I/12214/2023

रक्षा लेखा नियंत्रक (सेना)

Controller of Defence Accounts(Army)

बेल्वेडियर परिसर, आयुध पथ, मेरठ छावनी– 250001

Belvedere Complex, Ayudh Path, Meerut Cantt-250001

<u>**Through Website**</u>

No. IT&S/III/Cyber Security/2023   Date: 30/08/2023

To

    All sections of Main Office
    All sub offices under the aegis of CDA (Army) Meerut

<u>**Sub:**</u>   Advisory regarding usage of Watermarks in classified documents.

    'Watermarks' are visual marks that overlay a document to indicate its ownership, authenticity or status. Documents shared online have the propensity to be counterfeited or altered over time as they get downloaded multiple times. Watermarking can help protect documents from unauthorized copying, distribution, or alteration. Along with passwords, it is one of the most common ways to secure documents.

    Keeping in view the above, copy of an advisory issued by HQrs Office vide letter No. Mech/IT&S/810/Cyber Security/Misc dated 24.08.2023 is forwarded herewith for cognizance and strict compliance.

    This is issued with the approval of GO (IT&S).

<u>**Encl:**</u>   As stated above.

    NAVEEN PRAKASH, SAO(IT&S)-NAVEENP, IT&S-ARMY

    Accounts Officer

रक्षा लेखा महानियंत्रक

उलान बटाररोड, पालम, दिल्ली छावनी-110010

Controller General of Defence Accounts

Ulan Batar Road, Palam, Delhi Cantt.- 110010

(IT&S Wing)

Phone: 011-25665588   Fax: 011-25675030   email:cgdanewdelhi@nic.in

---

No. Mech/ IT&S/810/Cyber Security/Misc   **Circular**   Date: 24/08/2023

To

   All PCsDA/CsDA/PrIFA/IFA/PCA(Fys)
   (through DAD WAN/email)

Sub: Advisory regarding usage of watermarks in classified documents.

Security of classified information is crucial part of cyber security. Handling classified data in prescribed manner is major safeguard to prevent information breaches. While all sensitive data is being processed digitally as part of office functioning, has well defined security controls, effective and efficient control of physical manifestation of classified official documents is also crucial in order to ensure fool proof security. There is therefore a need to adhere to prescribed standard frame work for generation, storage and transmission of information in the print format, in conjunction with security of information stored digitally.

2.   An important aspect of security of printouts of official documents is that they should be in possession of only authorized personnel at times, and be used for official purposes only. Printed copies of official documents face the threat of unregulated usage and duplication, especially with the proliferation of social media coupled with easy availability of smart devices, high bandwidth and near omni present connectivity. This could lead to compromise of official documents and information breach.

3.   To overcome uncontrolled reproduction and pilferage of sensitive documents, appropriate classification   & water marking of printed documents is recommended   as a standard practice. Watermarking keeps the uniqueness of the copies of printed documents as well as identifies   the owner of the document, thus enhancing info security and accountability.

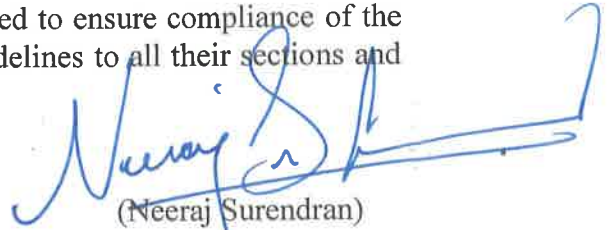4.   The following process is to be followed while printing official documents: -

(a)   As far as feasible, printing of documents as a general rule should be avoided and if necessary kept to barest minimum based on functional requirements. Copies of printed documents are to be distributed only on need to know basis.

(b)   All copies of printed/hand written drafts of classified correspondence are to be accounted for I destroyed .as per extant regulations.

(c)   Use semi-transparent watermark that covers the entire frame of the document. The watermark should not be small and positioned in corner of the document. to obviate its cropping.

(d)   The water marking should be in name of the intended recipient/Department so that any duplicate copy or its image on open/deep web can be easily traced back to the owner of the document fix accountability.

5. In view to the above, all departments are requested to use watermark of addressee in all official documents classified Confidential and above and for documents containing PII information of Service Personnel such as Name, Rank, No, Mob No, Ph No, E -mail, Appointment, PAN /License/Aadhar details, DoB etc. (especially in case of large number of PII being included in a single document such as Social Lists in Units, etc.). It is recommended to watermark classified restricted documents which are to be displayed on notice board so that people do not take photos and proliferate on Social Media.

6. In view of the above, all the Controllers are advised to ensure compliance of the guidelines given above and disseminate these guidelines to all their sections and sub offices for strict compliance.

(Neeraj Surendran)
Sr. ACGDA (IT&S)