



Dated Lahore, the 05<sup>th</sup> September, 2022

To

1. The Director General Agriculture (Ext. & A.R.), Punjab, Lahore.
2. The Director General Agriculture (Field) Punjab, Lahore.
3. The Chief Scientist Agriculture (Research), Ayub Agricultural Research Institute, Faisalabad.
4. The Director General Agriculture (WM), Punjab, Lahore.
5. The Director General, PW & QC of Pesticides, Punjab, Lahore.
6. The Director General, Soil Survey of Punjab, Multan Road, Lahore.
7. The Director of Agricultural Information, Punjab, Lahore.
8. The Director of Agriculture, Crop Reporting Service, Punjab, Lahore.
9. The Chief, P&E Cell, Agriculture Department, Lahore.
10. The Chief (WTO), Agriculture Department, Davis Road, Lahore.
11. The Director of Agriculture (E&M), Punjab, Lahore.
12. The Chief Coordinator, RAEDC, Vehari.
13. The Director of Floriculture (T&R), Punjab, Lahore.
14. The Director, Punjab Institute of Agriculture Marketing (PIAM), Lahore.
15. The Managing Director, Punjab Seed Corporation, Lahore.
16. The Registrar, University of Agriculture, Faisalabad.
17. The Chief Executive, Punjab Agricultural Research Board, Lahore.
18. The Registrar, Arid University of Agriculture, Rawalpindi.
19. The Director, Agriculture Marketing Development Fund, Lahore.
20. The Registrar, Muhammad Nawaz Sharif University of Agriculture, Multan.
21. The Chief Technical Advisor, Agriculture Delivery Unit (ADU), Lahore.
22. The Secretary Agriculture Commission, Lahore.
23. The Chief, Sugarcane Research & Development Board, Faisalabad.

Subject:- **CYBER SECURITY ADVISORY – PREVENTION AGAINST WEBSITE COMPROMISE ON THE EVE OF NATIONAL DAYS (ADVISORY NO.34)**

I am directed to refer to the subject noted above and enclose herewith a copy of letter No.SO(FG-I)3-72/2021 (Vol-I), dated 17.08.2022 alongwith its enclosure received from Section Officer (FG-I), Government of the Punjab, S&GAD is forwarded for information and further necessary action.

SECTION OFFICER (GENERAL)  
Ph. No.99210505

**C.C.**

1. PA to Additional Secretary (Admn), Agriculture Department.
2. PA to Deputy Secretary (Admn-I), Agriculture Department.

*Plz send scan copy  
to director IT  
AR (Aead)  
16/09/22  
Dip (HR)*

3843  
14/08/2022

GOVERNMENT OF PAKISTAN  
CABINET SECRETARIAT  
CABINET DIVISION  
(NTISB)

No. 1-5/2003 (NTISB-II)

Islamabad, the 12<sup>th</sup> August, 2022

Subject: - Cyber Security Advisory – Prevention against Website Compromise on the Eve of National Days (Advisory No. 34)

**Context.** Hostile elements/ state sponsored malicious actors typically target government departments/ ministries and defence sector websites on the eve of the National Days for disruption of services and defacement to tarnish the global image of Pakistan. It is likely that hostile elements may launch cyberattack on National IT Infrastructure on National Days (14 August, 6 September and 23 March). Accordingly, an advisory is being sent to sensitize website administrators and Service Providers to take additional security precautions (such as web server hardening, traffic/ integrity monitoring etc) to avoid possible website defacement/ hacking attempts. Moreover, webserver administrators should be made mindful of cyber security guidelines mentioned below.

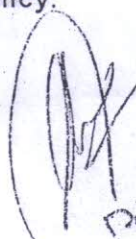
2. Cyber Security Best Practices for Websites Protection

- a. Upgrade OS and web servers to latest version.
- b. Website admin panel should only be accessible via white-listed IPs.
- c. Defend your website against SQL injection attacks by using input validation technique.
- d. Complete analysis and penetration testing of application be carried out to identify potential threats.
- e. Complete website be deployed on inland servers including database and web infrastructure.
- f. HTTPS protocol be used for communication between client and web server.
- g. Application and database be installed on different machines with proper security hardening.
- h. Sensitive data be stored in encrypted form with no direct public access.
- i. DB users privileges be minimized and limited access be granted inside programming code.
- j. Proper security hardening of endpoints and servers be performed and no unnecessary ports and applications be used.
- k. Updated Antivirus tools/ Firewalls be used on both endpoints and servers to safeguard from potential threats.
- l. Enforce a strong password usage policy.

copyive.

1557  
11/8/22

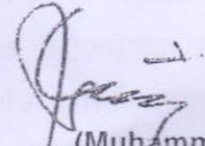
DPA



4742  
16-08-22

- m. Remote management services like RDP and SSH must be disabled in production environment.
- n. Deploy web application firewalls (WAF) for protection against web attacks.
- o. Employ secure coding practices such as parameterized queries, proper input sanitization and validation to remove malicious scripts.
- p. Keep system and network devices up-to-date.
- q. Log retention policy must be devised for at least 3x months on separate device for attacker's reconnaissance.

3. Kindly disseminate the above message to all concerned in your organizations, all attached/ affiliated departments and ensure necessary protective measures.



(Muhammad Usman Tariq)  
 Assistant Secretary-II (NTISB)  
 Ph# 051-9204560

All Secretaries of Ministries / Divisions of Federal Government and Chief Secretaries of Provincial Governments

Copy to: -

1. Secretary to the Prime Minister, Prime Minister Secretariat, Islamabad
2. Secretary to the President, Aiwan-e-Sadar, Islamabad
3. Cabinet Secretary, Cabinet Division, Islamabad
4. Additional Secretary-III, Cabinet Division, Islamabad
5. Director General (Tech), Dte Gen, ISI Islamabad
6. Director (IT), Cabinet Division, Islamabad