362/GW/AII
17.07.15

1475
14/7/15

Immediate

From

The Additional Chief Secretary to Government of Haryana,
Agriculture Department.

To

1. The Director General Agriculture, Haryana, Panchkula.
2. The Director General Horticulture, Haryana, Panchkula.
3. The Chief Administrator,
   Haryana State Agriculture Marketing Board, Panchkula.
4. The Managing Director,
   Haryana Seeds Development Corporation, Panchkula.
5. The Managing Director,
   Haryana Land Reclamation & Development Corporation,
6. The Managing Director ,
   Haryana State Warehousing Corporation, Punchkula.
7. The Managing Director,
   Haryana Agro-Industries Corporation, Panchkula.
8. The Director,
   Haryana State Seeds Certification Agency,
   Panchkula.
9. The Registrar,
   Chaudhary Charan Singh, Haryana Agriculture University Hisar

Memo No. 1813- Agri. II (4)-2015/12789
Chandigarh, Dated the 6/7/2015

Subject: Guidelines for securing Web Sites/Portal

Enclosed please find herewith a copy of the letter No HR
ISMO/2015/CISO/2464 dated 23.06.2015 received from Haryana State Informatic
Security Management office on the subject noted above for strict compliance.

Superintendent,
for Additional Chief Secretary to Govt. of Haryana
Agriculture Department.

1. A copy ... compliance
2. A copy may also be kept in Guard file.

3278-USA 1
25-06-15

Haryana State
Information Security Management Office

Society for IT Initiative Fund for e-Governance,
Department of Electronics & Information Technology, Haryana

INFORMATION SECURITY

कृषि - II शाखा
डायरी संख्या 82
दिनांक 26/6/15

HRY-ISMO/2015/CISO/ 2464

No. 7074 ACS(Agri)
Dated 24/6/15

19 June 2015
23

DHANPAT SINGH,IAS
Addl. CS Agri
24.06.15

Principal Secy. Agriculture

Dear Sir / Madam:

Subject: Guidelines for securing Web Sites/Portals.

You may be aware that the cyber space is vulnerable to a wide variety of threats due to which a strategic framework is required for countering cyber attacks. This should involve a combination of **preventive, detective and reactive** measures that are required to deal with cyber attacks. In view of this, the following guidelines should be implemented to mitigate the security risks of your organizational web site(s).

USA 9 82 25/6 Hari 25 S/A-I

1. All Web Sites/Portals with State Govt. bodies (Boards, Corporation, Departments) which are hosted on private web servers or hosted outside country should be hosted in Haryana State Data Centre (HSDC), Sector-17, Chandigarh.
2. Each Department should identify/nominate a website administrator, who would also be responsible for administering cyber security requirements.
3. Before hosting a new site, Security Audit is mandatory through an approved agency or ISMO.
4. In addition, it would be mandatory to carry out periodic security Audit/ Assessment of each departmental web portal(s) by ISMO.
5. Each Department should establish an Incident Response Team and report cyber security incidents as and when they occur with Cert-In and ISMO.
6. Maintaining the logs at all levels (application, webserver, Operating System) preserving and analyzing the logs to detect attacks.
7. Each department should identify appropriate information security management practices keeping in view their business needs. The identified practices should be implemented.
8. Implementation of important Security Controls for effective cyber security and continuous security assessment (Annexure-1).

Bays 73-76, Hartron Bhawan, Sector 2, Panchkula. 134151
Chairman, E.C.: 2740009, MSEC.: 2741547, Ad.O: 2748142, Fax:0172-2749985
ciso@haryanaismo.gov.in www.haryanait.gov.in

HARYANA GOVERNMENT / सरकार

Haryana State
Information Security Management Office

Society for IT Initiative Fund for e-Governance,
Department of Electronics & Information Technology, Haryana

Administrator and end-users have to keep pace with information security updates and get them implemented in their Web Application/Systems, review the 'zero day' (i.e. previously unknown) vulnerabilities with respect to their environment and apply the necessary patches. ISMO will facilitate State Departments/Organizations for security assessment of their Web Site/ Portals and also assist in addressing security vulnerabilities.

This may please be circulated within your organizations for prompt action by all concerned. More information and contact details of nodal officer for assistance are provided in the Advisory.

Yours truly,

Chief Information Security Officer
Haryana State ISMO

All the Administrative Secretaries to Govt. Haryana.

All the Heads of Departments in Haryana.

The Registrar, Punjab & Haryana High Court, Chandigarh.

All the Divisional Commissioners in Haryana.

All the Managing Directors/ Chief Administrators/ Chief Executive Officers of the Boards, Corporations, etc. in Haryana.

All the Deputy Commissioners in Haryana.

All the Registrars of Universities in Haryana

Bays 73-76, Hartron Bhawan, Sector 2, Panchkula. 134151
Chairman, E.C.: 2740009, MSEC.: 2741547, Ad.O: 2748142, Fax:0172-2749985
ciso@haryanaismo.gov.in www.haryanait.gov.in

3

Annexure - 1

Important Security Controls for Effective Cyber Security and Continuous Security Assessment

(1) Inventory of authorized and unauthorized hardware.
(2) Inventory of authorized and unauthorized software.
(3) Secure configurations for hardware and software for which such configurations are available.
(4) Secure configurations of network devices, such as firewalls and routers.
(5) Boundary defense.
(6) Maintenance and analysis of complete security audit logs.
(7) Application software security.
(8) Controlled use of administrative privileges.
(9) Controlled access based on need to know.
(10) Continuous vulnerability testing and remediation.
(11) Dormant account monitoring and control.
(12) Anti-malware defences.
(13) Limitation and control of ports, protocols and services.
(14) Wireless device control.
(15) Data-leakage protection.
(16) Secure network engineering.
(17) Red-team exercises.
(18) Incident-response capability
(19) Assured data backups.
(20) Security-skills assessment and training to fill gaps.

It is supposed, that all State Departments/Organizations should examine all twenty control areas against their current status and develop an organization-specific plan to implement the controls. Departments/Organizations with limited information security programs may choose to address certain aspects of the controls in order to make rapid progress and to build momentum within their information security program.