भारत सरकार

GOVERNMENT OF INDIA

विज्ञान और प्रौद्योगिकी मंत्रालय

MINISTRY OF SCIENCE AND TECHNOLOGY

जैव प्रौद्योगिकी विभाग

DEPARTMENT OF BIOTECHNOLOGY

CITIZEN'S CHARTER FOR CYBER SECURITY

INDEX

INTRODUCTION

In the digital era, cyber security is vital to safeguard sensitive data and personal information from unauthorized access, cyber-attacks, and data breaches. 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 to promote a resilient cyber ecosystem.

This Citizen's Charter for Cyber Security outlines the mechanisms to strengthen cyber security practices and to safeguard digital data & communication networks pertaining to Department of Biotechnology against cyber threats. It aims to sensitize employees of the Department about safe digital practices and to raise awareness on efficient mechanisms for reporting and responding to cyber incidents.

CYBER SECURITY CELL, DBT

Name	Designation	Email Id
Sh. Sankarsana Sahoo	Statistical Advisor & CISO	advisor-stat@dbt.nic.in
Sh. Ajay Kumar Tayal	Scientist-E & Dy. CISO	dciso-ctmost@nic.in

CYBER INCIDENT REPORTING FRAMEWORK

1. **Computer Emergency Response Team (CERT-ln)**
   Email: incident@cert-in.org-in
   Helpdesk: +91-1800-11-4949
   URL: https://www.cert-in.org-in

2. **CyMAC (Cyber Multi-Agency Centre) Control Room**
   (Ministry of Home Affairs)
   Email: cycordadmin.mha@gov.in
   Landline: 011-23094060

3. **Cyber Crime Reporting (I4c)**
   Report at: cybercrime.gov.in
   call: 1930

4. **CISO Cell (DBT)**
   Email: advisor-stat@dbt.nic.in, dciso-cstmost@nic.in
   Landline: 011-24363656

DOs (DATA SECURITY)

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 (DATA SECURITY)

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 Programe:**

   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