Government of Jammu & Kashmir
Information Technology Department
Civil Secretariat, J&K

Subject: Cyber Security Policy, 2022.

Government Order No. 02-JK(ITD) of 2023
Dated: 09.01.2023

Sanction is hereby accorded to the notification of Cyber Security Policy, 2022, UT of J&K, forming **Annexure** to this order (total 23 pages).

By Order of the Government of Jammu and Kashmir.

Sd/-
(Prerna Puri) IAS
Commissioner/Secretary to the Government
Information Technology Department

No: IT-Gen/280/2022 (232110) Dated: 09.01.2023

Copy to the:

1. Secretary, Information Technology & Communications.
2. Learned Advocate General, J&K.
3. All Financial Commissioners (Additional Chief Secretaries).
4. Director General of Police, J&K.
5. All Principal Secretaries to the Government.
6. Director General, J&K IMPA&RD.
7. Chief Electoral Officer, J&K.
8. All Commissioner/Secretaries to the Government.
9. Principal Resident Commissioner, J&K Government, New Delhi.
10. Joint Secretary (Jammu & Kashmir/Ladakh), Ministry of Home Affairs, Government of India.
11. Chairperson, J&K Special Tribunal.
12. Divisional Commissioner, Kashmir/Jammu.
13. All Heads of Departments/Managing Directors.
14. All Deputy Commissioners.
15. Director Information, J&K.
16. Director, Archieves, Archaeology and Museums.
17. Secretary, J&K Public Service Commission/BoPEE/SSB.
18. Director, Estates, Srinagar/Jammu.
19. Principal Private Secretary to the Lieutenant Governor.

09/01/23

20. General Manager, Government Press, Srinagar/Jammu.
21. Private Secretary to the Chief Secretary.
22. Private Secretary to Advisor (B) to the Lieutenant Governor.
23. Private Secretary to Commissioner/Secretary to the Government, Information Technology Department.
24. I/c Website, GAD.
25. Notification/Stock file.

09/1/23

Under Secretary to Government
Information Technology Department

09/1/23

JK - Cyber Security Policy - 2022

CYBERSECURITY POLICY, 2022

INFORMATION TECHNOLOGY DEPARTMENT

GOVERNMENTOFJAMMU AND KASHMIR

Version : 1.0

Drafted by : SeMT J&K

TABLE OF CONTENTS

Acronyms	
GoJK	Government of Jammu & Kashmir
GoI	Government of India
ITD	Information Technology Department
SeMT	State e-Governance Mission Team
JaKeGA	Jammu and Kashmir e-Governance Agency
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
IT Act	Information Technology Act
UTCSC	Union Territory Cyber Security Committee
ITES	Information Technology Enabled Services
SME	Small and Medium Enterprise
R&D	Research and Development
UTLBC	Union Territory Level Bankers Committee
SCADA	Supervisory Control and Data Acquisition
UT	Union Territory
DCS	Distributed Control System
CISO	Chief Information Security Officer
Dy. CISO	Deputy Chief Information Security Officer

1. INTRODUCTION

Today computers have pervaded every aspect of human existence – health care, communication, business and education. More and more activities are taking place in the cyberspace, including business deals and monetary transactions. Security of citizens interacting in cyber space is of utmost importance. The UT of Jammu and Kashmir is continuously working to provide a safe and secure cyber space to its citizens.

2. BACKGROUND

Government of India has took its first step towards ensuring a safe cyber space to all its stakeholders with the passing of Information Technology Act 2000. The Act was later amended giving way to the IT (Amendment Act 2008), mainly to cover emerging security related issues. Various other initiatives were simultaneously undertaken by the Government of India to address cybersecurity challenges. To integrate all the initiatives in this area and tackle the fast-changing and diverse nature of cyber-crimes, the Government 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.

Information Technology typically has had an exponential growth rate. Although, Government of India has passed laws and set up agencies, the onus is on the States/UTs to take initiatives, drive on-ground implementation and ensure that a safe cyber space is created in the local environment. Hence, it becomes imperative for the Union Territory of J&K to adopt a dynamic approach to maintain a safe cyber space through effective and ever evolving policies.

3. DEFINITIONS

1. **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.
2. **Cyber Security** - The activity or process, ability or capability, or state whereby information and communication systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.
3. **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.
4. **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:

a. **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, especially of a financial nature.
b. **Cyber terrorism:** Any act of terrorism committed through the use of cyber space or computer resources can be categorized as cyber terrorism.
c. **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.
d. **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.
e. **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.

5. **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.
6. **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.
7. **CCMP:** Cyber Crisis Management Plan to identify and counter any kind of cyber threat & cyber terrorism which needs to developed inline with National plan with required support from CERT-In.
8. **Cyber Security Analyst -**A computer expert engaged in the defense of information systems against outside attack.
9. **Adjudicating Officer-** means an adjudicating officer appointed under sub-section (1) of section 46 of I.T Act 2000.

4. VISION

The UT of Jammu and Kashmir is committed to create and sustain a safe and resilient cyber space to promote well-being of its citizens and t ensure protection and sustainability of its infrastructure in cybersecurity 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. Put in place equipment tools and techniques to anticipate, counter and mitigate the effects of cyber attacks.
3. Establish requisite Institutions and legal framework to counter cybercrime.
4. Build capacity and protect our Critical Information Infrastructure.
5. Equip professionals with requisite cyber security skills and knowledge and establish a pool of "Cyber Security Analysts" to work with the UT.
6. Create a log of incidents and continuously analyze it to indentify patterns and detect attacker profiles.
7. Promote the UT as an ideal destination for cyber security firms and startups to develop cyber security products.
8. Encourage UT-State/UT and inter-institutional partnerships to promote collaborative research efforts.
9. To build a knowledge base of best practices, tools and procedures to tackle cyber attacks.

5. MISSION

To identify, analyze, protect and build capabilities & resiliency to prevent and respond to cyber threats posed to UT's digital information and ICT & Operational Technology (OT) assetsc in cyber space through a combination of institutions, people, processes, technology, legal framework and interaction between all these.

6. OBJECTIVES

6.1 To create a secure cyber ecosystem in the UT, generate adequate trust & confidence in IT systems and transactions in cyberspace and thereby enhance adoption of safe practices of IT safe practices in all sectors of the economy and Government departments.

6.2 To create an assurance framework for design of security policies and for promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (product, process, technology & people).

6.3 To strengthen the Regulatory framework for ensuring a Secure Cyberspace ecosystem.

6.4 To create a workforce of professionals skilled in cyber security through capacity building, skill development and training.

6.5 To enable protection of information while in process, handling, storage & transit so as to safeguard privacy of citizen's data and for reducing economic losses due to cybercrime or data theft/ identity theft.

6.6 To enable effective prevention, investigation and prosecution of cybercrime and

enhancement of law enforcement capabilities through appropriate legislative intervention.

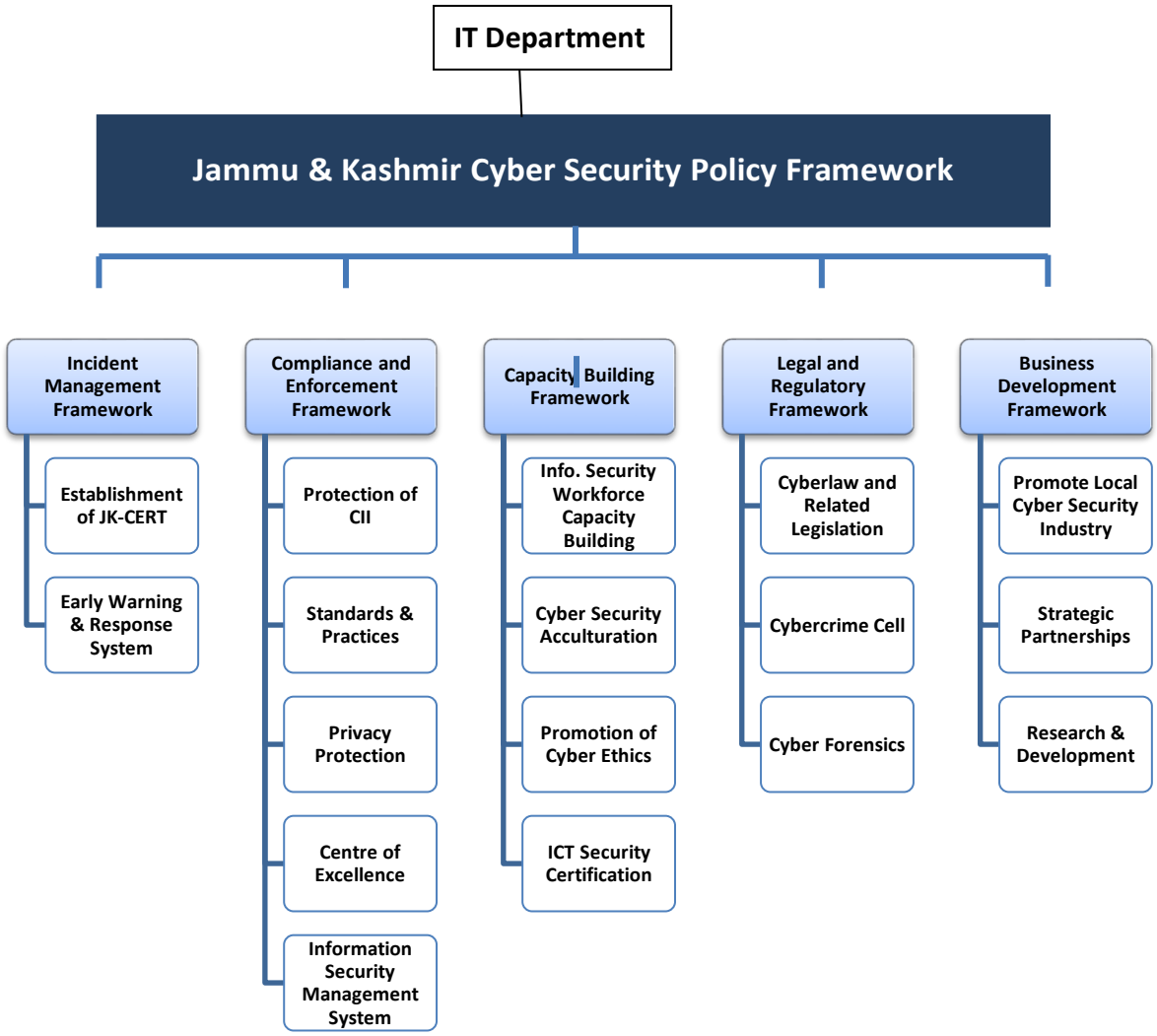
6.7 To engage information security professionals / organizations to assist e-Governance initiatives and ensure conformance to security best practices.

6.8 To work in collaboration with Cyber Crime Cells of the Police to ensure the culprit attackers are dealt with according to the law.

7. CYBERSECURITY POLICYFRAMEWORK

The Cyber Security Policy Framework intends to provide a holistic and complete solution for cyber security threats. The five pillars of the UT cyber security policy framework are as under:

1. Incident Management Framework
2. Compliance and Enforcement Framework
3. Capacity Building Framework
4. Legal and Regulatory Framework
5. Business Development Framework



7.1 INCIDENT MANAGEMENT FRAMEWORK

7.1.1 Establishment of JK-CERT

7.1.1.1 APEX AGENCY FOR UT-WIDE COORDINATION

The Government shall setup JK-CERT, a nodal agency for the UT to coordinate with institutions, organizations and companies. JK-CERT will contribute towards the UT's efforts for a safer, stronger Internet for all citizens by responding to major incidents, analyzing threats, and exchanging critical cybersecurity information with trusted partners.

7.1.1.2 The *primary* mandate of JK-CERT would be to:

a. Provide cyber security related actionable information to the Government, critical infrastructure agencies, private industries and general public through advisories and alerts
b. Provide cybersecurity protection through intrusion detection and prevention capabilities
c. Develop UT's Cyber Crisis Management Plan (CCMP) in line with National CCMP and implement the same in coordination with CERT-IN.
d. Assist the UT in collaborative efforts to improve the cybersecurity profile of the UT.
e. Initiate proactive measures to increase awareness and understanding of information security and computer security issues, among officials and public.
f. Establish round the clock support facility for emergency response and crisis management.
g. Conduct security audits or assessments of government and constituent IT infrastructure in the UT, evolving security policy for the UT.
h. Coordinate with stakeholders and drive the UT's efforts through a network of dedicated officers in every department; the support team shall continuously monitor the cyber situation in the UT.

7.1.1.3 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, Jammu and Kashmir shall strive to **ensure a culture of issuing and procuring cyber insurance.**

7.1.1.4 INCIDENT HANDLING & RESPONSE (IHR)

a. JK-CERT to serve as central point in the UT 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.
b. Cyber incidents shall be promptly handled by the JK-CERT for receipt, ticketing, triage, analysis and developing containment or response plan to build a resilient

ICT Infrastructure.

c. Standard Operation Process (SOP) Manual must be appropriately documented, reviewed, approved and be up to date to support the activities of JK-CERT
d. Standards for prioritizing Cyber Incidents shall be defined based on the criticality of the affected resource and the impact the incident has on the Constituent. Response Expectation should be stated by the Incident Priority Level.
e. Data collection for Incident Analysis should be adaptive to necessity. Relevant Data should be collected and should exclude the Data not directly relevant. The Data lifecycle shall be in accordance with legal and regulatory requirement and maintain a fool-proof chain of custody.

7.1.1.5 Early Warning and Response System

Understanding the importance of business continuity, the Government shall mandate an agency to design and develop a business continuity plan which needs to establish early warning and response system by establishing Security Operations Centre (SOC) at two locations, one each at Jammu & Srinagar. One location should work as standby to the other location in case of any type of calamity by continuously monitoring the threats towards all government websites and infrastructure etc. These will serve:-

a. To facilitate cooperation and collaboration with all stake holders (ISPs, Departments, Organizations etc. of Jammu and Kashmir) against cyber threats at highest level.
b. To create cyber security forum with relevant stakeholders for policy updates and analysis.
c. CISO to be (Designated by state/ UT) as per Section 12(1) shall coordinate with forums of cyber security at highest level through establishing dedicated responsible members teams (Section 12) across respective departments by coordinating security efforts and incident response for cyber security issues at the state level in tune with the national and international norms.
d. The JK-CERT shall also oversee the implementation of crisis management plan including cyber exercises collaborated with CERT-IN and other supported organizations to operate cohesively to achieve the mission.

7.2 COMPLIANCE AND ENFORCEMENT FRAMEWORK

7.2.1 Protection of CII

7.2.1.1 RISK-BASED APPROACH IN PROTECTING CRITICAL INFORMATION INFRASTRUCTURE(CII)

Absolute security exists only as a concept but cannot be achieved 100% practically, irrespective of the number of resources dedicated for. 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 other agencies like NCIIPC, CERT-IN, NCCC and also private sector and by adopting a risk-based analysis approach.

7.2.1.2 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.

7.2.2 Standards &Practices

7.2.2.1 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:

a. Development and implementation of Information Security Standards
b. Develop Information Security Guidelines and Best Practices
c. Joint development of a UT Cyber Crisis Management Plan (CCMP) to protect UT information assets and critical infrastructure
d. The UT shall develop Common Repository to identify latest threats and incidents and those will be shared with aligned agencies.
e. The UT shall also establish Security Operations Centre (SOC) which shall equipped with required infrastructure to do the analysis of logs generated from different sources. Dy.CISOs to be appointed as per Section 12 should be responsible for setting up the required incident response at respective organization level, under report to CISO.

7.2.2.2 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.

7.2.2.3 PROCUREMENT OF SAFE ICT PRODUCTS

Weak ICT products will increase vulnerability of information systems to external attacks and data leaks. The Government shall frame guidelines for procurement of trustworthy products by the UT. Government of Jammu & Kashmir may set up a centre or may collaborate with already existing centre(s) under MeiTY- GoI or under Government of Jammu & Kashmir for vetting the products to be used eventually.

7.2.3 Privacy Protection

J&K empowers its cyber 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 for the state's cyber security activities.

Government also has a special responsibility towards the citizens, Industry and organizations operating in the UT and further to national and international allies & partners and has to be able to assure them that every effort made is to render systems safety and to protect data and networks from cyber-attacks or any other unauthorized interference.

7.2.3.1 PERSONAL INFORMATION SECURITY (PIS)

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 their personal account to harm others may have severe implications in both economical and social affairs. The policy aims to enforce measures to safeguard the personal information of citizen stored in Govt databases.

7.2.3.2 ORGANIZATIONAL PRIVACY

Designing and developing a security policy for an organization is essential which includes the privacy of individual and organizations information to avoid information leakage where the basic information is initial target for attackers/ Cyber Criminals. The UT 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 and customers.

7.2.4 Center of Excellence

A Centre of Excellence (CoE) facility is proposed to be established for combating modern-day security threats. This State-of-the-Art facility will be equipped with means to detect and respond to both known and unknown security threats. CoE will also provide Centralized incubation facility to create specialized professionals for the UT and country to help combat cyber threats. It would also contribute towards real-time monitoring and analysis of security events as well as tracking and logging of security data for compliance or auditing purposes.

7.2.5 Information Security Management System (ISMS) Implementation

The Government shall encourage the implementation of ISMS across organizations in

the UT including critical infrastructure like SDC, SWAN, etc. 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.

7.3 CAPACITY BUILDING AND CYBER SECURE ACCULTURATION FRAMEWORK

7.3.1 Information Security Work force Capacity Building

The Government shall encourage, develop or impart training skill building along with knowledge sharing, technical drills & exercises to increase cybersecurity awareness at all levels. The Government will provide impetus to building a strong workforce of auditors, policy implementers, incident responders, data management experts and forensic personnel to provide cybersecurity related services. This will also include creating a pool of penetration testers and cybersecurity experts who can provide advisory services to the Government and UT-wide enterprises.

7.3.1.1 CERTIFICATION PROGRAMS

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

7.3.1.2 COLLABORATION WITH ACADEMIC AND RESEARCH INSTITUTIONS

The UT shall set up a Research and Development center in association with well-established academic institutions to boost research in specific areas of cyber security. The UT shall also launch specific R&D projects relevant to modern 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 UT 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 setup for students pursuing advanced academic degrees in cybersecurity fields.

7.3.1.3 CYBER SECURITY ANALYSTS

The UT shall create a pool of 'Cyber Security Analysts' trained in cyber security, to work as part-time security specialists of the Government, advising the Government in combating Cyber Terrorism, protecting from Cyber threats, simulating cyber-attacks to help find security loopholes, and assisting JK-CERT on the ground in case of a cyber-security incident. The CoE in

Cyber security shall specially focus on this area. Government of Jammu and Kashmir shall encourage full time jobs to the Cyber Security Analysts, so that talent remains within the region.

7.3.1.4 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 having critical infrastructure.

7.3.2 Cyber Security Acculturation

7.3.2.1 MULTI-CHANNEL AWARENESS CAMPAIGN

The Government shall launch a UT-wide multi-channel awareness campaign involving workshops, social,electronic, 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 cybersecurity measures to be adopted.

7.3.2.2 SCHOOL LEVEL CYBERSECURITY EDUCATION/ HYGIENE

Having identified that cyber security is an important aspect of digital education, Jammu and Kashmir 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, building cyber security hygiene, etc. As more and more human interaction is being shifted online, the importance of good and acceptable online behavior shall be outlined and communicated. Govt would collaborate with other Govt and Pvt organizations with the overall objective to build the Cyber Security Hygiene. Emphasis would be on developing online content for all age groups of students say Primary, Middle, Higher with special focus on Women, Children and Sr. Citizens.

7.3.2.3 GUIDELINES FOR SAFE PRACTICES

By collaborating with the private sector, the UT shall issue advisories and guidelines on best practices to help citizens and organizations stay aware of the latest developments in cyber crime and address them proactively.

7.3.2.4 CYBER SECURITY CHALLENGE

The Government shall promote an annual competition, named the Cyber Security Challenge, which will help identify and nurture individual talent. This will be a UT-wide drive to increase awareness as well as build assurance in the community about government initiatives and efforts to secure the cyber space with the help of its stakeholders. This challenge will have

different levels of complexity to appeal to personnel of varying levels of cyber security skills and competency.

7.3.3 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, UT shall encourage all departments to actively participate in the programs conducted by the UT 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.

7.3.4 Information and Communication Technology (ICT) Security Certification.

7.3.4.1 CERTIFICATION OF CYBER SECURITY PRODUCTS AND SERVICES

The Government shall establish Jammu and Kashmir 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

a) Vulnerability Assessment and Penetration Testing Services for critical infrastructure sectors
b) Security Assessment for control systems(SCADA/DCS)
c) ICT Product Security Assessment and Certification service
d) 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 cybersecurity products and critical ICT products will be made mandatory.

7.4 LEGAL AND REGULATORY FRAMEWORK

7.4.1 Cyber Law and Related Legislation

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

7.4.1.1 COLLABORATION TO ESTABLISH ROBUST LEGAL FRAMEWORK

The UT 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.

(***The privacy laws and data Protection Laws to be proposed by the Department of Law, Justice and PA)***

7.4.2 Cyber Crime Cell

7.4.2.1 CYBER GRIEVANCE REDRESSAL EFFORTS

The UT of Jammu and Kashmir will augment the existing 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 Jammu and Kashmir. The Government shall further strengthen this unit to simplify and galvanize reporting, tackling and tracking progress on cyber-crimes. The UT 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 UT will establish a Cyber Security Helpline / Grievances System to record and address the citizen grievances related to cyber theft, cyber frauds, pornography, especially (child pornography) cyber bullying, etc. The helpline would also advice various state entities to counter cyber threats in their respective organizations w.r.t computer infra, networks, application, etc.

7.4.3 Cyber Forensics

The UT will collaborate to establish a digital forensics lab to analyze and investigate cyber crime 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.

7.5 BUSINESS DEVELOPMENT FRAMEWORK

7.5.1 Promote Local Cyber Security Industry

7.5.1.1 DEDICATED INCUBATOR FOR CYBER SECURITY STARTUPS

The Government of Jammu and Kashmir shall setup a dedicated incubator for cyber security related start-ups. The UT shall also develop a venture capital model to provide assistance to first generation entrepreneurs, start-ups and SMEs operating and intending to enter in this field. The CoE infrastructure would also be used for the purpose.

7.5.1.2 CYBER SECURITY EXPO

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

7.5.1.3 PROMOTING SMEs IN CYBERSECURITY

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

7.5.1.4 FISCAL INCENTIVES

To boost the local industry, special fiscal and non-fiscal incentives will be given to firms operating in Jammu and Kashmir as per the prevailing policy(ies) of Government of Jammu & Kashmir.

7.5.2 Strategic Partnerships

7.5.2.1 COLLABORATION WITH PRIVATE SECTOR

In addition to collaborating with colleges for R&D projects, the UT shall outsource relevant R&D projects of the Government to corporate sector in Jammu and Kashmir. Startups incorporated in Jammu and Kashmir will be provided access to Government Applications to showcase their product as Proof of Concept (PoC). These projects may 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.

7.5.2.2 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 and devise strategies 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.

7.5.2.3 PARTNERSHIPS WITH INTERNATIONAL AGENCIES

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

8. SECURITY POLICY

JK-CERT will establish, operate, maintain, monitor and improve the Information Security Management System to ensure Confidentiality, Integrity and Availability of its Data, Information, Information Systems, Operation and Facilities used to offer Services to the Government. JK-CERT Services shall demonstrate Security Best Practices in compliance with the legal and regulatory requirements.

JK-CERT shall ensure timely and quality service to the Departments by Monitoring, Detecting, Assessing and Responding to the Cyber Vulnerability, Events causing Cyber Threats, Incidents and demonstrate Cyber Resilience.

Protection of IT/ICT and Information System Processes: The Government of J&K shall create an IT/ICT, Information Control Systems Protection Plan in collaboration with the public and private sector by adopting a risk-based management approach for infrastructure protection.

9. STAKEHOLDERS' RESPONSIBILITIES

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

9.1 CITIZEN

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:

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

9.2 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:

a) Be accountable for the products and services they provide and assure adequate guidance for the users
b) Adopt '***security by design***' and '***privacy by design***' principles into their standards
c) Maintain confidentiality/transparency in their security and data-handling mechanisms

d) Invest in training and capacity building to meet future cybersecurity needs

9.3 PARTNERS

Jammu and Kashmir Government shall partner with various institutions, PSU, government bodies like STPI, NIELIT etc for driving various initiatives. The potential partners include academic and research institutions, private players, other Government organizations etc. These partners shall:

a) Participate in information sharing efforts driven by the UT
b) Assist the UT in promoting it at the global stage
c) Assist the UT in its research efforts
d) Tie up with the UT Government to deploy/test new products developed

9.4 GOVERNMENT

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

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 cybercrimes
5. Facilitate the development to secure ICT products
6. Advise public on safe practices to improve awareness
7. Collaborate with private sector to carry out capacity building and take needful steps for creating infrastructure to increase the number of cybersecurity professionals.

10. INSTITUTIONAL ARRANGEMENT

With the purpose of monitoring the activities under cyber security framework and in order to smoothly implement the vision of **Cyber Safe J&K,** following organizational structure will be put in place:

10.1 Administration level

a. As per the Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018 issued vide Gazette Notification No. 1(4)/2016-CLFE, dated: 22-05-2018, an **Information Security Steering Committee (ISSC)** constituted in Jammu & Kashmir vide Government order number 1053-JK(GAD) of 2022, dated 12.09.2022 shall function as given at 10.1(b)

b. **The committee shall preferably meet every quarter to take needful decisions**

w.r.t:

i. All the Information Security Policies of the "Protected System "shall be approved by Information Security Steering Committee.
ii. Significant changes in network configuration impacting "Protected System" shall be approved by the Information Security Steering Committee.
iii. Each significant change in application(s) of the "Protected System" shall be approved by Information Security Steering Committee.
iv. A mechanism shall be established for timely communication of cyber incident(s) related to "Protected System" to Information Security Steering Committee.
v. A mechanism shall be established to share the results of all information security audits and compliance of "Protected System" to Information Security Steering Committee.
vi. Assessment for validation of "Protected System" after every two years.

10.2 Organization level

a. To strengthen the security posture throughout the UT of J&K, the concept of Dy.CISO(as per section 12 of the policy) would be carried out to have one Officer in each Department, Board, Corporation, Agency, District, etc..
b. The roles and responsibilities of Dy. CISOs are as under:
   i. **Implement**: Implement the instructions in their respective organizations, issued by IT department, Cert-In, NCIIPC and other Govt recognised bodies related to Cyber security
   ii. **Capacity Building**: Attend all the specialised training programs related to cyber security introduced by IT department
   iii. **Master Trainer**: Act as master trainer in the respective organization and spread Cyber Security related awareness.
   iv. **Information exchange**: Dy. CISOs are expected to stay connected to Chief Information Security Officer (CISO) for information exchange.
   v. Any other direction issued from Chairman ISSC/ CISO from time to time.

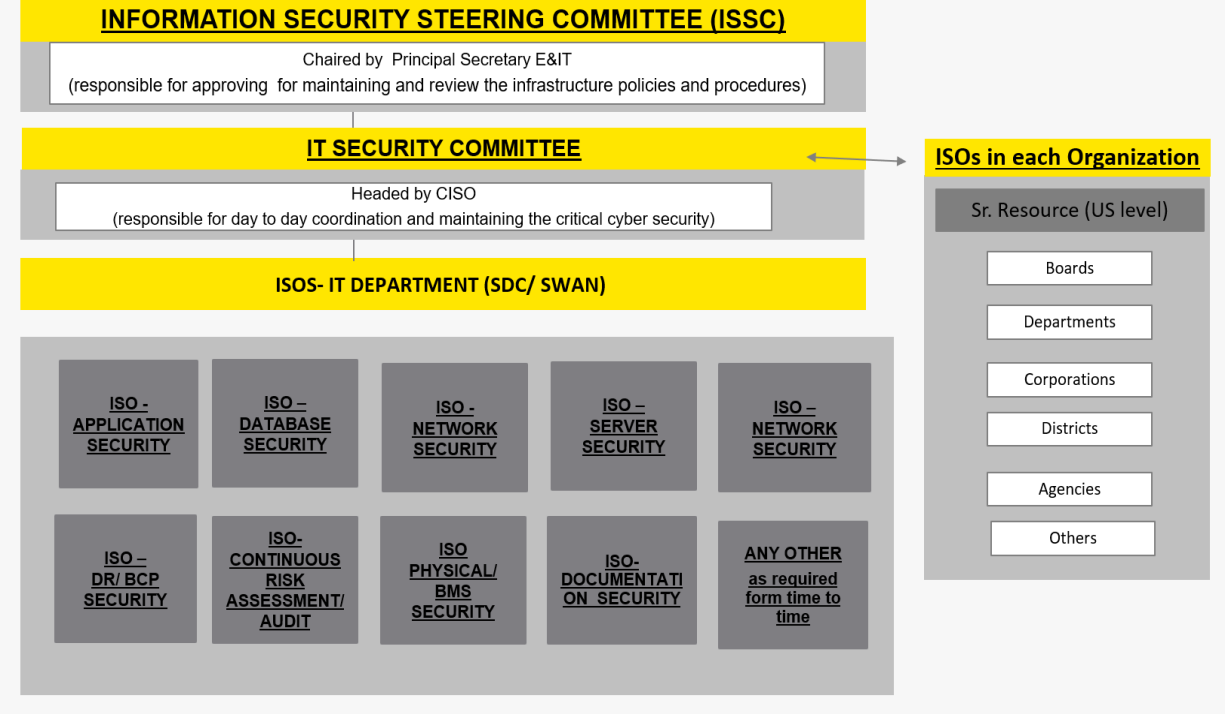
10.3 IT Department Level

10.3.1. Considering the hosting of all the Departmental applications in State Data Centre, Dy.CISOs shall be appointed at District level as well as at HQ level i.e. in the office of CISO. Government of Jammu & Kashmir shall nominate / depute/ appoint DIO,NIC, J&K of each Districts and ISO of each department as Dy.CISO for respective

district / department respectively and Additional SIO,NIC,J&K or officer of equivalent rank from NIC,J&K headquatered at Jammu / Srinagar (in the premises / vicinity of the office of CISO) shall be nominated / appointed as Dy. CISO Headquarter .

10.3.2. Dy. CISOs would report to CISO for Cyber Security related matters like Application Security, Database Security, Network Security, Server Security, DR / BCP Security, Physical Security, Documentation Security, Continuous Risk assessment/ Audits: Audits / Compliance & Enforcement, Continuous VA/ Checks/ periodicity of Audits, Coordination with Stake holder departments, etc.

10.4 UT Information Security - Organization structure



11. MANPOWER ALLOCATION

For successful implementation of the UT Cyber Security Framework, it is suggested to constitute teams with dedicated members to lead and manage various specialized teams/units. The team members can be on deputation/ additional charge or recruited directly from open market on Contract/ Outsource/ Third Party basis / otherwise, as deemed fit, by Government of Jammu and Kashmir.

12. Roles and Responsibilities:

#	Role	Responsibilities	Experience	Additional Requirements
1.	CISO	Overall head of ISMS, interface with State Government Departments & Districts, Centre Government Agencies (CERT-In, NCIIPC, MeitY, etc) and other collaboration with respect to cyber security issues in UT	Special Secretary/Additional Secretary to Government, ITD shall be CISO of UT of J&K	Govt Appointed
2.	Dy CISO	Shall report to CISO for Cyber Security related matters like Application Security, Database Security, Network Security, Server Security, DR / BCP Security, Physical Security, Documentation Security, Continuous Risk assessment/ Audits: Audits / Compliance & Enforcement, Continuous VA/ Checks/ periodicity of Audits, Coordination with Stake holder departments, etc.	• 15+ years' experience in information technology. • DIO NIC JK shall be Dy CISO in every District of UT of J&K. • Addl SIO NIC JK shall be Dy CISO(HQ).	Govt Appointed
3.	Head - JK CERT	Would be overall in-charge for JK-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	Appropriate Certification(s)
4.	Information Security Officer (As per requirement)	Would be responsible for Policy Compliance & Enforcement of Application Security/ Database Security/ Network Security/ Server Security/ DR and BCP Security/ Physical Security/ Documentation Security/ Continuous Risk assessment/ Audits, etc	10+ years' experience in information technology	Government Appointed
5.	Team Lead - Incident Management	Would provide expert guidance to the team members for continuous support to HK-CERT activities	5-7 years' experience in managing security incidents	Relevant certification & experience
6.	Team Lead - Compliance and Enforcement	Would provide expert guidance to the team members on compliance and enforcement of standards, procedures and managing Information Security Management System (ISMS)	5-7 years' experience in drafting and enforcing standards, procedures and managing ISMS	Relevant certification & experience
7.	Team Lead -Capacity Building	Would be overall in-charge for capacity building activities in state in terms of Information security activities	5-7 years' experience in education, training activities	Exposure in designing and developing courseware in IT/ITES courseware
8.	Team Lead - Legal &	Would be overall in-charge for handing all legal matters and regulatory compliance related to	5-7 years' experience in	Relevant experience in

	Regulation	cyber security, cyber forensics and head the cybercrime cell.	managing cyber cell, cyber forensics, legal compliances, and regulations	concerned domain
9.	Team Lead - Business Development	Would manage the development and promotion of local cyber security industry, strategic partnerships, research and development related activities.	5-7 years' experience in IT related business development, liaising, etc.	Relevant experience in concerned domain
10.	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 JK-CERT activities	5-7 years' experience in managing security incidents	Relevant certification
11.	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 JK-CERT activities	5-7 years' experience in managing security incidents	Relevant certification
12.	Team Member- JK-CERT/ Incident Management/ Compliance / Legal/ Capacity Building/ SOC/ Threat Intelligence (3 members each)	The member would be having experience in design and development capabilities in the areas of incident management/ Legal/ Compliance/ 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

12.1. Policy in the first instance mentions Roles and Responsibilities of 12 officials to be recruited / deputed/ outsourced/ otherwise, as deemed fit, by the Government of Jammu & Kashmir, however, smooth / effectively functioning and operation of various aspects of 'Jammu & Kashmir Cyber Security Policy' may require 40-50 manpower, the decision for which shall be taken by the Government of Jammu & Kashmir on the recommendation of ISSC (refer section 13 (13.2) - Appendix of the policy.

13. APPENDIX

13.1 FISCAL INCENTIVES

Relevant incentives mentioned in other policies of UT of Govt of J&K for IT/ITeS shall be applicable for Cyber Security firms.

13.1.1 Server Space: Rack space shall be provided from the State Data Centers to cyber

security startups incorporated in Jammu and Kashmir at a subsidized cost. In addition, the option of subsidizing cost of server space leased through third party vendors shall also be explored.

13.1.2 Promoting SMEs:

For procurements, 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.

13.1.3 Promoting Start-ups:

Information Security Steering Committee (ISSC) shall decide and issue separate guidelines for the same.

13.2 Budget / manpower Expansion Requirement:

Information Security Steering Committee (ISSC) shall review and decide on the following:

a. Manpower requirement / expansion
b. Budgetary requirements.
c. Usage of IT services prospectively by Government IT professional already appointed on permanent payroll.
d. Reviewing of skill sets and their budgetary requirements on half-yearly or yearly basis, as per requirement.
e. Promoting up of Start-ups.

14. Operative Period of Policy:-

This Policy shall come into force with effect from the date of notification of the policy and shall remain in force for a period of 5 years or till the declaration of a new or revised Policy, whichever is earlier.

15. Rights of the J&K Government:-

a. The UT of Government reserves the right to make/amend the provisions of this Policy and the necessary rules for implementation of this policy as and when required.
b. The decision of IT Department, Government of J&K , about the interpretation of this policy shall be final.

16. Exclusive Jurisdiction:

The courts in Jammu and Kashmir shall have exclusive jurisdiction to try any case arising out of the J&K Cyber Security Policy, 2022

<End of document>