



# තාක්ෂණ අමාත්‍යාංශය தொழில்நுட்ப அமைச்சு MINISTRY OF TECHNOLOGY

1106-1108, 11 වන මහල, වන් ගෝල් ශේෂ්, # 1 ඒ, මැද පාර, කොළඹ 02  
1106-1108, 11 වැනු மாடி, வந்த கோல் பேஸ், # 1A சென்டர் வீதி, கொழும்பு 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

### වක්‍රලේඛය

- සියලුම අමාත්‍යාංශ ලේකම්වරුන්
- සියලුම රාජ්‍ය අමාත්‍යාංශ ලේකම්වරුන්
- සියලුම පළාත් ප්‍රධාන ලේකම්වරුන්
- සියලුම දෙපාර්තමේන්තු ප්‍රධානීන්
- සියලුම දිස්ත්‍රික් ලේකම්වරුන්
- සියලුම රාජ්‍ය සංස්ථා/ව්‍යවස්ථාපිත මණ්ඩල ප්‍රධානීන්

### රජයේ වෙබ් අඩවි සහ වෙබ් යෙදුම් සුරක්ෂිත කිරීම

01. මෑත භාගයේ රජයේ වෙබ් අඩවි සහ වෙබ් යෙදුම් විවිධ සයිබර් ප්‍රහාරවලට නතු වීමේ ප්‍රවණතාවයක් දැකිය හැකි අතර එමඟින් රාජ්‍ය ආයතන සහ තොරතුරු තාක්ෂණ පද්ධති පිළිබඳව වන මහජන විශ්වාසය පලදා විම පමණක් නොව ජාතික ආරක්ෂාවට ද, සමාජීය යහපැවැත්ම ද සහ ආර්ථික කටයුතුවලට බලපෑම් ඇතිවිය හැකිය.
02. එබැවින්, තාක්ෂණ අමාත්‍යාංශය, ශ්‍රී ලංකා පරිගණක හදිසි ප්‍රතිචාර සංසදය (Sri Lanka CERT) සහ ශ්‍රී ලංකා තොරතුරු හා සන්නිවේදන තාක්ෂණ නියෝජිතායතනය (ICTA) සමඟ එක්ව රජයේ ආයතනවල වෙබ් අඩවි (websites) සහ වෙබ් යෙදුම්වල (web applications) සයිබර් ආරක්ෂණය ඉහළ නැංවීමේ අරමුණින් මෙම වක්‍රලේඛය නිකුත් කර ඇත. මේ අනුව, සියලුම රාජ්‍ය ආයතන සිය වෙබ් අඩවි සහ වෙබ් යෙදුම් සයිබර් ප්‍රහාරයන්ට ලක්වීම වැළැක්වීමට හෝ අවම කිරීමට මෙම වක්‍රලේඛයේ සඳහන් උපදෙස් පිළිපැදිය යුතු වේ.
03. රාජ්‍ය ආයතනවල වෙබ් අඩවි සහ වෙබ් යෙදුම් සංවර්ධනයේදී, ආරක්ෂක ක්‍රමවේදයන් එහි නිර්මාණාත්මක චක්‍ර ජීවන ක්‍රමය තුළට අන්තර්ගත කළ යුතුය. ඒවායේ සංවර්ධන ජීවන චක්‍රය (systems development lifecycle) පුරාවටම ආරක්ෂාව තහවුරු කරගත් මෘදුකාංග සංවර්ධනය ක්‍රමවේදයන් භාවිතා කළ යුතුය. තවද, වෙබ් අඩවි සහ වෙබ් යෙදුම් නිර්මාණය කිරීමේදී ICTA ආයතනයෙහි තාක්ෂණික සහාය ලබා ගත යුතුය.
04. සියලුම වෙබ් අඩවි සහ වෙබ් යෙදුම් භාවිතය සඳහා මුදා හැරීමට පෙර Sri Lanka CERT ආයතනය විසින් සිදු කරනු ලබන ආරක්ෂණ විගණනයක් (Security Assessment) මගින් ඒවායේ ආරක්ෂිත දෝෂ රහිත බව සහතික කර ගත යුතුය.
05. රාජ්‍ය ආයතනයේ වෙබ් අඩවි සහ වෙබ් යෙදුම්වල ආරක්ෂණය පිළිබඳ වගකීම් එම ආයතනය සතු වේ.
06. රාජ්‍ය ආයතන තමන් සතු සියලුම වෙබ් අඩවි සහ වෙබ් යෙදුම් අවම වශයෙන් වාර්ෂිකව, Sri Lanka CERT ආයතනය මගින් ආරක්ෂණ විගණනයකට ලක් කර ගැනීම අනිවාර්ය වේ. තවද, පහත සඳහන් අවස්ථා වලදී ද වෙබ් අඩවි සහ වෙබ් යෙදුම් සඳහා ආරක්ෂණ විගණනයක් Sri Lanka CERT ආයතනය මගින් සිදු කරගැනීම අත්‍යාවශ්‍ය වේ:

- (අ) වෙබ් අඩවි සහ වෙබ් යෙදුම්වලට සිදු වූ යම් ආරක්ෂණ සිදුවීමකින් අනතුරුව
- (ආ) වෙබ් අඩවි සහ වෙබ් යෙදුම්වල සිදු කරන ලද ප්‍රධාන වෙනස් කිරීමකින් අනතුරුව

- (ඇ) වෙබ් අඩවි සහ වෙබ් යෙදුම් ස්ථාපනය කර ඇති පරිගණකවල හෝ මෘදුකාංගවල සිදු කරන ලද යම් වෙනසකින් අනතුරුව
- (ඈ) වෛරස්, හෝ අනිෂ්ට මෘදුකාංග පැතිරීමකින් පසුව
- (ඉ) ප්‍රතිපත්ති, ප්‍රමිතීන් සහ මාර්ගෝපදේශ වල සිදු වූ යාවත්කාලීන කිරීමකින් පසුව හෝ
- (ඊ) ආයතනය විසින් තීරණය කරනු ලබන ඕනෑම අවස්ථාවකදී

07. Sri Lanka CERT ආයතනය විසින් ප්‍රකාශයට පත් කරන ලද පහත සඳහන් ආරක්ෂණ මාර්ගෝපදේශවල දක්වා ඇති උපදෙස් රාජ්‍ය ආයතන අනුගමනය කළ යුතු වේ.

- (අ) රාජ්‍ය ආයතන සඳහා වෙබ් අඩවි ආරක්ෂණ මාර්ගෝපදේශය (Website Security Guidelines for Government Organizations)
- (ආ) රාජ්‍ය ආයතන සඳහා වෙබ් යෙදවුම් ආරක්ෂණ මාර්ගෝපදේශය (Web Application Security Guidelines for Government Organizations)
- (ඇ) වෙබ් යෙදුම් / වෙබ් අඩවි ආරක්ෂණ මාර්ගෝපදේශයෙහි ඇමුණුම (Annexure of Web Application/Website Security Guideline)
- (ඈ) වෙබ් අඩවි සහ වෙබ් යෙදුම් ආරක්ෂාව සඳහා වන තාක්ෂණික මාර්ගෝපදේශය (Technical Guide for Website and Web Application Security)

08. ඉහත සඳහන් මාර්ගෝපදේශ පහත වෙබ් අඩවියෙන් බාගත කළ හැකිය;  
[www.cert.gov.lk](http://www.cert.gov.lk): “Knowledge Base - Resources” යොමුව වෙත පිවිසෙන්න.  
[www.onlinesafety.lk](http://www.onlinesafety.lk) : “Resources” යොමුව වෙත පිවිසෙන්න.


09. Sri Lanka CERT ආයතනය විසින් සියලුම ආරක්ෂණ විගණනයන් එහි පරාසය (Scope) මත පදනම්ව යම් ගාස්තුවකට යටත්ව සිදු කරනු ඇත. රාජ්‍ය ආයතන සිය වාර්ෂික අයවැයෙන් මේ සඳහා අවශ්‍ය මූල්‍ය ප්‍රතිපාදන වෙන් කර ගත යුතුය.

10. රාජ්‍ය ආයතන සිය වෙබ් අඩවියට සහ වෙබ් යෙදුම්වලට අදාළ ඕනෑම සයිබර් ආරක්ෂණ සිදුවීමක්, Sri Lanka CERT ආයතනය වෙත වාර්තා කිරීම අනිවාර්ය වේ. (උපරිම පැය 24 ක් ඇතුළත)

11. සයිබර් ආරක්ෂාව සම්බන්ධයෙන් වන ගැටළු සඳහා Sri Lanka CERT ආයතනය රාජ්‍ය ආයතනවලට සිය තාක්ෂණික සහාය සැපයිය යුතුය. තවද, ICTA ආයතනය විසින් රාජ්‍ය ආයතන වල වෙබ් අඩවි සහ වෙබ් යෙදුම්වලට අවශ්‍ය යටිතල පහසුකම් සැපයීම සහ අදාළ ආරක්ෂණ ක්‍රමවේද ක්‍රියාවට නැංවීම සඳහා සහාය විය යුතුය.

12. මෙම වක්‍රලේඛයේ ආරක්ෂක මාර්ගෝපදේශවලට අමතරව, වෙබ් අඩවි සංවර්ධනය සහ නඩත්තු කිරීම සඳහා ICTA ආයතනය විසින් නිකුත් කර ඇති “ශ්‍රී ලංකා රජයේ වෙබ් අඩවි සංවර්ධනය සඳහා මාර්ගෝපදේශ” <https://bit.ly/gosl-website-guide> ලේඛනය ද අනුගමනය කරන ලෙස ඔබට උපදෙස් දෙනු ලැබේ.

13. මේ පිළිබඳ වැඩිදුර විස්තර Sri Lanka CERT ආයතනය (0112691692, [websec@cert.gov.lk](mailto:websec@cert.gov.lk)) සහ ICTA ආයතනය (0112369099, [info@icta.lk](mailto:info@icta.lk)) මගින් ලබා ගත හැකිය.

  
 ජ්‍යෙෂ්ඨ ද සිල්වා  
 ලේකම්  
 තාක්ෂණ අමාත්‍යාංශය

# Website Security Guidelines for Government Organizations



An Agency under the Ministry of Technology

Version 1 Issue: 22 Feb 2022

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.

## 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.