कर्मचारी राज्य बीमा निगम
(श्रम एवं रोजगार मंत्रालय, भारत सरकार)
EMPLOYEES' STATE INSURANCE CORPORATION
(Ministry of Labour & Employment, Govt. of India)

सत्यमेव जयते

उप क्षेत्रीय कार्यालय,ठाणे
प्लॉट: ए-12/1, एम आई डी सी, एल बी एस मार्ग,
वागले इस्टेट डाकघर के पास, ठाणे (प.), महाराष्ट्र-400604
Sub Regional Office, Thane
Plot No.-A-12/1, MIDC, LBS Marg, Next to Wagle Estate
Post Office, Thane(W), Maharashtra-400604
Telephone- 022-69074700 to 799
Email: dir-thane@esic.nic.in, Website: -esic.nic.in

सं.:**34/T/Facility & ICT/Compliance Report Cyber Security/24** दिनांक: 08-01-26

परिपत्र Circular

विषय Sub: साइबर सुरक्षा दिशानिर्देश Cyber Security Guidelines

Information and communication technologies (I. C.T) have become ubiquitous amongst government ministries and departments across the country. The increasing adoption and use of ICT has increased the cyber-attacks and threat perception to government, due to lack of adoption of proper cyber security measures on the ground. In order to sensitize the government employees, contractual /outsourced resources and build awareness amongst them on DO'S and DON'TS on cyber-security perspective, these guidelines have been compiled. Strict adherence of these uniform cyber security guidelines is required to be followed by all the employee including contractual/outsourced who are under the jurisdiction of SRO Thane to ensure a proper secured environment for ESIC to carry out the Scheme activities.

साइबर सुरक्षा क्या करें CYBER SECURITY DO'S

Use complex passwords with a minimum length of 10 characters, using a combination of capital letters, small letters, numbers and special characters.

1. Do use hard-to-guess passwords or passphrases.
2. Change your passwords at least once in 45 days.
3. Always change the password from a computer which is Virus/malware free.
4. Use multi-factor authentication, wherever available such as **Kavach** authentication for email.
5. Save your data and files on the secondary drive (ex: d:\).
6. Maintain an offline backup of your critical data. Regular backups of important data are to be done as per standards.
7. When you leave your desk temporarily, always lock/log-off from your computer session. Do lock your computer, Laptops and mobile phone when not in use. This protects data from unauthorized access and use.
8. When you leave office, ensure that your computer and printers are properly shutdown
9. Keep the GPS, Bluetooth, NFC and other sensors disabled on your computers and mobile phones. They maybe enabled only when required.
10. Wireless communication is inherently insecure. Security protocols and selective access control must be ensured based on roles and responsibilities
11. While sending any important information or document over electronic medium, kindly encrypt the data before transmission. You can use a licensed encryption software or an Open PGP based encryption or add the files to a compressed zip and protect the zip with a password. The password for opening the protected files should be shared with the recipient through an alternative communication medium like SMS, Sandes etc.
12. Observe caution while opening any shortened uniform resource locator (URLs) (ex: tinyurl.com/ab534/). Many malwares and phishing sites abuse URL shortened services.
13. Observe caution while opening any links shared through SMS or social media, etc., where the links are preceded by exciting offers/discounts, etc., or may claim to provide details about any current affairs. Such links may lead to a phishing/malware webpage, which could compromise your device.
14. Report suspicious emails or any security incident to incident@cert-in.org.in, incident@nic-cert.nic.in and to your authority/head of division immediately.
15. Adhere to the security advisories published by NIC-CERT (https://niccert.nic.in/advisories.jsp) and CERT-In (https:/Iwww.cert-in.org.in).
16. Always ensure that the "REMEMBER PASSWORD "option isn't configured anywhere i.e. in the browser or in IMAP/POP mail client i.e. Outlook, Thunderbird, seamonkey, Windows Mail etc
17. Every system/computer/laptop used in workplace environment must be password protected.
18. Two factor authentications (such as KAVACH) must be used to access emails by all. Password for mail ID must not be shared with anyone.
19. If system is found to be infected with any virus/malware/phishing software: -
    a) Disable IMAP service in KAVACH for all users (both in desktop and mobile client).
    b) Disconnect the infected computers from LAN/ internet immediately.
    c) Hard disks of the infected computers may be formatted after taking backup of data files;
    d) Operating systems and applications should be re-installed from clean and updated software
    e) Backup data should be scanned for virus before restoring it;
    f) Educate colleagues and other staff about security policy and related information(s).

साइबर सुरक्षा क्या न करें CYBER SECURITY DON'T

1. Don't use the same password in multiple services/websites/apps.
2. Don't share the password with anyone. The password must not be shared with others, whether you know them or not. Do keep your passwords or passphrases confidential. You are responsible for all activities associated with your credentials.
3. Don't save your passwords in the browser or in any unprotected documents.
4. Don't write down any passwords, IP addresses, network diagrams or other sensitive information on any unsecured material (e.g.: sticky/post-it notes, plain paper pinned or posted on your table, etc.)
5. Don't save your data and files on the system drive (e.g.: c:\ or root).
6. Don't upload or save any internal/restricted/confidential government data or files on any non-government cloud service (e.g. Google Drive, Dropbox, etc.).
7. Don't connect official computer/laptop and any other device with private network (Mobile Hotspot)
8. Nobody should use any private mail ID for communications for official purposes, from official Computers, systems or Laptops. All officials must use official e- Mails ending with gov.in (nic.in), etc.
9. Don't use personal work on official systems.
10. Don't plug in portable devices such as pen drive, etc., without permission from ESI management. These devices may be compromised with code just waiting to launch as soon as you plug them into a computer.
11. Don't connect any other site (unrelated to official requirement) on official system.
12. Don't use any 3rd party DNS Service or NTP Service.
13. Don't use any 3rd party anonymization services (e.g.: Nord VPN, Express VPN, Tor, Proxies, etc.).
14. Don't use any 3rd party toolbars (e.g.: download manager, weather tool bar, ask me tool bar, etc.) in your internet browser.
15. Don't install or use any pirated software (e.g.: cracks, keygen, etc.).
16. Don't open any links or attachments contained in the emails sent by any unknown sender.
17. Don't share system passwords or printer passcode or Wi-Fi passwords with any unauthorized persons.
18. Don't disclose any sensitive details on social media or 3rd party messaging apps.
19. Don't plug-in any unauthorized external devices, including USB drives shared by any unknown person
20. Don't use any unauthorized remote administration tools (e.g.: TeamViewer, Ammy admin, Any desk, etc.)
21. Don't use any external email services for official communication.
22. No unverified or untrusted links or websites must be accessed at any time.
23. Don't jailbreak or root your mobile phone.
24. Don't use any external mobile App based scanner services (e.g.: Cam scanner) for scanning internal government documents.
25. Don't use any external websites or cloud-based services for converting/compressing a government document (ex: word to pdf or file size compression)
26. Don't share any sensitive information with any unauthorized or unknown person over telephone or through any other medium.
27. Avoid using public Wi-Fi hotspots.
28. Don't leave wireless or Bluetooth turned on when not in use. Only do so when planning to use and only in a safe environment

अस्थायी, संविदा/आउटसोर्स मानव संसाधनों सहित सभी क.रा.बी. निगम के कार्मिकों को उपर्युक्त दिशानिर्देशों का सख्ती से पालन करना आवश्यक है।

All ESIC employees including temporary, contractual/outsourced resources are required to strictly adhere the guidelines mentioned above.

यह संयुक्त निदेशक (प्रभारी) के अनुमोदन से जारी किया गया है।

This issues with the approval of Joint Director (I/c).

Digitally signed by GEETANJALI ANTIL
Date: 08-01-2026 11:19:53

सहायक निदेशक/ Asst. Director

(सुविधा एवं सूचना तथा संचार प्रौद्योगिकी शाखा Facilitation & ICT)

सेवा में To,

1. सभी उप/सहायक निदेशक, उप क्षेत्रीय कार्यालय, ठाणे।
   All Deputy/Assistant Directors, Sub Regional Office, Thane.
2. सभी शाखा अधीक्षक/सा.सु.अधिकारी, उप क्षेत्रीय कार्यालय, ठाणे।
   All Branch Superintendents/SSOs, Sub Regional Office, Thane.
3. सभी डीसीबीओ प्रभारी/शाखा प्रबंधक, अधीनस्थ डीसीबीओ/शाखा कार्यालय, उप क्षेत्रीय कार्यालय, ठाणे।
   All DCBO Incharges/Branch Managers, subordinate DCBOs/Branch Offices, Sub Regional Office, Thane.
4. सभी शाखाएं/शाखा कार्यालय/औषधालय सह शाखा कार्यालय, उप क्षेत्रीय कार्यालय, ठाणे।
   All Branches/Branch Offices/DCBOs, Sub Regional Office, Thane.
5. वेबसाइट प्रबंधक/आईसीटी शाखा, उप क्षेत्रीय कार्यालय, ठाणे को वेबसाइट पर अपलोड करने हेतु।
   Website Manager/ICT Branch, Sub Regional Office, Thane to upload on website.