Subject: **Advisory – Website Security (Advisory No. 16)**

1. Recently, a number of hacking attempts have been observed against critical Info Infrastructure of the country. A number of servers with weak security policies have been compromised and hackers restored to ransom ware for return back of data.

2. In the light of recent cyber attacks, following measures to enhance database security are recommended for immediate implementation: -

a. Utilize **latest version** of Web server, Database Server and applications such as PHP, JSP, ASP, JBos etc. **Ensuring that web servers run the most up-to-date software to address these risks and reduce the attack surface.**

b. **Apply appropriate updates / patches on the OS** and Application software.

c. **Maintain up-to-date antivirus signatures** and engines.

d. **Validate and sanitize all user input**, and present error messages that reveal little or no useful information to the user **to prevent SQL injection attacks**.

e. Install software only from **Trustworthy sources** to protect from possible malware infections.

f. **Change default settings**, such as login credentials, to prevent them from being used in hacking attempts.

g. **Enforce a strong password policy** and **implement regular password changes.**

h. **Never allow unrestricted file uploads** and limit these uploads only to what users need. Apply Security Information and Event Management (SIEM) or Database Activity Monitoring (DAM) solutions.

i. **Periodically check the web server directories for any malicious / unknown web shell files and remove as and when noticed.**

j. **Perform regular backups of all critical information** to limit the impact of data or system loss and to help expedite the recovery process. Ideally, this data should be kept on a separate device and backups should be stored offline.

k. **Ensure strict application of security controls at the data centre**. In addition, perform periodic & regular compliance of such security controls.

l. **Disable remote Desktop Connections** when not required.

m. **Consider disabling, PowerShell / windows script hosting**, if not required.

n. **Deploy, maintain and update a well reputed web application firewall**.