

15 -ാം കേരള നിയമസഭ

11 -ം സമ്മേളനം

നക്ഷത്ര പിന്നം ഇട്ടാത്ത പ്രോഡ്യുസ് നം. 3877

28-06-2024 - തു മുട്ടടിയ്ക്ക്

മന്ത്രിയുടെ പേജ്സംൽ സ്ഥാപി അംഗങ്ങൾക്ക് കൈകളിലി

പ്രോഡ്യുസ്	ഉത്തരം
ശ്രീ രാജീ എം. ജോൺ	ശ്രീ പിണറായി വിജയൻ (മുഖ്യമന്ത്രി)
(എ) ബോട്ടുകൾക്ക് പെൻഡിറ്റ് നൽകുന്നതുമായി ബന്ധപ്പെട്ട് നൽകിയ കൈകളിലി തിരികെ ആവശ്യപ്പെട്ട് ഒരു വിഭാഗം ബോട്ട് ഉടമകൾ രജിസ്ട്രേഷൻ, മൃസിയം, ആർക്കിയോളജി വകുപ്പ് മന്ത്രിയുടെ ഓഫീസിൽ എത്തി ബഹാദുര്മാന്ദാക്കിയതായി പറയപ്പെട്ടുന്ന സംഭവം ശ്രദ്ധയിൽപ്പെട്ടിട്ടുണ്ടോ; എക്കിൽ മന്ത്രിയുടെ ആരോപണ വിധേയരായ പേജ്സംൽ സ്ഥാപി അംഗങ്ങളെ പുറത്താക്കാൻ നിർദ്ദേശിച്ചിട്ടുണ്ടോ; വ്യക്തമാക്കുമോ;	(എ) ശ്രദ്ധയിൽപ്പെട്ടില്ല.
(ബി) മന്ത്രിയുടെ പേജ്സംൽ സ്ഥാപി അംഗങ്ങൾക്ക് കൈകളിലി നൽകിയതുമായി ബന്ധപ്പെട്ട് ബോട്ട് ഉടമകൾ മുഖ്യമന്ത്രിക്ക് പരാതി നൽകിയിട്ടുണ്ടോ; എക്കിൽ പ്രസ്തുത പരാതിയിൽ നാളിതുവരെ എന്താക്കു നടപടികൾ സീകർച്ചുവെന്ന് വ്യക്തമാക്കുമോ;	(ബി) ഇല്ല.
(സി) പ്രസ്തുത സംഭവത്തിൽ അഴിമതിക്കാരായ ഉദ്യോഗസ്ഥരെ സംരക്ഷിക്കുന്നതായി പറയപ്പെട്ടുന്ന നിലപാട് സീകർച്ചു മന്ത്രിയെ മന്ത്രിസഭയിൽ നിന്നും മാറ്റി നിർത്തിക്കൊണ്ട് അനേകംശാം നടത്തി കുറക്കാൻകു എത്തിരെ ശിക്ഷാനടപടി സീകർക്കുമോ; വിശദാംശം നൽകുമോ?	(സി) ബാധകമല്ല.

സെക്രഡറി ഓഫീസർ

139
15/10/15



GOVERNMENT OF KERALA

Abstract

Information Technology Department – Hosting of websites in State Data Centre after security auditing – Guidelines - Approved – Orders issued.

Information Technology (IT Cell) Department

G.O.(Ms) No. 43/2015/ITD

Dated, Thiruvananthapuram, 01.10.2015.

Read: - 1. G.O.(P) No.24/2009/ITD dated 29.09.2009.

2. G.O.(R) No.17/2011/ITD dated 24.01.2011.

3. Minutes of the meeting of the Apex Committee on e-Governance held on 16.07.2015.

ORDER

More than 50 websites under Government of Kerala were defaced in the month of April, 2015. Statistics clearly shows that hackers all over the world are targeting websites of various Governments and India stands among the top in the list of affected nations. Since the Government of Kerala is quite advanced in e-Governance and set a role model for other States in India, continuous defacements of websites show the Government in poor light in terms of security of its e-Governance domain.

2. While analyzing the defaced websites, it is found that all of them are hosted outside the State Data Centres and majority of these are developed using Joomla and other open source Content Management Framework. Mostly, the attacks are a result of the security patches for the software platform and framework not being updated on the servers. Security vulnerabilities in a website/application hosted in a co-hosting server at State Data Centre may adversely affect other applications hosted on the same server which may lead to mass defacement.

3. Due to the increase in the number of defacement of Government websites, Safe to Host Security Audit certificate has been mandated for hosting websites/applications in State Data Centres under Kerala State IT Mission. At both State Data Centres, different levels of security measures have been implemented at both server and network layer which has significantly helped reduce security threats.

However, it is noticed that certain departments host their websites outside State Data Centre to bypass security audits.

4. The Apex Committee on e-Governance held on 16.07.2015 has recommended to host all Government websites at State Data Centre subject to the condition that expense required for the technology upgradation for the purpose of hosting at State Data Centre should be met by the Department concerned and to get website security audit done before even if it is outside State Data Centre.

5. Government have examined the matter in detail and orders that the following guidelines should be followed by all departments and application development/ maintenance teams:

- i. Government web applications shall be hosted at the State Data Centre (SDC) that provides hosting services with adequate security controls at minimal charges. The State Data Centres are ISO 27001 certified in relation to Information Security. Hence, the Departments shall avail SDC facility in hosting any web applications rather than incurring charges for external hosting service providers not certified for any ISO security standards.
- ii. The expense required for the technology upgradation for the purpose of hosting at State Data Centre shall be met by the Department concerned.
- iii. CERT-K under Kerala State IT Mission does Security Audits for Government websites. Security auditing of the application by CERT-K or any CERT-IN empanelled agency has to be carried out in the hosting environment. A copy of the security certificate shall be provided to the hosting service provider. The hosting service provider should allow hosting on production servers only after receiving security audit certificates which needs to be maintained in records.
- iv. Any Hosting Service Provider that hosts Government web sites should have sufficient credentials to provide a secure hosting environment along with capabilities for ensuring Reliability, Availability, Scalability, Data Retention

and Backup, Redundancy and Disaster Recovery. The Data Centre should have multiple levels of security measures and controls implemented and should be audited once in a year by Third Party Auditors for Information Security against global standards such as ISO 27001.

- v. Security audit certificate also needs to be submitted along with Sub-domains registration requests to Information & Public Relations Department.
- vi. Director, Kerala State IT Mission is authorized to order de-allocation of the domain name and pull down Government web sites if security audit has not been done or if security level of the site is found to be insufficient at any point of time.
- vii. Once audited and hosted, the department shall inform the hosting service provider of any subsequent changes to the application. The provider shall verify the technical changes and evaluate if a subsequent security audit is required before the changes are deployed on the production server. If changes to the application have been deployed without intimation to the hosting service provider and without a subsequent security audit, Director, Kerala State IT Mission reserves the right to de-allocate domain name and pull down the web site.
- viii. Periodic security auditing is also necessary; the department should get the sites audited once in every 2 years by a CERT-IN empanelled agency. Hence, when work order is given to a CERT-IN empanelled agency, it may consider multiple audits over the years to be included.
- ix. Contents of the websites/applications shall not be against the interest and reputation of Government of Kerala.
- x. The websites in Government domain should follow various security guidelines/standards as specified by State or Government of India.

xi. The department is required to submit any application logs and dumps that are required by CERT-K for any analysis.

xii. A Government website that has been defaced shall be shut down. Further, it shall be enabled in production only after a subsequent Security Audit is done and the audit certificate submitted to the hosting service provider.

(By Order of the Governor),

P H KURIAN
Principal Secretary to Government

To

The Director, Kerala State IT Mission, Vellayambalam, Thiruvananthapuram
All Departments in Government Secretariat / Head of the Departments /
District Collectors

The State Informatics Officer, National Informatics Centre, Vellayambalam,
Thiruvananthapuram

The Director, Standardisation Testing and Quality Certification, Akkulam,
Sreekariyam Road, Sreekariyam, Thiruvananthapuram - 695 017

The Director, C-DAC, Vellayambalam, Thiruvananthapuram

The Registrar, C-DIT, Thiruvallam, Thiruvananthapuram

The Information & Public Relations Department

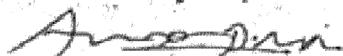
The Principal Accountant General (Audit) Kerala, Thiruvananthapuram

The Principal Accountant General (A & E) Kerala, Thiruvananthapuram

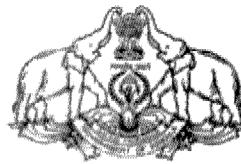
The Web & New Media, Information & Public Relations Department

SF/OC.

Forwarded / By Order



Section Officer



GOVERNMENT OF KERALA

Abstract

Electronics & Information Technology Department – Guidelines for engaging the Security Auditing Agencies- revised - orders issued

ELECTRONICS & INFORMATION TECHNOLOGY (C) DEPARTMENT

G.O.(Ms)No.44/2021/ITD

Dated, Thiruvananthapuram, 22/12/2021

Read:- 1.GO(MS) No.8/2019/ITD Dated:22/04/2019
 2.Letter No. CERT-K/11/2018-KSITM/646 dated 19/05/2021 from the Director, Kerala State IT Mission.

ORDER

As per the Government order read as 1st paper above, Government have issued guidelines specifying the rates and procedure for conducting security audit of websites and applications. Two CERT-In empaneled home grown startups viz.M/s Mirox and M/s Value Mentor Consulting LLP have been authorized for doing security auditing for applications and websites of State Government entities. At present M/s Value Mentor Consulting LLP is not in the list of agencies empaneled by CERT-in rendering M/s Mirox Cyber Security & Technology Pvt Ltd the only authorized agency to conduct security auditing for Government of Kerala establishments which is causing inordinate delay for completion of the security audit assignments received from State Government entities.

As per the letter cited 2nd, the Director, Kerala State IT Mission has requested Government to revise the guidelines for security auditing of software applications. Government have examined the matter in detail and are pleased to revise the guidelines for security auditing of websites & applications in following terms:

1. All agencies having valid CERT-In empanelment in the country are eligible to carry out the various categories of security auditing tasks from establishments of Government of Kerala. The various categories of security audit include the Vulnerability Assessment & Penetration Testing of Websites/Web application/Web services/Mobile Application, Network Security audit, VAPT Server Security Audit, Log audit etc. There will be no difficulty to carry out the security auditing procedures as the auditing agencies are connected remotely to the testing environment for audit purpose.

2. It is mandatory for Government departments/entities in the State to obtain at least three quotations from amongst the CERT-In empanelled agencies to determine the lowest price in procurement process for availing the service for security audit. In the case of internal network security audit, the audit agency must visit the local environment for carrying out the audit.
3. CERT-K shall undertake security auditing in exceptional cases with prior approval of Director, Kerala State IT Mission in the following case:
 - i. Applications which have to be made live in the production server for a limited time period, or if the total time period is less than or equal to one year for production server hosting at State Data Centre.
 - ii. A critical service/application which has to be made available to the citizen on an urgent basis. The initial security auditing for hosting those applications at State Data Centre shall be conducted and hosting will be allowed for 6 months. Certificate from a CERT-In empaneled agency has to be obtained within 6 months failing which the service/application would be removed from the production server environment without prior intimation.
4. The static websites which are developed using HTML codes / Content Management Systems (CMS) like Drupal, Word Press etc are exempted from the additional security auditing from CERT-In empaneled agencies on the condition that no third party plugins are used. The Department Organisation has to regularly update the CMS as and when the patches are released. The periodical audits must be carried out once in every two years through CERT- K.
5. Departments / Organisations shall get the websites/web applications audited once in every two years by a CERT-In empaneled agency to ensure periodical auditing. Kerala State IT Mission would ensure the periodic checksof the auditing of various applications.
6. Certification by NIC/C-DAC after the internal audits certified by its technical directors will not be considered to have authenticated security audit.

(By Order of the Governor)

BISHWANATH SINHA
PRINCIPAL SECRETARY

To ,

The Director, Kerala State IT Mission, Thiruvananthapuram
 The Registrar, High Court of Kerala, Ernakulam (with C/L)
 The Secretary, Kerala Public Service Commission, Thiruvananthapuram (with C/L)
 The Director General of Police, Thiruvananthapuram
 The Advocate General, Ernakulam
 All Departments in Secretariat (including Law and Finance)
 All Heads of Departments (Through administrative Departments)

5768826/2021/IT (C)

Chief Executive Officer/Managing Director of All PSUs/Autonomous Bodies
(Through Administrative Departments)

All District Collectors

The Registrar, All Universities in Kerala

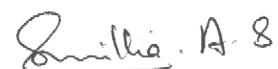
M/S Value Mentor Consulting LLP, Infopark, Thrissur (Through KSITM)

M/S Mirox Cyber Security & Technology Pvt Ltd, Technopark, Thiruvananthapuram,
(Through KSITM)

The Account General (A &E), Kerala, Thiruvananthapuram

Stock File/ Office Copy

Forwarded/ By Order



Smita A. S.
Section Officer