



තාක්ෂණ අමාත්‍යාංශය
தொழில்நுட்ப அமைச்சு
MINISTRY OF TECHNOLOGY

1106-1108, 11 වන මහල, වත් ගෝල් ෆේස්, # 1 ඒ, මැද පාර, කොළඹ 02
1106-1108, 11 වන මහල, වත් ගෝල් ෆේස්, # 1A සෙන්ටර් වීච්, කොළඹ 02
Unit 1106-1108, 11th Floor, One Galle Face Tower, # 1A, Centre Road, Colombo 02

මගේ අංකය
எனது இல
My No.

MOT/Circular/GovWeb

ඔබේ අංකය
உமது இல
Your No.

දිනය
திகதி
Date

2022-07-07

All Secretaries of Ministries
All Secretaries of the State Ministries
All Secretaries of Provincial Chief Ministries
All District Secretariats
All Heads of Departments
All Heads of Corporations and Statuary Boards

SECURING OF GOVERNMENT WEBSITES AND WEB APPLICATIONS

01. With the rapid adoption of digital technologies within Sri Lanka in the recent years, Government Websites and Web Applications have become prime targets of cyber-attacks with a significant increase in website compromises, which could affect the national security and safety, economic, social and cultural dimensions of country.
02. Therefore, this Ministry in collaboration with the Information and Communication Technology Agency of Sri Lanka (ICTA) and Sri Lanka Computer Emergency Readiness Team (Sri Lanka CERT) issues this circular with the aim of increasing the cyber resilience of government institutes' websites and web applications. Thus, all government institutes and statutory bodies are required to adhere to the instructions mentioned herein to prevent or mitigate website or web application compromise.
03. The Websites and Web Applications of government institutions shall be developed with security measures inbuilt into its respective structure. A security by design approach will be utilized to ensure security measures are taken into considerations through the development lifecycle. Websites and Web Applications shall be designed with the technical assistance of ICTA.
04. All new websites and web applications require security assessments to be conducted by Sri Lanka CERT prior to the production release to ensure that these are risk free at the time of launch.
05. The government organization is responsible for the security of its websites and web applications.
06. It is mandatory that government organizations carry out a Security Assessment through Sri Lanka CERT at least on an annual basis. Further, it is required to carry out a Security Assessment in the following instances:
 - (a). after an incident has occurred
 - (b). after a major change is made
 - (c). after changes have been made to the platform or hosting environment
 - (d). after the spread of virus/malware
 - (e). after changes to policies, standards, and guidelines or
 - (f). as determined by the organization
07. The government organizations shall follow the instructions outlined in the following security guidelines published by Sri Lanka CERT.
 - (a). Website Security Guidelines for Government Organizations,
 - (b). Web Application Security Guidelines for Government Organizations

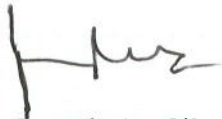
දුරකථන
தொலைபேசி
Telephones } +94112334562

ෆැක්ස්
பெக்ஸ்
Fax } +94112334576

ඉ-මේල්
மின் அஞ்சல்
E-mail } info@mot.gov.lk

- (c). Annexure of Web Application / Website Security Guideline
- (d). Technical Guide for Website and Web Application Security

08. The aforementioned guidelines can be downloaded from the following websites;
www.cert.gov.lk : Refer “Knowledge base – Resource” tab.
www.onlinesafety.lk : Refer “Resource” tab.
09. All Security Assessments shall be conducted by Sri Lanka CERT at a nominal fee based on the scope of the engagement. The fee should be allocated from the annual budget of the government organizations.
10. It is mandatory to report occurrences of any cyber incident related to the government organization’s website and web applications to Sri Lanka CERT by the respective organization. (Maximum within 24 hours)
11. Sri Lanka CERT shall provide assistance to the Government Organizations for cyber security related issues. ICTA shall provide infrastructure support and assisting in implementation.
12. In addition to the security guidelines in this circular, you are advised to follow the “Guidelines for Developing Sri Lanka Government Websites” <https://bit.ly/gosl-website-guide> document by ICTA to ensure your websites are developed and maintained as specified by the ICTA.
13. For any further clarifications Government Organizations may contact Sri Lanka CERT (0112691692, websec@cert.gov.lk) and ICTA (0112369099, info@icta.lk).



Jayantha De Silva
Secretary
Ministry of Technology

Website Security Guidelines for Government Organizations



An Agency under the Ministry of Technology

With the advancement of technology, there has been a significant increase in information security threats that websites are being subjected to. This guideline outlines the basic principles that are to be followed by government organizations to prevent or mitigate website defacement or compromise.

Version 1 Issue: 22 Feb 2022

Prior to Development

- Identify the criticality of the contents of the website based on the types of information which will be published, processed and stored, and determine security requirements for the protection of the website in accordance with the Technical Guidelines for Web Application and Website Security issued by Sri Lanka CERT.
- Include mandatory security requirements to the tender document as depicted in Table 10-1 Section 10 of the Information and Cyber Security Implementation Guide, an extract is attached as Annexure A.
- A clause shall be included in tender document to ensure that the website is developed and hosted in accordance with the Technical Guidelines for Web Application and Website Security.
- If the website offers a service through a web application, refer to the Web Application and Website Security Guidelines for Government Organizations for more information.

Design and Development

- Websites of government organizations shall be in the “gov.lk” domain name.
- Websites shall use latest and stable version of content management tool (CMS).
- Website Security Risks mentioned in “OWASP” shall be taken into consideration when designing and developing the website.
- Input validation shall be in place for allowing input of the data fields at the client and server sides for data types (integer, text, etc.) and data specification (For example, the number of digits in telephone number).
- Malware detection through scanning is essential when attachments in the form of pdf, word, excel, text files are uploaded to the website. Encrypted / compressed files shall not be allowed to be uploaded on the website. Exceptions shall only be accommodated with the recommendation of Sri Lanka CERT.
- Ensure “HTTPS” has been enabled on the web server. Login details shall only be delivered over HTTPS, login form is delivered over HTTPS, and tokens only delivered over HTTPS.

- Use two-way SSL authentication for accessing the backend (or CMS) of the website. Sensitive information must be encrypted in transit and at rest. E.g. Storing in databases, file servers, backups and when managing unstructured data for compliance, privacy and security as mentioned in the Data Protection Regulation.
- Establish multifactor authentication for users who have access to CMS or backend. Enforcing strong passwords policies is also essential for government organizations as mentioned in the Section 4.4. of the Minimum Information Security Standards for Government Organizations.
- Developer shall limit the usage of third-party components in the form of plugins and codes. In the event if such components are to be used, a comprehensive risk assessment is to be performed before deployment.
- Default and/or vendor supplied passwords shall be changed or disabled prior to deployment.
- Government organizations shall take into consideration the security requirements mentioned under Section 2.1.1. of the Technical Guideline for Web Application and Website Security.
- Whenever possible, an effective CAPTCHA shall be implemented to minimize potential attacks.
- Prior to deployment of the website, an assurance shall be obtained from the vendor that website is developed in accordance with the Technical Guideline for Web Application and Website Security.
- A security assessment must be carried out through Sri Lanka CERT prior to the production release.

Deployment and Maintenance

- If the website is developed by a vendor, the government organization shall always have an active maintenance agreement with the vendor.
- The website CMS, database, operating system and webserver platform need to be patched and updated with latest security patches.
- Access credentials to the website CMS or backend shall be given to authorized users only. Sharing credential with unauthorized users shall be strictly prohibited.
- If the website administrator uses their own devices to access the CMS or the website administration panel, it is essential the stated devices are adequately secured and updated with security patches.

- A security assessment is to be performed by Sri Lanka CERT at least on an annual basis. Other circumstance in which that organization shall perform security assessment include, after an incident has occurred or after a change is made to the website, platform or hosting environment, standards, policies and guidelines, after the spread of virus/malware, or as determined by the organization.
- Maintain a formal and up to date copy of the Website on a host that is not connected to the Internet. Maintaining regular backups of website, content and data are essential.

Retirement and Disposal

- At the decommissioning stage, the website shall be securely disposed of to ensure that its data and other information assets cannot be accessed and recovered by unauthorized individuals as mentioned in the Section 4.14. of the Minimum Information Security Standards for Government Organizations.