Haryana Government
Secretariat for Information Technology

हरियाणा सरकार
सूचना प्रौद्योगिकी सचिवालय

No. Admn/315/ISIT/16914

From

Principal Secretary to Government Haryana,
Information Technology Electronics & Communication Department, Chandigarh.

To

1. All the Administrative Secretaries to Govt. Haryana.
2. All the Heads of Departments in the State of Haryana.
3. All the MDs/CAs of Government Companies, Boards & Corporations in the State of Haryana.
4. All the Divisional Commissioners in the State of Haryana.
5. All the Deputy Commissioners in the State of Haryana.
6. The Registrar of all the Universities in the State of Haryana

Chandigarh dated, the 17.01.2022

Subject: - Strict cyber security controls on Web Sites providing Citizen Services.

Sir/ Madam,

The State Government has increased the level and scale of providing online services to citizens resulting in a high level of interaction among various applications disseminating a wide portfolio of services. Web Sites are communicating in heterogeneous environment and continuously collecting data from multiple websites /portals from various organizations through API (Application Programming Interface). Our State is heading towards providing service delivery to the Citizen via a single gateway/dashboard.

At the same time, the risks of data breach and unauthorized access to the heterogeneous e-government Systems have increased. In light of recent cyber security incidents of disseminating online services/facilities to ineligible/fake entities reported in the media with respect to a Government of India portal, it is requested to consider cyber security as a top priority and establish appropriate security controls with strict protocols. It is also requested to review the services, particularly those involving Citizen service portals on a daily basis, so as to ensure that fake users / entities are not using /manipulating such portals.

To maintain basic cyber hygiene at the organization level, general security guidelines at Annexure 'A' and a security advisory for securing Web Applications/Server(s) at Annexure B are attached herewith for your consideration. For any specific assistance/security support related to Cyber Security services, Haryana ISMO team (support.desk@haryanaismo.gov.in) may be contacted.

Looking for your support in setting up an effective Cyber hygiene across the State IT Systems and prevent un-authorized exploitation / un-ethical usage of IT Systems and Networks.

Special Secretary to Government of Haryana,
Information Technology, Electronics and Communication Deptt.

;58553/2022/IT Cadre

Annexure 'A'

GENERAL GUIDELINES ON CYBER SECURITY

"Cyber Security is everyone's responsibility"

Area	Guidelines
General Computer Usage	DO'S: • Use only genuine/licensed version of Operating System and Anti-Malware software on Computer System/Laptop. Nothing is free over internet like "Free" Screensavers, cracked software's etc., so be aware. • Remove files or data you no longer need to prevent unauthorized access to such data. • Treat passwords as sensitive information and do not share it with anyone. Passwords should not be stored in readable form in computers, notebook, notice board. • Always download software or applications from known trusted sources only. • Cyber Security Incidents are inevitable. Please report all security incidents such as payment fraud, Data Theft etc. with Haryana ISMO through email at support.desk@haryanaismo.gov.in or for direct assistance please contact Haryana Cyber Security helpline no. 0172-2709250. • Incidents like Cyber-attack/Web Site hacking, Ransomware etc. be reported directly to Cert-In at incident@cert-in.org.in with cc to support.desk@haryanaismo.gov.in" DON'TS: • Don't share Computer System/Email/ Application Log-In Passwords/OTP with anyone. • Don't use common passwords for different applications/accounts. • Don't store personal information of any citizen (like Aadhar Number, Bank Account Details, Mobile Number etc.) Information on publically accessible website/applications. • Don't leave the computer system/mobile device unattended with sensitive information. a) Windows based system can be locked by pressing "ctrl +alt+del" and choosing "lock this computer" or "window button+ L" b) Linux based system can be locked by pressing "window button+ L" c) Mobile devices can be locked by pressing Power Key once.
Internet Browsing	DO'S: • Make use of two-factor authentication (OTP, Secret Question etc.), while getting into accounts/online services such banking, accessing server etc. • Private browsing mode should be used, such as Incognito in Chrome or InPrivate mode in Edge in case of sensitive / critical applications, such as payment / finance applications on public/open Internet connections (at Airports/Railways Station etc.) DON'TS:

	• The "Save password" or "Remember Password" option prompted by the browser/applications should never be selected. Don't save account information, such as passwords or credit card information in web browsers. • Always be careful when clicking on links carrying offers/flashing prize money, free tickets, heavy discounts etc. during web browsing. • Be cautious on tiny or shortened URL"s (appears like http://tiny.cc/bz1j7y) and don't click on it as it may take you to a malware infected website. • Do not use file sharing softwares, torrents etc., as file sharing opens your Computer/Mobile to the risk of malicious files and attacks. • Distributing, disseminating or storing images, text material that might be considered indecent, pornographic, obscene, illegal, politically motivated, anti-national, provoking religious or caste bias is prohibited.
Email ommunic ation	DO'S: • Check and verify email sender ID and web links before opening email attachments, clicking on links in email. • Always check and verify the sender email details like email-ID, subject, domain name such as ""Income tax Department - Tax Refund"" from emails like <incomtaxxxxx@gmail.com> before opening, as the subject matter can be misleading." • If you receive an email from a foreign lottery or sweepstakes, money from an unknown relative, or requests to transfer funds from a foreign country for a share of the money it is guaranteed to be a scam and do not respond and delete such emails. • Avoid filling forms that come via e-Mail asking for your personal information. And do not click on links that come via e-Mail like "tax refund online forms". DON'TS: • Don't download attachments from e-Mails into your Computer/Mobile Phone from untrusted sources. Scan the attachment with updated antivirus software before saving it. • Do not send or open attachment having extension such as EXE, DLL, VBS, SHS, PIF, SCR. Typical example., .txt.exe,.doc.exe, Word documents with macros etc.
SSWORD nageme nt	DO'S: • Ensure all devices/accounts are protected by a strong PIN or passcode. Never share your PIN or password with anyone. Strong password can be created with a combination of letters, numbers, and special characters having minimum of 8 characters" and it should be regularly updated. • If your work requires you to communicate passwords, such as while sending password for an encrypted file sent as an attachment through email it must be communicated through a different channel such as over a phone call or SMS. Passwords shared over WhatsApp should be deleted by the sender "Delete for Everyone" upon confirmation from recipient. DON'TS: • Do not allow someone to stand behind and look at your password entry. • Do not write the password on paper/sticky notes and paste on the System/Desk.

Wi-Fi Network	DON'TS: • Do not connect to Public/Open Wi-Fi Networks, until it is utmost required.
Social Media / Engineering	DO'S: • Social Media Sites should be filtered and access should be provided as per HoD approvals • Avoid sharing your personal information such as address, phone number, date of birth, photographs and videos on social media. DON'TS: • Don't respond to unsolicited phone calls, visits, or email messages from individuals asking about personal or other Government information. • Dot not disclose official information on social media or social networking portals or applications. • Do not trust online users unless you know and can trust them in real life. • Do not reply or click on Link on SMS or photos send by strangers. • Do not share your net-banking password, One Time Password (OTP), ATM or phone banking PIN, CVV number etc. with any person even if he/she claims to be an employee or a representative of the bank and report such instances to your bank immediately.
Mobile Security	DO'S: • Be careful while downloading applications through Bluetooth or as MMS attachments. They may contain some harmful software, which will affect the mobile phone • Avoid downloading the content into mobile phone or laptop from an untrusted source • Preferably, Store your data on external SD card of your mobile and take out the SD card before giving the mobile for repair DON'TS: • "The mobile based banking solutions should be used with utmost care, as passwords/IDs can be leaked due to mobile operating system vulnerabilities particularly old versions of Android. • Do not store copies of your AADHAAR Card, PAN Card, passwords on your mobile devices • Avoid downloading untrusted Mobile Apps which leads to Data Theft/Financial Fraud. • Don't click on suspicious/Tiny URLs shared over SMS, Social Messaging platforms by unsolicited senders

claimer: Do's and Don'ts are basic minimum precautions to be taken however, individual/organization should identi ditional measures for information security in accordance with their business use.

Annexure-B

Security Advisory (Technical) - Securing Web Application & Web Server

#	Action Item(s)
1	Each Web Application should have a Content Security Policy (CSP) to prevent cross-site scripting (XSS), clickjacking and other code injection attacks resulting from execution of malicious content.
2	HTTP Strict Transport Security-HSTS (in case of HTTPS), Content Security Policy (CSP), Cross Site Scripting Protection (X-XSS), X-Frame-Options, X-content type options, Public-Key-Pins (in case of HTTPS) Security Headers should be implemented and validated on the web site.
3	Each input box/parameter should be sanitized and validated (using the whitelisted approach) in terms of checking, cleaning, and filtering data inputs from end users, APIs, and web services for any unwanted characters and strings to prevent the injection of harmful codes into the System.
4	Input validation/data validation should be implemented (using the whitelisted approach) for proper testing of any input supplied by a user and also to prevent improperly formed data entering into the system.
5	In case of File upload functionality on Web Application, file type validation should be implemented by checking file extension before uploading into the System. For example, to validate for file type Image/Picture the file extensions should be verified such as .jpeg/.jpg/.png/.gif at Client Side & Server Side. Further, during upload any file into System, the file content validation should also be implemented.
6	The Log-In Passwords should be complex in nature, which consist of at least 8 to 12 characters, including uppercase letters, lowercase letters, numeric digits, and non-alphanumeric characters such as & $ * and !

7 For elevated log-in security practice, Multi-factor Authentication (such as OTP) may be used.

8 CAPTCHA/Anti-Automation technique should be implemented in Input Form/Log-in.

9 DMARC and SPF records should be added to your DNS for the Domain.

10 The Web Server (like Apache/IIS/Tomcat etc.) should be hardened to prevent any sensitive information leakage such as Web server version disclosure and Technology stack version disclosure etc.

11 SSL/TLS certificate should be implemented properly to provide secure communication between your website and its users.

12 Only GET and POST methods are allowed as per requirement only. Disable PUT, TRACE, OPTIONS, DELETE methods on System.

13 Each Web Server should have Anti-malware system installed and should be updated for continuous scans.

14 Server & Application should have installed latest security patches/updates.

15 Server should be configured to store Logs/metadata to discover any cyber-attack activity or un-ethical usage.

16 Each Web Application should be Security Audited at-least once a Year.