



Warehousing Development and Regulatory Authority भांडागारण विकास और विनियामक प्राधिकरण

**Government of India
Ministry of Consumer Affairs,
Food & Public Distribution**

CITIZEN'S CHARTER FOR CYBER SECURITY

This Charter sets forth the foundational principles and strategic directives underpinning WDRA's commitment to a secure and resilient digital future. It establishes a unified framework for the protection of critical infrastructure, the safeguarding of sensitive information, and the cultivation of a robust cyber ecosystem across the organization and its stakeholders.

INTRODUCTION

In the digital era, cybersecurity has become an essential pillar for safeguarding sensitive data, critical infrastructure, and digital identities from unauthorized access, malicious attacks, and data breaches. As cyber threats grow in sophistication and frequency, fostering widespread awareness and collective responsibility is more important than ever to ensure a secure and resilient digital environment.

Cybersecurity is not merely a technical issue but a shared responsibility that encompasses governments, organizations, and individuals alike. Raising awareness is fundamental to establishing a secure digital environment, while continuous education, training, and active engagement are essential to mitigating cyber threats and fostering a resilient cyber ecosystem.

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

CYBER SECURITY DIVISION



CHIEF INFORMATION SECURITY OFFICER (CISO):

Dr. Ashish Kumar

Director (IT)

Warehousing Development and Regulatory Authority (WDRA), New Delhi

Email: dirit-wdra@gov.in

Tel: (011)-49536496 (Ext. 19)

CYBER INCIDENT REPORTING

Computer Emergency Response Team (CERT-In)

1

Email: incident@cert-in.org.in

Helpdesk: +91-1800-11-4949

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

Incident Reporting form: <https://www.cert-in.org.in/PDF/certinirform.pdf>

2

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

Email: cycordadmin.mha@gov.in

Landline: 011-23094060

3

CISO Office

Email: drit-wdra@gov.in

Cyber Crime Reporting (I4C)

4

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>