CITIZEN'S CHARTER

FOR CYBER SECURITY

Ministry of Housing and Urban Affairs

INDEX

Section	Item/Subject	Page No.
1.	Introduction	3
2.	Cyber Security Division	4
3.	Cyber Incident Reporting	5
4.	Best Practices: DOs	6
5.	Best Practices: DON'Ts	7
6.	User Awareness and Digital Empowerment	8
7.	Guidelines	9

1. Introduction

In the digital era, cyber security has become a critical necessity to protect sensitive data, infrastructure, and digital identities from unauthorized access, cyber-attacks, and data breaches. As cyber threats continue to evolve, the need for widespread awareness is more crucial than ever.

Human as the Weakest Link: Most cyber incidents occur due to lack of awareness or human error.

Cyber security is not just a technical issue but a shared responsibility that involves governments, organizations, and individuals. Raising awareness is fundamental to creating a secure digital environment. Continuous education, training, and engagement are essential to prevent cyber threats and promote a resilient cyber ecosystem.

2. Cyber Security Division

CHIEF INFORMATION SECURITY OFFICER (CISO):

Sh. PRAVEER KUMAR

Joint Secretary

Ministry of Housing and Urban Affairs,

Government of India, New Delhi

Email: jsnudm-mohua@gov.in, ciso-mhua@nic.in

DIRECTOR (CISO MATTERS):

Sh. RAGHVENDRA PAL SINGH

Director

Ministry of Housing and Urban Affairs,

Government of India, New Delhi

Email: raghavendra.singh@gov.in

DEPUTY CISO:

Shri Amit Saxena

Director (IT)

Email: dciso-cstmhua@nic.gov.in

3. Cyber Incident Reporting

Computer Emergency Response Team (CERT-In)

Email: incident@cert-in.org.in

Helpdesk: +91-1800-11-4949

Url: https://www.cert-in.org.in/

Incident Reporting form: Link

CyMAC (Cyber Multi-Agency Centre) Control Room (Ministry of Home Affairs).

Email: cycordadmin.mha@gov.in

Landline: 011-23094060

CISO Office

Email: ciso-mhua@nic.in, dciso-cstmhua@nic.gov.in

Landline: 011-24011283

4. Best Practices: DOs

- Use Strong Passwords
  - At least 12–14 characters, mix of uppercase, lowercase, numbers, and special characters.
  - Change passwords regularly and avoid reuse.
- Enable Multi-Factor Authentication (MFA)
  - Always activate MFA where available for critical accounts (email, banking, portals).
- Keep Systems Updated
  - Regularly install OS, application, and antivirus updates/patches.
- Use Only Authorized Software
  - Install apps/software only from trusted sources or official app stores.
- Lock Devices When Not in Use
  - Use screen locks, auto-lock timers, and secure logins.
- Backup Data Securely
  - Maintain regular backups on secure and encrypted storage.
- Report Suspicious Activity
  - Immediately inform the IT/security team about phishing emails, suspicious links, or abnormal device behaviour.
- Be Aware of Phishing
  - Verify sender before clicking links or downloading attachments.
- Secure Your Network
  - Use VPN when on public Wi-Fi.
  - Change default router passwords.
- Follow Organizational Security Policies
  - Adhere to IT policies, incident reporting guidelines, and acceptable use norms.

5. Best Practices: DON'Ts

- Don't Share Passwords
  - Never share login credentials with colleagues, friends, or family.
- Don't Use Default or Weak Passwords
  - Avoid using "123456," "password," or personal details (DOB, phone number).
- Don't Ignore Security Warnings
  - Browser or antivirus warnings should not be bypassed.
- Don't Leave Devices Unattended
  - Especially in public areas or while logged into sensitive systems.
- Don't Download from Untrusted Sources
  - Pirated software and unknown apps may contain malware.
- Don't Click on Unknown Links/Attachments
  - Phishing emails often look genuine – always verify first.
- Don't Use Public Wi-Fi Without Protection
  - Avoid accessing sensitive accounts on free/open Wi-Fi.
- Don't Disable Security Features
  - Firewalls, antivirus, or encryption should always remain enabled.
- Don't Connect Unauthorized USB Devices
  - External storage can spread malware or lead to data theft.
- Don't Post Sensitive Information Online
- Avoid oversharing personal or organizational data on social media.

6. User Awareness and Digital Empowerment

The following links may be visited for latest information on awareness:

1. **InfoSec Awareness** through workshops and trainings to make citizens aware about internet ethics, online frauds, etc. For more information, please click this link.

2. **Cyber Aware Digital Naagrik Programme**: ISEA is a user-specific cyber awareness programme that aims to educate Digital Naagrik about safe and secure digital practices through mass awareness, user engagement and role-based awareness progression. For more information, please click this link.

3. **Cyber Swachhta Kendra (CSK)**
   Security Best Practices: https://www.csk.gov.in/security-best-practices.html
   Security Tools: https://www.csk.gov.in/security-tools.html

4. **Indian Cybercrime Coordination Centre (I4C, MHA)**
   Report Cyber Crime at: https://cybercrime.gov.in/ or call "**1930**"

5. **Sanchar Saathi, DoT**
   Telecom and information security
   Report at: https://sancharsaathi.gov.in/

7. Guidelines

The following sources may be visited for latest guidelines:

- CERT-In Guidelines:

  https://www.cert-in.org.in/s2cMainServlet?pageid=GUIDLNVIEW01

- CERT-In Advisories:

  https://www.cert-in.org.in/s2cMainServlet?pageid=PUBADVLIST

- CERT-in Information Desk:

  info@cert-in.org.in

- Act/Rules/regulations:

  https://www.cert-in.org.in/s2cMainServlet?pageid=AUTHORITY