



Central Warehousing Corporation

(A Government of India Undertaking)

**Under Ministry of Consumer Affairs, Food &
Public Distribution**

CITIZEN'S CHARTER FOR CYBER SECURITY

This Charter outlines the foundational principles and strategic directives guiding our nation's commitment to a secure digital future. It establishes a unified framework for protecting critical infrastructure, safeguarding sensitive information, and fostering a resilient cyber ecosystem across all government agencies and national partners.

INDEX

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

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.

CYBER SECURITY DIVISION



CHIEF INFORMATION SECURITY OFFICER (CISO):

Shri Anil Manik Rao

Group General Manager

MIS Division

Central Warehousing Corporation

Email: ggmsystem@cewacor.nic.in

Tel: 011-26515178

DEPUTY CISO:

Shri Gautam Kumar Das

Deputy General Manager

MIS Division

Central Warehousing Corporation

Email: gautam.das@cewacor.nic.in

CYBER INCIDENT REPORTING

1 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](#)

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

Email: cycordadmin.mha@gov.in

Landline: 011-23094060

3 CISO Office

Email: ggmsystem@cewacor.nic.in, gautam.das@cewacor.nic.in

Landline: 011-26515178

4 Cyber Crime Reporting (I4C)

Report at: cybercrime.gov.in

Call: 1930

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 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

- Inform IT/security team immediately about phishing emails, suspicious links, or abnormal device behavior.



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.

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.

USER AWARENESS AND DIGITAL EMPOWERMENT

- 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/>

IMPORTANT REFERENCE LINKS

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>