ICAR – DIRECTORATE OF MUSHROOM RESEARCH
CHAMBAGHAT, SOLAN, HIMACHAL PRADESH

ACTION TAKEN REPORT

Observance of National Cyber Security Awareness Month (NCSAM)

Dated : 05.11.2026
No.F.AKMU/CyberSecurity/NCSAM-2026

Submitted by: AKMU Cell (Computer/IT Cell)

Through: I/c AKMU
Subject: Action Taken Report on Cyber Security Awareness Month (NCSAM) activities and implementation of cyber security measures at ICAR-DMR, Solan.

With reference to the communication received from ICAR regarding the observance of National Cyber Security Awareness Month (NCSAM), the AKMU Cell (Computer/IT Cell), ICAR-DMR, Solan, has undertaken various awareness, security and compliance-related activities to strengthen the cyber security posture of the Institute and promote safe digital practices among all officials and employees.

The following activities have been completed and measures initiated:

1. Cyber Security Awareness and Publicity

- Designed and developed a dedicated Cyber Security Awareness banner highlighting the importance of cyber hygiene and safe digital practices.
- Hosted the cyber security awareness banner on the official website of ICAR-DMR, Solan.
- Circulated the awareness banner through the official WhatsApp group of Institute officials to ensure wider dissemination of cyber security messages.

2. Development of Cyber Security Awareness Presentations

Prepared PowerPoint presentations covering the following important areas:

- Multi-Factor Authentication (MFA): Importance of enabling MFA for secure access to official accounts and digital services.
- Cyber Security Incident Reporting: Awareness regarding timely identification and reporting of suspicious activities, phishing attempts, malware infections and other cyber incidents.
- Device and Software Hygiene: Safe use of computers, operating systems, applications, antivirus software and regular security updates.

These presentations were developed to sensitize officials and employees regarding their individual responsibilities in maintaining a secure IT environment.

3. Symantec Endpoint Protection (SEP) Server Audit

- Conducted an audit of the Symantec Endpoint Protection (SEP) Server.
- Prepared an audit report covering the status of endpoint security management.
- Reviewed the antivirus definition update status of client computers and server machines.
- Undertaken updating of SEP virus definitions on all connected client computers and servers to strengthen protection against malware and emerging cyber threats.

4. Official Website Security and Compliance

- Updated the SSL certificate of the official website of ICAR-DMR, Solan, to ensure secure HTTPS communication.
- Conducted a security audit of the Institute's official website.
- Reviewed website security aspects and initiated necessary measures to improve its security and compliance posture.

5. Awareness Regarding Unauthorised Software and Digital Resources

All users have been advised:

- Not to download, install or use unauthorised freeware, cracked software or unlicensed applications on official computers and the Institute network.
- Only duly licensed and authorised software/tools shall be permitted on the official network.
- To avoid using unofficial IT-related websites, software repositories, online tools and unauthorised digital resources for research or official purposes.
- To use only trusted and authorised digital platforms and resources for official and research-related activities.

6. Restrictions on Personal Devices

Users have been advised that:

- Personal laptops and computers shall not be connected to the official Institute network.
- Personal laptops shall not be used for official work or granted access to office/laboratory network resources.
- Official work shall be performed only through authorised Institute-provided desktop computers and approved IT infrastructure.

7. Network Security, CCTV and Log Monitoring

Users have been informed about the importance of maintaining network activity records and monitoring digital infrastructure.

The following measures have been communicated:

- CCTV system records, server logs, client computer logs and network activity logs should be retained and monitored in accordance with applicable Government/ICAR cyber security policies.
- A log retention period of 6–12 months is proposed for relevant security logs, subject to applicable policies, storage capacity and technical feasibility.
- Open or unsecured Wi-Fi networks shall not be permitted within the Institute premises.
- Wi-Fi credentials shall not be shared with unauthorised persons or visitors.
- Access to the official network shall be restricted to authorised users and devices.

8. Centralised Firewall and Network Monitoring

The Institute proposes to procure and deploy a robust Centralised Firewall solution in the near future to strengthen network security and enable centralised monitoring and reporting.

The proposed firewall infrastructure is intended to facilitate:

- Centralised monitoring of network traffic and connected devices.
- Recording and analysis of network activity.
- Monitoring of suspicious connections and unauthorised access attempts.
- Maintenance of security logs and reports for the prescribed retention period.
- Improved network access control and incident investigation capabilities.

9. Special Instructions for GeM Users

In view of the security requirements and monitoring mechanisms associated with the Government e-Marketplace (GeM), all registered GeM users of ICAR-DMR, Solan, have been advised:

- All official GeM-related activities must be performed exclusively through the respective authorised/allotted official desktop computers.
- Users must not use personal laptops, computers or unauthorised devices for GeM-related official work.
- Users should be aware that GeM portal security mechanisms may record and monitor IP addresses and other relevant access information.
- GeM users must ensure that their official activities are performed securely and in accordance with applicable GeM guidelines and Government instructions.

10. Implementation of Cyber Security Controls

All officials and employees have been advised that the above-mentioned cyber security controls and instructions shall come into force with immediate effect.

The AKMU Cell shall continue to monitor compliance, provide technical guidance and undertake necessary awareness activities to strengthen the Institute's cyber security framework.

Conclusion

The AKMU Cell, ICAR-DMR, Solan, has undertaken several awareness and technical initiatives during the observance of National Cyber Security Awareness Month. These activities include cyber security awareness campaigns, preparation of educational presentations, SEP Server auditing, antivirus definition updates, SSL renewal, website security audit and dissemination of guidelines on secure use of IT infrastructure.

Further, the Institute proposes to strengthen its network security through the procurement and implementation of a robust centralised firewall solution.

All officials, scientists, technical staff and other users are expected to strictly adhere to the prescribed cyber security instructions and cooperate with the AKMU Cell in maintaining a secure and reliable IT environment at ICAR-DMR, Solan.

Submitted for kind information and further necessary action, please.

Sd/-

I/c AKMU Cell
ICAR-Directorate of Mushroom Research
Solan, Himachal Pradesh

OFFICE NOTE / CIRCULAR

CYBER SECURITY INSTRUCTIONS FOR ALL USERS OF ICAR-DMR, SOLAN

Subject: Mandatory Implementation of Cyber Security Guidelines and IT Security Controls at ICAR-DMR, Solan – Regarding.

In continuation of the cyber security awareness initiatives undertaken during National Cyber Security Awareness Month (NCSAM), all officers, scientists, technical staff, contractual employees, research scholars and other users of ICAR-DMR, Solan, are hereby informed that maintaining cyber security is a collective responsibility.

To safeguard the Institute's IT infrastructure, official information, research data and digital services, the following instructions shall be strictly followed by all users with immediate effect.

A. Use of Official Computers and Personal Devices

1. Official work shall be performed only through authorised/allotted Institute desktop computers.
2. Personal laptops and computers are strictly prohibited from being connected to the official Institute network.
3. Personal laptops shall not be used for official work or provided access to office/laboratory network resources.
4. Users shall not connect unauthorised USB devices, external storage devices or other peripherals to official computers without due authorisation.

B. Software Installation and Usage

1. Installation and use of cracked, pirated, unauthorised or unlicensed software are strictly prohibited.
2. Only duly licensed and authorised software and tools shall be permitted on the Institute network.
3. Users shall not download software, utilities or applications from untrusted websites.
4. Any requirement for new software installation must be referred to the AKMU Cell for examination and approval.

C. Antivirus and Endpoint Security

1. Symantec Endpoint Protection (SEP) shall remain active on all designated official client computers and servers.
2. Antivirus definitions must remain updated.
3. Users shall not disable, uninstall or tamper with antivirus or other endpoint security settings.
4. Any antivirus alert, malware detection or suspicious computer behaviour must immediately be reported to the AKMU Cell.

D. Network and Wi-Fi Security

1. No open or unsecured Wi-Fi network shall be operated within the Institute premises.
2. Wi-Fi passwords and network credentials must not be shared with unauthorised users, visitors or outsiders.
3. Unauthorised routers, Wi-Fi access points, switches or network devices shall not be connected to the Institute network.
4. Users must not attempt to bypass network security controls or access restrictions.

E. Password and Account Security

1. Strong and unique passwords must be used for official accounts.
2. Multi-Factor Authentication (MFA) should be enabled wherever supported and applicable.
3. Passwords, OTPs and login credentials must never be shared with anyone.
4. Users must remain alert to phishing emails, suspicious links, fraudulent attachments and impersonation attempts.

F. Cyber Security Incident Reporting

Any suspected cyber security incident, including phishing, malware infection, unauthorised access, data leakage, suspicious network activity or loss of an official device, must immediately be reported to the AKMU Cell for necessary action and escalation through the prescribed reporting channels.

G. Monitoring and Log Retention

1. Official network infrastructure, servers, client computers and CCTV systems may be subject to authorised monitoring and security logging.
2. Relevant logs, including server, client and network activity records, shall be maintained centrally wherever technically feasible and as per applicable Government/ICAR guidelines.
3. A log retention period of 6–12 months is proposed, subject to applicable instructions, technical feasibility and storage capacity.
4. Users shall not attempt to delete, alter or tamper with official system or security logs.

H. Special Instructions for GeM Users

1. All GeM users must perform their official GeM-related activities exclusively through their allotted/authorised official desktop computers.
2. Use of personal laptops or unauthorised computers for GeM-related official activities is prohibited.
3. Users must exercise due care while accessing the GeM portal, as IP addresses and relevant access information may be recorded by the portal's security mechanisms.
4. GeM login credentials and OTPs must not be shared with other individuals.

I. Centralised Network Security

The Institute is planning to procure a robust Centralised Firewall solution to improve network security, access control, traffic monitoring, security reporting and log management.

Until its implementation, all users YP, RA, SRF etc. are required to strictly follow the existing security instructions and cooperate with the AKMU Cell in maintaining the security of the Institute network.

IMPLEMENTATION

All the above cyber security instructions and controls shall come into force with immediate effect. All Sections, In-charges of Laboratories and all concerned officials are requested to ensure strict compliance by their respective staff and users.

Any violation of these instructions or unauthorised use of the Institute's IT infrastructure may be viewed seriously.

For any technical assistance, software installation requirements, network access or reporting of cyber security incidents, users may contact the AKMU Cell (Computer/IT Cell).

Sd/-

AKMU Cell
ICAR-Directorate of Mushroom Research
Solan, Himachal Pradesh

Distribution:

1. All I/c Sections, ICAR-DMR, Solan.
2. All Scientists, Administration YP, RA and Technical staff.
3. Notice Board / Official Website / Official WhatsApp Group.

This circular may be displayed on the official website and circulated through the official communication channels of the Institute.

Sd/-

I/c AKMU Cell
ICAR-Directorate of Mushroom Research
Solan, Himachal Pradesh