

**(Empowering Citizens to Build a Safe and Secure Cyberspace)**



# Government of India

**Reviewed by: CISO, MIB**

## Table of Contents

|                                                                       |   |
|-----------------------------------------------------------------------|---|
| Preamble.....                                                         | 3 |
| Vision .....                                                          | 3 |
| Mission .....                                                         | 3 |
| Target Audience .....                                                 | 3 |
| Our Commitments .....                                                 | 3 |
| Service Security .....                                                | 3 |
| Data Protection .....                                                 | 3 |
| Service Availability .....                                            | 4 |
| Incident Response .....                                               | 4 |
| Service Standards .....                                               | 4 |
| Web Services & Applications of M/o Information and Broadcasting ..... | 4 |
| Cyber Security Best Practices .....                                   | 5 |
| Ministry Responsibilities .....                                       | 5 |
| Employee Responsibilities .....                                       | 5 |
| Citizen Responsibilities .....                                        | 6 |
| Awareness Initiatives.....                                            | 6 |
| Citizen Grievance Redressal .....                                     | 6 |
| Continuous Improvement .....                                          | 7 |
| Contacts .....                                                        | 6 |
| Important links of Government issued guidelines and advisories .....  | 7 |

## ➤ Preamble

The Ministry of Information and Broadcasting is committed to providing secure, reliable, transparent, and citizen-centric digital services. This Citizen Charter outlines our commitment towards protecting citizens' information, ensuring secure online services, and promoting cyber security awareness.

The Ministry shall continuously strengthen its cyber security posture in accordance with Government of India guidelines issued by the Ministry of Electronics and Information Technology, Indian Computer Emergency Response Team (CERT-In), and other applicable standards.

---

## ➤ Vision

To provide secure, trusted, resilient, and citizen-friendly digital services while safeguarding information assets against cyber threats.

---

## ➤ Mission

- Ensure secure dissemination of government information through MIB platforms.
  - Protect Government and citizen information.
  - Ensure confidentiality, integrity, and availability of information.
  - Strengthen cyber resilience through proactive risk management.
  - Foster cyber security awareness among citizens.
  - Provide awareness for responsive actions to be taken.
- 

## ➤ Target Audience

This Citizen Charter is intended for all citizens engaging with the digital platforms and services of M/o I&B, including:

- General public - People seeking information about government policies, schemes over MoIB's digital platforms
  - Media & Press Organizations – Journalists/ editors/publishers and print/digital media houses that rely on M/o I&B services.
  - Film Industry Stakeholders
  - Advertising & Communication Agencies – Agencies working with CBC for govt campaigns. Creative professionals involved in public awareness drives.
- 

## ➤ Our Commitments

The Ministry is committed to:

### ❖ Service Security

- Maintaining secure online portals and websites.
- Using industry-standard encryption for online communications.
- Protecting online transactions and digital interactions.
- Conducting regular security assessments and vulnerability testing.
- Ensuring timely security updates and patch management.

### ❖ Data Protection

- Collect only information necessary for service delivery.
- Protect citizen information from unauthorized access.
- Maintain appropriate access controls.
- Securely store and dispose of information using appropriate encryption and hashing techniques.

- Protect official sensitive information against cyber threats.

### ❖ Service Availability

- Maintain continuous availability of digital services.
- Minimize service disruptions.
- Restore services promptly following cyber incidents.
- Maintain disaster recovery and backup arrangements.

### ❖ Incident Response

- Detect cyber incidents promptly.
- Respond quickly to minimize impact.
- Notify competent authorities as per Government guidelines.
- Restore services with minimum disruption.
- Conduct post-incident analysis.

## ➤ Service Standards

| Service                             | Standard                            |
|-------------------------------------|-------------------------------------|
| Availability of online services     | 24×7 (planned maintenance excluded) |
| Reporting of cyber incidents        | Online/Email/Helpline               |
| Acknowledgement of incident reports | Within 24 hours                     |
| Initial assessment                  | Within 1 working day                |
| Escalation of major incidents       | Immediate                           |
| Citizen queries on cyber security   | Within 3 working days               |

## ➤ Web Services & Applications of M/o Information and Broadcasting (For Public Use)

| Website                                                                      | Purpose                                                                                                                                                                                                                                   |
|------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="http://pib.gov.in">pib.gov.in</a>                                   | <b>Official Press Information Bureau (PIB) website.</b> Serves as the primary source for Government of India press releases, cabinet decisions, speeches, media advisories, photographs, videos and ministry-wise official announcements. |
| <a href="http://accreditation.pib.gov.in">accreditation.pib.gov.in</a>       | Online portal for <b>PIB media accreditation</b> . Journalists can apply for fresh or renew accreditation.                                                                                                                                |
| <a href="http://archive.pib.gov.in/archive2">archive.pib.gov.in/archive2</a> | Archive of historical <b>Press Information Bureau</b> press releases.                                                                                                                                                                     |
| <a href="http://newindiasamachar.pib.gov.in">newindiasamachar.pib.gov.in</a> | Digital edition of <b>New India Samachar</b> , a government publication highlighting major development initiatives, policy achievements, governance stories, and flagship schemes.                                                        |
| <a href="http://photodivision.gov.in">photodivision.gov.in</a>               | Website of <b>Photo Division</b> , providing official Government of India photographs, photo archives, and media images.                                                                                                                  |
| <a href="http://factcheck.pib.gov.in">factcheck.pib.gov.in</a>               | <b>PIB Fact Check</b> portal that verifies misinformation related to Government of India policies, notifications, and announcements, allowing citizens to report suspected fake news.                                                     |
| <a href="http://employmentnews.gov.in">employmentnews.gov.in</a>             | Official <b>Employment News</b> portal publishing Central Government job vacancies, recruitment notices, career guidance, and examination information.                                                                                    |
| <a href="http://rojgarsamachar.gov.in">rojgarsamachar.gov.in</a>             | Hindi edition of <b>Employment News (रोजगार समाचार)</b> carrying government recruitment advertisements and employment-related information.                                                                                                |
| <a href="http://publicationsdivision.nic.in">publicationsdivision.nic.in</a> | Publications Division website offering Government of India                                                                                                                                                                                |

|                                                                  |                                                                                                                                                                                    |
|------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                  | books, journals, magazines, children's literature, and official publications.                                                                                                      |
| <a href="http://eneversion.nic.in">eneversion.nic.in</a>         | E-version portal of <b>Employment News</b> , providing digital editions and online subscriptions.                                                                                  |
| <a href="http://prgi.gov.in">prgi.gov.in</a>                     | Official website of the <b>Press Registrar General of India (PRGI)</b> earlier RNI. Provides newspaper registration services, publisher records, regulations, and online services. |
| <a href="http://presssewa.prgi.gov.in">presssewa.prgi.gov.in</a> | Online <b>Press Sewa</b> portal of PRGI for newspaper registration, title verification, ownership changes, annual statements, and related services.                                |
| <a href="http://cbcindia.gov.in">cbcindia.gov.in</a>             | Website of the <b>Central Bureau of Communication (CBC)</b> , responsible for government outreach, advertising, public awareness campaigns, and integrated communication.          |
| <a href="http://presscouncil.nic.in">presscouncil.nic.in</a>     | Official website of the <b>Press Council of India</b> , a statutory body that preserves press freedom and maintains standards of journalism.                                       |
| <a href="http://mib.gov.in">mib.gov.in</a>                       | Official website of <b>Ministry of I&amp;B</b> , containing policies, notifications, schemes, tenders, and organizational information.                                             |
| <a href="http://engage.mib.gov.in">engage.mib.gov.in</a>         | Citizen engagement portal of MIB for consultations, public participation, campaigns, surveys, and feedback initiatives.                                                            |

## ➤ Cyber Security Best Practices

- Beware of phishing emails.
- Avoid clicking suspicious links.
- Verify website URLs before login.
- Download software only from trusted sources.
- Update operating systems regularly.
- Backup important documents.
- Report cyber fraud immediately.

Be cautious of digital scams such as:

| Threat Type               | Description                                                             |
|---------------------------|-------------------------------------------------------------------------|
| <b>Phishing</b>           | Fake emails or websites pretending to be legitimate to steal data       |
| <b>Smishing</b>           | Fraudulent SMS messages urging users to click malicious links           |
| <b>Vishing</b>            | Scam calls posing as officials to steal sensitive information           |
| <b>Pretexting</b>         | Social manipulation to gain access to personal data                     |
| <b>Social Engineering</b> | Deceptive tactics to trick individuals into revealing confidential info |

## 1. Ministry Responsibilities

- Maintain updated cyber security policies and guidelines.
- Conduct regular Vulnerability Assessment and Penetration Testing (VAPT) and compliance of the same.
- Quick response on Security Operations Centre (SOC) reported incidents.
- Deploy Endpoint security tools like EDR/UEM.
- Maintain secure backup policy.
- Conduct regular cyber security awareness programmes for the govt. officials and spread awareness among general public by means of posters/banners.
- Periodically review of cyber risks identified.
- Ensure compliance with Government cyber security advisories from time to time.
- Periodic review and updation of CCMP, BCP and BIA documents as part of the organization's cyber preparedness and resilience planning framework.

## 2. Employee Responsibilities

- Follow Ministry cyber security policies.

- Protect official sensitive information and credentials.
- Use strong passwords with complexity as per guidelines.
- Avoid use of Administrator account for routine work.
- Report cyber incidents immediately to competent authority.
- Use only authorized devices in official network.
- Complete mandatory cyber security training.
- Handle official information responsibly.
- Strictly follow Admin and USB usage policies.
- Avoid installation of unauthorized/unapproved software
- Keep their systems updated.
- Scan systems periodically through approved EDR tool.

### 3. Citizen Responsibilities

- Use strong passwords with complexity mentioned in guidelines.
- Enable Multi-Factor Authentication wherever possible.
- Never share OTPs or passwords. Keep it safe and confidential.
- Verify Ministry websites before entering personal information.
- Keep computers and mobile devices updated.
- Install genuine antivirus software.
- Avoid using public computers for sensitive transactions.
- Log out after using the services.
- Don't use public Wifi to access websites.
- Avoid downloading files from untrusted sources.
- Beware of any fraudulent emails sent in the name of ministry.
- Report suspicious emails and fake websites to competent authority.
- Immediately report any suspected cyber incident.

#### ➤ Awareness Initiatives

- Organized cyber awareness campaigns.
- Conducted employees training.
- Issued cyber advisories on regular bases through e-Office/websites/physical banners and standees at strategic locations.
- Celebrated Cyber Security Awareness Month with rewards to employees following best practices.

#### ➤ Citizen can report about following:

- Website defacement
- Phishing emails
- Fake/Cloned Ministry websites
- Identity theft
- Unauthorized access
- Data leakage
- Malware infections
- Online fraud involving Ministry services

Reports may be submitted through:

- \*Official email
- \*Telephone support

#### ➤ \* Official email/ Telephone support in case of cyber Incident

**CISO, MIB**

Email: [rk.jena@gov.in](mailto:rk.jena@gov.in) / 011-24015809

|                                              |                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Dy. CISO, MIB</b>                         | Email: <a href="mailto:dciso-cstmoib@nic.in">dciso-cstmoib@nic.in</a> / 011-24305000 Ext. 65531                                                                                                                                                                                                                                                           |
| <b>NIC team</b>                              | Email/Telephone: <a href="mailto:hod-iandb@nic.in">hod-iandb@nic.in</a> / 011 24366505<br><a href="mailto:officer1.iandb@nic.in">officer1.iandb@nic.in</a> / 011-24015828<br><a href="mailto:officer3.iandb@nic.in">officer3.iandb@nic.in</a> / 011-2338 5256 Ext. 222<br><a href="mailto:officer4.iandb@nic.in">officer4.iandb@nic.in</a> / 011-24369572 |
| <b>Certi-In</b><br><br><b>NIC-Cert</b>       | Email: <a href="mailto:incident@cert-in.org.in">incident@cert-in.org.in</a><br>Toll Free no.: +91-1800-11-4949<br><br>Email: <a href="mailto:incident@nic-cert.nic.in">incident@nic-cert.nic.in</a><br>Phone: 011-24305114/24305116 (24x7)                                                                                                                |
| <b>National Cyber Crime Reporting Portal</b> | Website: <a href="https://cybercrime.gov.in">https://cybercrime.gov.in</a><br>Helpline No.: 1930                                                                                                                                                                                                                                                          |

## ➤ Continuous Improvement

The Ministry shall periodically review this Charter based on:

- Emerging cyber threats
  - Citizen feedback
  - Security audits
  - Government guidelines
  - Technological advancements
- 

## ➤ Important links for Government issued guidelines and advisories

- <https://www.cert-in.org.in/s2cMainServlet?pageid=GUIDLNVIEW01>
  - <https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2024-0050>
  - <https://i4c.mha.gov.in/newsletter-manual.aspx>
- 

The Ministry of Information and Broadcasting is committed to maintaining a secure digital environment and delivering trusted, resilient, and citizen-centric digital services while protecting citizens' information and continuously improving cyber security practices.

---