OFFICE OF THE
CHIEF ELECTORAL OFFICER: MANIPUR
***

www.ceomanipur.nic.in
Telefax : 0385-2414239/2414859
Email: ceo_manipur@eci.gov.in
jtceo_manipur@eci.gov.in

A D D E N D U M
Imphal, the 6th February 2024

No. e-Roll-101/1/2022-ELEC-ED: - In continuation of this office notification of even number dated 05.02.2024 regarding the bids for the supply of personalized pre-printed colour PVC EPIC, an addendum has been incorporated as per Election Commission of India's letter No.23/INST/2024-ERS dated 05.02.2024. The addendum may be viewed from the following link **www.ceomanipur.nic.in**

Binod Salam 6/2/2024

(Binod Salam)
Assistant Chief Electoral Officer, Manipur

Copy to:-

1. Commissioner -cum- Secretary (Election), Government of Manipur.
2. Relevant e-file.

***

ELECTION COMMISSION OF INDIA

Nirvachan Sadan, Ashoka Road, New Delhi-110001

No. 23/INST/2024-ERS Dated: 5th February, 2024

To,

The Chief Electoral Officers
Of all States/Union Territories.

Subject: Standard Operating Procedure (SOP) for printing of EPIC with new security features- regarding.

Ref: 1. ECI letter No. 23/EPIC Security/2021-ERS, dated 18th January 2022
2. ECI letter No. 23/EPIC Security/2021-ERS, dated 19th May 2022

Sir/Madam,

I am directed to refer to the Commission's above-cited letters and to state that the Commission has introduced EPICs with new security features in the year 2022 and Chief Electoral Officers of all States/UTs were instructed to select "Colour PVC Card –cum-Security Printer ", having in-house printing facilities on PVC sheet incorporating security features and personalisation capacity. Further, detailed instructions on security feature and other specification/dimension of such secured PVC EPIC were issued by the Commission vide its letter dated 19th May 2022, referred to above.

2. It has been observed that in the absence of specific protocol for transaction and handling of data between the senders (at the level of electoral authority) and the printing agency for printing of EPIC, there has not been uniform pattern of following security protocols for printing of EPICs in all the States. Further, it has been noticed that in some States, the Electoral Registration Officer(ERO) directly sends the EPIC pdf to the Printing Agency without taking respective Chief Electoral Officer (CEO) in the loop, whereas, in some other States CEO collates the EPIC pdf from all the EROs and sends the data to the Printing Agency. In most of the States, District Election Officer (DEO) is not in the loop at all.

3. The Commission, after taking all aspects into consideration and with a view to strengthen the security protocol for the purpose of printing of secured EPICs, has formulated Standard Operating Procedure (SOP) to be followed in States/UTs at each and every stages prescribed therein, irrespective of whether data transmission is done at the level of EROs/DEOs/CEO.

4. A copy of SOP for printing of EPICs is enclosed herewith. All the Chief Electoral Officer are requested to ensure that SOP, as laid down by the Commission is strictly followed.

5. CEOs of all States and UTs shall implement the security protocol, including third party audit of printing agency's system and premises to ensure Quality Assurance and Quality Control, as mentioned in the enclosed SOP, by **20th February 2024 (Tuesday)** and send a compliance report to the Commission immediately thereafter.

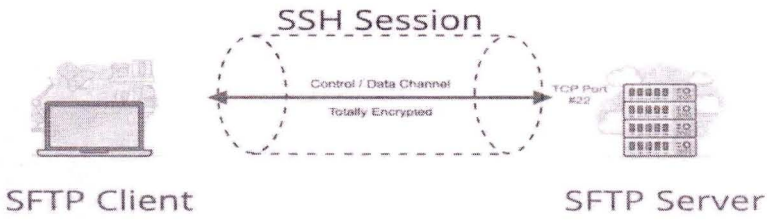
Yours faithfully,

(PAWN DIWAN)
SECRETARY

SOP for Printing of EPIC with new security features

1. Only DEO or maximum one more person duly authorized by DEO, shall be designated to transfer the data to the printing agency.

2. The Data from the DEO to the printing agency shall be transferred in SFTP (Secured File Transfer Protocol) format only to ensure encrypted communication protocols for data transfer. The same can be given in the pictorial Diagram as below:



3. Security measures to be followed by DEOs/Designated Officers while transferring data:

After generating EPIC PDF through ERO Net printing tool, the ERO shall transfer the same to DEO in SFTP format for its further transmission to the printing agency. The DEO/Designated Officer should follow protocol as detailed under while transferring the data to the printing agency:

i. The DEO shall use their login credentials (user/password) for the system and preferably this system access may have biometric access to avoid use by any other person.

ii. In advance, the printing agency shall inform the DEO of the credentials of the authorized person who will be responsible to receive the data through SFTP.

iii. The system at DEO's end being used for EPICs pdf transfer shall have all security measures including Antivirus, Firewall, hardening of system etc.

iv. A dedicated system shall be used for this purpose, which shall not be used for internet access in general.

v. The IP addresses/path of the computer system to be used at the both ends, i.e.DEO and printing agency should be well defined and non-violable.

vi. Both the authorised sender (DEO) and receiver at the printing agency side shall be responsible to ensure all security protocols laid down in the data handling norms as prescribed by ECI and Meity from time to time.

vii. The computer system at the sender's and receiver's end shall be regularly updated and patched the software to address security vulnerabilities.

4. Access Control:

The sender and receiver shall ensure the following:

i. Enforce access controls to limit data transfer, printing, and deletion rights.

ii. Implement role-based access to restrict privileges based on job responsibilities.

iii. Regularly review and update access permissions to align with organizational changes.

5. Password Policy:

A password policy by both DEOs and Printing Agency shall at least follow with following features:

i. There should be two Factor authentication (Password & Biometric) for system.

ii. Password must contain minimum 8 characters at least 1- Uppercase Alphabet, 1 Lowercase Alphabet, 1 Number and 1 Special Character.

iii. Password needs to be mandatorily changed after 90 days.

iv. New password shall not match with the last three passwords.

v. In case of five times wrong entry of password, user should be blocked.

6. Hardening of System:

The sender and receiver shall ensure:

i. that all software installed with genuine copy of operating system and other application software solutions. Pirated or unsupported OS/software shall NOT be installed on official systems.

ii. the installation of reputed Antivirus/EDR software on all the systems with regular signature updates.

iii. to Set/enable BIOS Password at system boot. Enable disk encryption policy on laptop/mobile devices, if possible.

iv. to enable standard user (non-administrator) accounts for all users on all office systems used for regular work. Admin access shall be given to limited users on requirement with approval of competent authority. For day-to-day work / operations use standard user account / privileges and use the admin privilege only for specific tasks wherever applicable. Disable Guest user on all office systems.

v. to install only whitelisted software on office systems based on the roles of the users. Do not allow installation of Tor browsers or such anonymizer plug-ins for standard web-browsers.

vi. not to allow peer-to-peer file sharing application to be installed on office systems or to communicate with outside internet.

vii. that external USB storage devices (i.e., pen drive, memory cards, hard disk, mobile phone storage etc.) shall NOT be allowed, only authorized USB storage devices (approved by department) shall be allowed on official systems based on the roles & requirements of the user.

viii. to enable system level firewall.

ix. to enable system level user password policy (password complexity & password expiry)

x. to make a policy regarding timely update of firmware, operating systems and other software should be formed and strictly enforced. Products, which have reached end of support, should NOT be used in office network.

7. Physical security:

There shall be a proper physical security protocol at the premises where servers have been installed at the ends of both DEOs and Printing Agency, having at least following checks:

i. Round the clock security provision;

ii. CCTV surveillance Cameras at all strategic location (both inside and outside the premise) with 30 days recording facilities;

iii. Entry only through biometric/Card punching system.

8. Secure Printing at Printing Agency:

i. A dedicated resource person should be appointed by the printing agency and the details of such person should be immediately intimated to DEO and only that person shall be allowed to use system at printing agency. He/she shall use his/her login credentials (user/password) for the system and preferably this system access shall have biometric access to avoid use by any unauthorized person.

ii. The system at the end of printing agency being used for receiving and printing of EPICs pdf shall have all security features including Anti-virus, Firewall etc. as per the standards defined by Ministry of Electronics and Information Technology (Meity) and shall not be used for internet access in general.

iii. Printing agency shall establish a secure printing environment with restricted access of the area where printing work is executed.

iv. Printing Agency shall ensure print release mechanisms to ensure confidentiality.

v. Printing Agency shall regularly audit and monitor print logs for any unauthorized activity.

vi. Printing Agency shall take appropriate steps to ensure the security and prevention of misuse of data.

vii. Printing agency should ensure that there is no deviation of any provisions of MoU/agreement signed by the printing agency.

viii. As the Intellectual Property Right of the EPIC data given to printing agency lies with CEO/ECI and therefore, the given data should not be copied in any form, not shown/given to any entity, not retained in any form, not used for the purpose other than the purpose mentioned in the agreement etc. by the printing agency.

9. Security of Printing machine:

The printer being used for the printing of EPICs shall not be connected to network preferably, however, if the printer is connected to network, then the printing agency shall–

i. disable default credentials on printers.

ii. disable default services (i.e. FTP, HTTP, SSH, SMB, Telnet etc.) on printers, if not in use and enable security if using any of these services for managing printer remotely.

iii. restrict internet access for all printers, cloud-printing etc. and enable Stricter User Access Controls.

10. Permanent Deletion/Disposal

i. Printing agency shall ensure that data to be erased entirely once the matter of the lot of supply is materialized/settled. Printing agency shall submit a certificate in this regard to the DEOs.

ii. Printing agency shall use secure deletion methods, like overwriting data with random patterns.

iii. Printing agency shall implement secure file shredding tools to ensure unrecoverable deletion.

iv. Printing agency shall train their staff on proper procedures for permanently deleting sensitive information.

v. Printing agency shall ensure regular audit and track deletion activities to ensure compliance.

vi. Printing agency should ensure that unused/defected PVC EPIC be disposed of immediately on daily basis by way of shredding and a certificate to the effect that such material has been disposed of, and shall furnish certificate to this effect to the DEO concerned along with the printed lot of the EPICs.

11. Employee Training:

i. Printing agency should conduct regular training sessions on secure data handling practices.

ii. Printing agency should ensure that employees understand the importance of data security in transfer, printing, and deletion processes.

iii. Printing agency should provide clear guidelines on handling sensitive information to prevent inadvertent breaches.

12. Incident Response:

i. Printing agency should develop a robust incident response plan for any security breaches.

ii. Printing agency should establish a reporting mechanism for employees to notify security incidents promptly.

iii. Printing agency should conduct regular drills to test the effectiveness of the incident response plan.

iv. Printing agencies and other officials, who are handling such data, shall be suitably advised and cautioned that any unauthorized release of data to any person/agency will be liable for severe action against the vendor/person/ officer/ operator responsible for the same. Strict measures shall be put in place to steer clear of any attempts to make Electoral Roll Data available in an unauthorized manner to certain quarters.

v. Any breach of security while handling and sharing of electoral data/database and misuse of such data by any **unscrupulous/unauthorized means, if noticed/ brought to the notice of the electoral authority, FIR shall be lodged** immediately by the Concerned DEO, wherever required, after assessment of severity of impact and damages caused due to such illegal activities. A copy of FIR, so lodged along with a brief incidence shall also be sent to the Commission for its information by the respective Chief Electoral Officer.

vi. Remember to customize these guidelines based on the organization's specific needs and security policies. Regularly review and update the SOP to adapt to evolving security threats and technologies.

13. Agreement arrangement:

A proper agreement between state (CEO) and Printing agency shall be defined and signed as per draft RFP defined by ECI and incorporating the SoP defined here:

i. No Copy & Deletion of data: The EPICs shall be printed from the system where these have been downloaded and no copy shall be made of EPIC data. All the data shall be permanently deleted after printing of the same. A certificate shall be provided to DEOs in this regard on monthly basis.

ii. Provision of Inspection: Inspection shall be conducted by a team of officers designated by CEO, to check security arrangements, infrastructure, machines and equipment, personnel as per the agreement any deviations may result in immediate disqualification.

iii. It should be made clear to the printers that any breach of security of data, or its misuse, would invite severe punitive action.

iv. A Non-Disclosure Agreement shall be defined as per standard format of ECI (Annexure -1).

v. Third Party Audit: CEOs shall engage an agency (STQC, C-DAC) or any agency empanelled under Meity) for the audit of printing agency's system and premises to ensure Quality Assurance and Quality Control.

****

Annexure -1

EMPLOYEE NON-DISCLOSURE AGREEMENT

This Agreement ("Agreement") is made and entered into on this [ ] day of [ ], 2023 ("Effective Date"), by and between Ltd. ("Company"), an Indian company with its principal place of business at ; and ("Employee"), with an address at .

For good consideration, and in consideration of being employed by the Company, the undersigned Employee hereby agrees and acknowledges as follows:

1. That during the course of my employment by the ------- Company and deployment at Election Commission of India, there may be disclosed to me certain confidential information of the Election Commission of India; said confidential information consisting but not necessarily limited to:
    a. Technical information: Methods, processes, systems, techniques, technical know-how, inventions, machines, computer programs and research projects.
    b. Other information: Operational process, security arrangements and administrative/organisational matters, documents including electronic ones etc.
2. That I shall not during, or at any time after the termination of my employment with TCS, use for myself or others, or disclose or divulge to others, including future employees, any confidential information or any other proprietary data of the Election Commission of India, in violation of this Agreement.
3. Upon the termination of my employment from TCS:
    a. I shall return to the Election Commission of India all documents and property of the ECI, including but not necessarily limited to drawings, blueprints, reports, manuals, correspondence, computer programs, and all other materials and all copies thereof relating in any way to the ECI's activities, or in any way obtained by me during the course of the engagement. I further agree that I shall not retain copies, notes or abstracts of the foregoing.
    b. TCS may notify any future or prospective employer or third party of the existence of this Agreement and shall be entitled to full injunctive relief for any breach.
4. That this Agreement shall be binding upon me and my personal representatives and successors in interest and shall inure to the benefit of TCS, its successors and assigns.
5. That I shall indemnify TCS against any and all losses, damages, claims, or expenses incurred or suffered by TCS, whether directly or indirectly, including reasonable attorney's fees and costs, resulting from my breach of this Agreement.
6. This Agreement shall remain in full force and effect with respect to the confidential information without limitation of time.
7. This Agreement shall be governed by and construed under the laws of India.

Signed this _____ day of _____, 2024__.

_____ _____

Company Employee