F.No. 1/12/2018 VS (CRS)
GOVERNMENT OF INDIA
MINISTRY OF HOME AFFAIRS
OFFICE OF THE REGISTRAR GENERAL, INDIA
V.S. Division, West Block –I, R.K. Puram, New Delhi-110066
E-mail: drg-crs.rgi@nic.in

Dated 24th Dec., 2021

To,

The Chief Registrars of all States/UTs

Subject: Advisory regarding registration of births and deaths.

Sir/Madam,

Please refer to this office letter of even number dated 28th July 2021 (copy attached) vide which an advisory was issued to all states/UTs for taking precautionary measures in registration of births and deaths in order to avoid misuse of online portal credentials i.e. User ID and password. In said advisory, the State governments and Administrators were requested to issue necessary instructions to all the registration authorities, not to share password with any person, periodically change the password and update the credentials in the existing portal/ software developed for online registration of birth and deaths. The said advisory was followed by a reminder dated 29th September, 2021 and in this context, a Press Note was also issued in October, 2021.

2. In spite of aforesaid instructions, it has come to the notice of this office that some unauthorized persons, by misusing Login ID/ Passwords, have issued fake birth/death certificates in few cases through online portal/website. Also, few instances have been reported that existing portal/software developed for online registration of birth and death has come under phishing attacks. Thus, fake portal/websites have been designed with the aim to steal and misuse User/Login ID and password for issuance of fake birth and death certificates. Consequently, some criminal cases have been registered by the concerned registration authorities.

3. In view of the above, it is requested that any such matter, if reported or otherwise, may be taken up with the concerned authority to conduct a proper inquiry and take appropriate action required under the law. ORGI would provide assistance in the said inquiry, if required.

4. In this respect, all registration authorities may be directed to exercise due diligence while accessing the existing portal/software and ensure that they enter the complete and correct Uniform Resource Locator (URL) of the website/portal. Further, as reiterated in the past, login credentials of the active users (State/District/Registration Units/Hospitals etc) may be checked, verified and updated on regular basis. You are also requested to sensitize general public, at large, about the URL of the official website of births & deaths registration through necessary publicity measures. The general instructions for handling of login ID and password along with Dos and Don’ts for the users of Portal/website is attached as Annexure-A for compliance.

Yours faithfully,

Encl: As above.

(Sanjeev Kumar)
Addl. Registrar General (CRS)

Copy to:

(i) The Chief Secretaries of all States/UTs for information and necessary action.

(ii) The Directors of all DCOs to follow up with the concerned Chief Registrar. Further, the Annexure-A is to be translated in local language and to be given to Chief Registrars for further circulation among the Registration Authorities.

(A. K Pandey)
Joint Director (CRS)

Annexure-A

General Instructions
FOR HANDLING OF USER/LOGIN ID AND PASSWORD IN PORTAL/WEBSITE

ORGI CRS portal (https://crsorgi.gov.in) is highly secure with CAPTCHA challenge response to prevent and handle the robotic cyber-attacks as well as page authenticity is highly encrypted and private. Accordingly, the existing portal/website developed for online registration of births and deaths in states/UTs must be run under Secure Socket Layer (SSL). The two factor authentication must be set for Users of the portal/websites.

Safe custody and safe methodology for User/Login ID activation is the primary requirement to deal with IT security threats so there is a need of Standard Operating Procedure (SOP) for secure custody and handling of User/Login ID in Portal/website as well as security of email ID and mobile number linked with portal user's Profile. This document contains the SOP guidelines along with DO's and DON'Ts for the users of Portal/website developed for online registration of births and deaths.

For USERS: Registrar/Institutions/Data Entry Operator

1. Login id and password to be kept strictly confidential and should not be written on any document.
2. Email id and Mobile number registered in user's profile must be certified in records before use.
3. Email-id and mobile number as given in profile must remain in use and activated.
4. Only registered email id and Mobile number may be used for official communications while contacting user administrator.
5. Prefer ink signed letter in email message if email is regarding activation of email id and reset of password.
6. Compromise of portal id/password, profile email id and issue of fake B&D certificates must be reported by ink signed letter to the concerned authority for immediate action like deactivation of user id without fail as well as matter should be reported to the nearest police station/cyber-crime cell through proper channel.

For USERS: Chief Registrar and District Registrar

1. Login id and password to be kept strictly confidential and should not be written on any document.
2. Email id and mobile number registered in user profile must be certified in records before use.
3. Prefer to use only official email id (@gov.in) in profile.
4. Email-id and mobile number as given in profile must remain in use and activated.
5. Only registered email id may be used for official communications while contacting user administrator at State level/ORGI. Prefer ink signed communications.
6. Compromise of portal id/Password, profile email id and mobile number and issue of fake B&D certificates must be reported by ink signed letter to the concerned authority for immediate action like deactivation of user id without fail as well as matter should be reported to the nearest police station/cyber-crime cell through proper channel.

DO'S

1. Keeping built-in windows defender firewall always ON is a good practice to secure your PC even if third-party Antivirus is installed. It will ensure double safety of your PC.
2. Always lock your PC with Win+L key even on short TEA break.
3. Always logout from the Portal when your task is completed.
4. Authorized PC can only be used by Operator and Registration authority even working in Office environment.
5. User Profile of all the Operators/Registrars/Informants may be verified from time to time. Specially verify the registered email ID and Mobile number for authenticity.
6. Email ID as mentioned in the profile of Registrars and Operators must be authenticated and certified to ensure the security of the login IDs.
7. Password to be changed periodically and log to be maintained but password should not be mentioned in the log book etc.
8. Please make your user ID, Password strong and long.
9. Use Alpha-Numeric, Special Character etc to create password for your user ID.
10. After transfer, make sure to reset your user ID's password as per the prescribed procedure.
11. Before login into portal, kindly confirm the complete and correct URL**. A**ny other similar looking website must be reported to police as well as to Chief Registrar and Cyber Crime Cell.

DON'Ts

1. Do not store your Password in the browser. If it is saved by mistake please remove/Clear password entry from the Browser's settings.
2. Never use Anonymous/unauthenticated third Party browser. Use Standard browsers like Internet Explorer, Chrome, and Firefox only.
3. Do not logon to Portal from Public Computer/Cyber café, own mobile device even if you are an authorized user.
4. Please don't install remote access software like Remote Desktop, Team viewer, Any-desk etc. on your Office PC.
5. No password disclosure in the email communication to be made by Registrars and Operators while communicating with admin users.
6. Do not keep your password in your mobile, nor take a photo of it.
7. Do not share password with anyone.
8. Do not open attachments of unknown email in your PCs.
9. Don't login or click any similar looking link/website.

****