security/sedition (d) anonymity etc. will also be addressed to protect information flow on the internet.

### **5.1.2 Cyber Crime Cell**

#### *5.1.2.1 CYBER GRIEVANCE REDRESSAL EFFORTS*

The State of Madhya Pradesh will augment a specialized Cyber Crime Cell for investigating into complaints pertaining to offences under the Information Technology Act. Cyber Crime Cell is currently setup under the Home Department, Govt. of Madhya Pradesh. The Government shall further strengthen this unit to simplify reporting, tackling and tracking progress on cyber-crimes.

The State will strive to create a cyber space free of pornography, especially child pornography, cyber bullying, and sexual harassment. The cyber grievance system will be put in place to lay special emphasis on these crimes. The State shall also appoint adjudicating authority for holding an inquiry related to cybercrimes in the manner prescribed by Central Government. The adjudicating authority shall be the Secretary to Government of Madhya Pradesh and will discharge his duties as per the procedures defined in I.T Act 2000 and the amendment in 2008.

### **5.1.3 Cyber Forensics**

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

## **5.2 COMPLIANCE AND ENFORCEMENT FRAMEWORK**

### **5.2.1 Protection of CII**

#### *5.2.1.1 RISK-BASED APPROACH IN PROTECTING CRITICAL INFORMATION INFRASTRUCTURE (CII)*

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

#### *5.2.1.2 THINK TANK FOR POLICY AND DECISION INPUTS*

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

### **5.2.2 Emergency Response (MP-CERT)**

#### *5.2.2.1 APEX AGENCY FOR STATE-WIDE COORDINATION*

The government shall set up MP-CERT, a nodal agency for the state to coordinate with institutions, organizations and companies. MP-CERT will contribute towards the State's efforts for a safer, stronger internet for all citizens by responding to major incidents, analyzing threats, and exchanging critical cyber security information with trusted partners.

The primary mandate of MP-CERT would be to:

1. Provide cyber security related actionable information to the Government, critical infrastructure agencies, private industries and general public through advisories
2. Provide cyber security protection through intrusion detection and prevention capabilities
3. Develop state's crisis management plan and implement the same in coordination with CERT-IN.
4. Assist the State in collaborative efforts to improve the cyber security posture of the State
5. Initiate proactive measures to increase awareness and understanding of information security and computer security issues
6. Round the clock support facility will be established for emergency response and crisis management.
7. To conduct security audits or assessments of government and constituent IT infrastructure in the state, evolving security policy for the state
8. Coordinate with stakeholders and drive the State's efforts. Through a network of dedicated officers in every department, the support team shall continuously monitor the cyber situation in the State.

#### *5.2.2.2 BUSINESS CONTINUITY*

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

### **5.2.3 Standards and Practices**

#### *5.2.3.1 INFORMATION SHARING AND ANALYSIS CENTRE*

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

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

4. The State shall develop Common Repository for the state to identify latest threats and incidents and will be shared with aligned agencies.
5. The State shall also establish Security Operations Centre which shall equipped with required infrastructure to do the analysis of logs generated from different sources.

#### *5.2.3.2 PROMOTION OF OPEN STANDARDS*

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

#### *5.2.3.3 PROCUREMENT OF SAFE ICT PRODUCTS*

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

### **5.2.4 Information Security Management System (ISMS) Implementation**

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

### **5.2.5 Information and Communication Technology (ICT) Security Certification**

#### *5.2.5.1 CERTIFICATION OF CYBER SECURITY PRODUCTS AND SERVICES*

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

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

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

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

### **5.3 CAPACITY BUILDING AND CYBER SECURE ACCULTURATION FRAMEWORK**

#### **5.3.1 Information Security Workforce Capacity Building**

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

##### **5.3.1.1 CERTIFICATION PROGRAMS**

The State shall develop certification programs and collaborate with academic institutions to encourage students to sign up for these programs. The state shall aim to provide recruitment assistance to private sector, which will significantly reduce on-boarding costs for employers.

##### **5.3.1.2 COLLABORATION WITH ACADEMIC AND RESEARCH INSTITUTIONS**

The State shall set up Research and Development center in association with well-established academic institutions to boost research in specific areas of cyber security. The State shall also launch specific R&D projects relevant to current day challenges that the Government faces, which will be addressed through these centers.

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

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

#### *5.3.1.3 CYBER WARRIORS*

The state shall create a pool of 'cyber warriors' trained in cyber security, to work as part-time security consultants with the Government, advising the Government in procuring ICT and cyber security products, simulating cyber-attacks to help find security loopholes, and assisting MP-CERT on ground in case of a cyber-security incident.

#### *5.3.1.4 CUSTOMIZED TRAINING PROGRAMS*

The Government shall conduct customized training programs on cyber security for Government Departments, PSUs, Banks, Telecom Companies and other key Industries which are associated with critical infrastructure.

### **5.3.2 Cyber Security Acculturation**

#### *5.3.2.1 MULTI-CHANNEL AWARENESS CAMPAIGN*

The Government shall launch a state-wide multi-channel awareness campaign involving workshops, social, print and digital media etc. to create cyber security awareness amongst its citizens. The Government shall also coordinate with banks, mobile companies and financial institutions to improve awareness regarding cyber security measures to be adopted.

#### *5.3.2.2 SCHOOL LEVEL CYBER SECURITY EDUCATION*

Having identified that cyber security is an important aspect of digital education, Madhya Pradesh will modify curriculum for high schools to include aspects of cyber security relevant to children. This will be deployed along with the School Computer Literacy Program. The Government will also launch a program that will be accessible to all children to deal with issues such as cyber bullying, cyber etiquette, identity theft, privacy etc. As more and more human interaction is being

shifted online, the importance of good and acceptable behavior online shall be outlined and paralleled with that of offline behavior.

#### *5.3.2.3 GUIDELINES FOR SAFE PRACTICES*

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

#### *5.3.2.4 CYBER SECURITY CHALLENGE*

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

### **5.3.3 Promotion of Cyber Ethics**

The Government shall endeavor to promote cyber ethics in citizens and government officials through conducting training programs and workshops. For this purpose, state shall encourage all departments to actively participate in the programs conducted by the state to make sure that the cyber ethics message is understood by them and proper steps have been taken to ensure that their respective cyber space is secured.

## **5.4 BUSINESS DEVELOPMENT FRAMEWORK**

### **5.4.1 Promote Local Cyber Security Industry**

#### *5.4.1.1 DEDICATED INCUBATOR FOR CYBER SECURITY STARTUPS*

The Government of Madhya Pradesh shall setup a dedicated incubator for cyber security related start-ups. The state shall also develop a venture capital model to provide assistance to first generation entrepreneurs, start-ups and SMEs operating in this field.

#### *5.4.1.2 CYBER SECURITY EXPO*

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

#### *5.4.1.3 PROMOTING SMEs IN CYBER SECURITY*

The Government shall award a certain number of cyber security contracts every year to SMEs incorporated in Madhya Pradesh and devise a mechanism to ensure transparency in the allotment procedure.

#### *5.4.1.4 FISCAL INCENTIVES*

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

### **5.4.2 Strategic Partnerships**

#### *5.4.2.1 COLLABORATION WITH PRIVATE SECTOR*

In addition to collaborating with colleges for R&D projects, the State shall outsource relevant R&D projects of the Government to corporates incorporated in Madhya Pradesh. Startups incorporated in Madhya Pradesh 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. The Government will enter into strategic partnerships with the private sector to set up infrastructure such as cyber security training and development labs, which in turn will facilitate the development of new products.

#### *5.4.2.2 PARTNERING WITH SERVICE PROVIDERS*

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

#### 5.4.2.3 PARTNERSHIPS WITH INTERNATIONAL AGENCIES

Numerous international institutions and agencies who have already established a name for themselves at the global level. Madhya Pradesh shall strive to enter into strategic alliances with such organizations to benefit from their infrastructure, skillset and research capabilities.

## 6. STAKEHOLDERS' RESPONSIBILITIES

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

### 6.1 CITIZENS

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

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

### 6.2 PRIVATE SECTOR

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

1. Be accountable for the products and services they provide and provide adequate guidance for the users
2. Adopt 'security by design' and 'privacy by design' principles into their standards
3. Maintain transparency in their security and data-handling mechanisms

4. Invest in training and capacity building to meet future cyber security needs

### **6.3 PARTNERS**

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

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

### **6.4 GOVERNMENT**

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

1. Protect Critical Information Infrastructure (CII)
2. Develop safe and secure e-Governance products, applications and services
3. Protect sensitive citizen data
4. Strengthen the laws to effectively handle cyber crimes
5. Facilitate the development of secure ICT products
6. Advise public on safe practices to improve awareness
7. Collaborate with the private sector to grow the cadre of cyber security professionals
8. Any other activity in the interest of citizen and protecting the secured cyber space.

## 7. Institutional Arrangement

I. A State Cyber Security Committee (SCSC) shall be formed to monitor the activities under cyber security framework. Following committee structure shall be constituted, namely

1. Chief Secretary to Government of Madhya Pradesh as Chairman
2. Principal Secretary to Government of Madhya Pradesh, Department of Home, as member
3. Principal Secretary to Government of Madhya Pradesh, Department of Commerce & Industries, as member
4. Principal Secretary to Government of Madhya Pradesh, Department of Finance, as member
5. Principal Secretary to Government of Madhya Pradesh, Department of Technical Education, as member
6. Principal Secretary to Government of Madhya Pradesh, Department of Planning, Economics & Statistics, as member
7. Principal Secretary to Government of Madhya Pradesh, Department of Law & Legislation, as member
8. Principal Secretary to Government of Madhya Pradesh, Department of Science & Technology, as member secretary
9. Principal Secretary to Government of Madhya Pradesh, Department of Higher Education, as member
10. Principal Secretary to Government of Madhya Pradesh, Department of School Education, as member
11. Principal Secretary to Government of Madhya Pradesh, Department of Cooperation, as member
12. Principal Secretary to Government of Madhya Pradesh, Department of Public Relations, as member
13. State Informatics Officer, National Informatics Centre, Madhya Pradesh, as member
14. State Level Banker's Committee (SLBC) Convener, as member
15. Any other invitee as per approval of the chairman

- II. SCSC will approve administrative and operational framework including resources, roles and responsibilities, reporting system.
- III. SCSC will approve rules and guidelines for effective implementation of Cyber Security Policy in Madhya Pradesh
- IV. SCSC will facilitate inter-departmental coordination required to meet the policy objectives;
- V. Madhya Pradesh Agency for Promotion of Information Technology (MAP\_IT), Department of Science & Technology will be the Nodal Agency for effective implementation of this policy. However, individual responsibilities will be assigned to other departments time to time.



# APPENDIX

APPENDIX

## 8. APPENDIX I

### 8.1 FISCAL INCENTIVES

Relevant incentives mentioned in the other Government policies for IT/ITeS shall be applicable for cyber security firms.

In addition to that, the following incentives shall be provided:

1. **Server Space:** Rack Space shall be provided from the State Data Centers to cyber security startups incorporated in Madhya Pradesh at a subsidized cost. In addition, the option of subsidizing cost of server space leased through third party vendors shall also be explored.
2. **Promoting SMEs:**
  - a. **Procurement:** Additional preference shall be given to SMEs in the field of Cyber Security for procurement of cyber security services by the Government. Separate guidelines will be issued for the same.
3. **Promoting Start-ups:**
  - a. **Financial Assistance as Matching Grants:** The Government would match the funding raised by the start-up in the field of cyber security from Government of India on a 1:1 basis as matching grants.
  - b. **R&D grants:** The Government of Madhya Pradesh will facilitate to provide specific R&D grants to IT companies who are in cyber security domain in tune of 10% of overall R&D expenses of the company's Madhya Pradesh operations or INR 500,000, whichever is lesser.

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



## Adjudicating Authority:

Contact Details	Jurisdiction	Address
Secretary, Government of Madhya Pradesh Department of Science and Technology	Madhya Pradesh	Mantralaya, Bhopal, Madhya Pradesh

**Government of Madhya Pradesh**  
**Department of Science & Technology**

