भाकृअनुप
ICAR
भारतीय कृषि अनुसंधान परिषद

Indian Council of Agricultural Research

कृषि भवन, डॉ. राजेंद्र प्रसाद रोड, नई दिल्ली -110001

Krishi Bhawan, Dr. Rajendra Prasad Road, New Delhi – 110 001

F. No.: 10(3)/2025-ICT (e/file-378086) **Dated the 20th May, 2026**

CIRCULAR

Subject: Strengthening of Cyber Security Preparedness against Emerging AI-driven Cyber Threats – reg.

Attention is invited to the advisory issued by Indian Computer Emergency Response Team (CERT-In), Ministry of Electronics and Information Technology (MeitY), Government of India, regarding "Defending Against Frontier AI Driven Cyber Risks".

2. In view of the increasing cyber security threats arising from rapid advancements in Artificial Intelligence (AI) and AI-enabled cyber-attack tools, all ICAR Institutes / Bureaux / NRCs / ATARIs / Project Directorates / KVKs and other ICAR Units are advised to undertake immediate review of their cyber security preparedness and strengthen cyber resilience measures on priority.

3. All Institutes / Units shall, inter alia, ensure the following:

i. Timely updation and patch management of operating systems, servers, applications, antivirus software, endpoint security solutions, and security devices;

ii. Protection and continuous monitoring of internet-facing systems, applications, websites, VPNs, and remote access infrastructure, including disabling unused ports/services;

iii. Enforcement of Multi-Factor Authentication (MFA) and strengthening of access control mechanisms for critical systems and official eMail / VPN services;

iv. Regular vulnerability assessment, security audit, monitoring of logs/network activities, and implementation of appropriate cyber security controls;

v. Maintenance of secure and offline backups of important institutional data and review of disaster recovery / cyber incident response mechanisms;

vi. Enforcement of strong password policies and avoidance of weak / default / shared passwords;

vii. Conduct of cyber security awareness and sensitization programmes regarding phishing, malicious links / attachments, impersonation, social engineering, and AI-enabled cyber threats;

viii. Restriction on use of unapproved external AI platforms / tools for processing or sharing official/confidential/sensitive data; and

ix. Immediate reporting of cyber security incidents / suspicious activities to CERT-In and concerned authorities as per prescribed guidelines.

4. All Institutes / Units are further requested to nominate a suitable officer as Nodal Officer of Cyber Security at the level of Scientist / ACTO and above for coordination, implementation, monitoring, and review of cyber security preparedness measures and compliance with CERT-In advisories. Details of the designated Nodal Officer may be shared with the CISO, DARE / ICAR on the email id shashibhushan.iasri@icar.org.in for coordination and dissemination of cyber security related advisories/instructions in the future.

5. The matter may be accorded top priority to safeguard institutional ICT infrastructure, official digital assets, sensitive data, and continuity of critical services.

This issues with the approval of the Competent Authority.

20.05.2026

(K.P. Singh)
Assistant Director General (ICT)

Distribution:

1. All Directors, ICAR Institutes / PDs / Bureaux / ATARIs / NRCs / KVKs.
2. Dr S.B Lal, Principal Scientist & CISO (DARE / ICAR), ICT Unit, ICAR Hqrs., Krishi Bhawan, New Delhi.
3. eOffice Notice Board.
4. Guard File.