ඩිජිටල් ආර්ථික අමාත්‍යාංශය
டிஜிட்டல் பொருளாதார அமைச்சு
Ministry of Digital Economy

1101, 11 වන මහල, වන් ගෝල් ෆේස්, # 1ඒ, මැද පාර, කොළඹ 02
1101, 11 வது மாடி, வந் கோல் பேஸ், # 1A, சென்டர் வீதி, கொழும்பு 02
Unit 1101, 11th Floor, One Galle Face Tower, # 1A, Centre Road, Colombo 02

/modesrila
mode.gov.

මගේ අංකය / எனது இல / My No. MODE/DEV/GENERAL/SLCERT VII

ඔබේ අංකය / உமது இல / Your No.

දිනය / திகதி / Date 22 · 06 ..2026

Circular No: MODE/2026/02

All Secretaries of Ministries
All Chief Secretaries of Provincial Councils
All Heads of Departments
All Heads of Corporations, Statutory Bodies and Government Owned Companies

**Implementation of Information and Cyber Security Policy for Government Organizations**

1. Reference to the Circular MOT/2023/01 issued by the Ministry of Technology dated 2nd May 2023.

2. Recent cyber security incidents and rising financial fraud cases in Sri Lanka have highlighted the urgent need to strengthen the security of government digital systems. Cyber-attacks and online financial scams threaten sensitive data, disrupt public services, and cause economic losses, making strong cyber security measures essential for protecting national digital infrastructure.

3. As you are aware, the Cabinet of Ministers has approved the Information and Cyber Security Policy for Government Organizations (hereinafter referred to as the "Policy"), which shall be implemented by all government organizations defined as "Public Authorities" under the Right to Information Act No. 12 of 2016. The Policy defines the baseline security standards for the government.

4. The primary objective of the Policy is to protect data and IT systems used by government organizations from unauthorized access, cyber threats, and disruptions. The implementation of the Policy includes adherence to prescribed information security standards, procedures, and controls, together with the implementation of the necessary hardware, software, and infrastructure safeguards.

5. Heads of Organizations are hereby reminded that the implementation of the Policy in their respective organizations is mandatory. Further, the Government has established the National Cyber Security Operations Centre (NCSOC) to real-time monitoring of cyber security incidents on Critical National Information Infrastructure (CNII), and established Threat Hunting and Malware Analysis Lab (MATH Lab) to vulnerabilities of the public facing websites. CNII are required to obtain the services of NCSOC, and all critical government

දුරකථන / தொலைபேசி +94112334562
ෆැක්ස් / பெக்ஸ் +94112334576
ඉ-තැපෑල / மின் அஞ்சல் info@mod

organizations are obligated to address and resolve incidents escalated by the MATH Lab in a timely manner as per the Ministry of Digital Economy Circular No. MODE/2026/01 dated 03 March 2026.

6. Government organizations are required to obtain security assessments for their systems and digital infrastructure on a priority basis, as stipulated in Section 4.3.18 of the policy.

7. As directed by the Cabinet of Ministers, it is a responsibility of the Heads of the organizations to allocate necessary budgets for cyber security activities through the annual budget.

8. All organizations shall appoint an Information Security Committee (ISC), an Information Security Officer (ISO), and an Assistant Information Security Officer (AISO) for the effective implementation of the Policy and formally assign information security responsibilities in accordance with the approved Terms of Reference in Annex 1. Organizations that have not yet appointed an ISO and AISO are hereby instructed to make such appointments with immediate effect and communicate the details to Sri Lanka CERT without delay.

9. Further, if previously appointed ISOs or AISOs have been transferred, retired, resigned, or are otherwise unable to continue performing their assigned responsibilities, replacement officers shall be appointed immediately, and the updated nomination details shall be informed to Sri Lanka CERT.

10. In the field of cybersecurity, the human factor remains one of the most vulnerable elements despite existing technical safeguards. Accordingly, every government organization shall ensure the continuous conduct of cybersecurity awareness, capacity-building, and training programmes for employees at all levels without further delay. Furthermore, such programmes should be incorporated into the organization's annual training plans.

11. The Information and Cyber Security Policy for Government Organizations are available in all three languages and can be downloaded from the "Resource Tab" of Sri Lanka CERT official website: www.cert.gov.lk. *Home Page => Resource => Policy & Guidelines.*

12. To assess the implementation progress, all Government Organizations shall complete the Chapter 6 questionnaire of the Information and Cyber Security Policy for Government Organizations (attached as Annex 4) on a bi-annual basis and submit the same to Sri Lanka CERT via email to chaturanga@cert.gov.lk on or before 30th June and 31st December of each year.

13. Should you require further clarification or assistance please contact following officials of Sri Lanka CERT.

a. Implementation of the Information and Cyber Security Policy: Mr Chaturanga Angammana, Lead Information Security Engineer, 074 084 5583, 011 2 692 692 , and email chaturanga@cert.gov.lk.

b. National Cyber Security Operations Center: Mr. Mahinda Kandapahala, Chief Information Security Officer, 077 148 4629, 011 2 692 692 , and email mahinda@cert.gov.lk, info@ncsoc.gov.lk.

c. Malware Analysis and Threat Hunting Lab: Mr. Senalike Dewalawatta, Manager- IS, 076 932 4038, 011 2 692 692, and email senalike@cert.gov.lk

d. Technical Assessments: Mr. Nirosha Ananda, Chief Information Security Officer,076 314 3287, 011 2 692 692, and email nirosha@cert.gov.lk.

e. Capacity Building: Mr. Thilina Dissanayake, Project Manager – Capacity Building, 077 295 4866, 011 2 692 692, and email thilina@cert.gov.lk.

**Waruna Sri Dhanapala**
Secretary

Copy: Secretary to the President, Presidential Secretariat - f.y.i. please
Secretary to the Prime Minister, Prime Minister's Office - f.y.i. please
Secretary to the Cabinet Minister, Cabinet Minister's Office - f.y.i. please
Auditor General, National Audit Office of Sri Lanka - f.y.i. please

## Annex 1: Terms of Reference of ISC, ISO and AISO

### a. Appointment of Information Security Committee (ISC)

*Reference: Sections 4.1.1, 4.1.2 (a), (b), (c), and 4.1.3 of the Information and Cyber Security Policy*

a. The organization shall appoint an ISC to provide strategic directions to the activities related to the implementation of the Policy.

b. Committee's responsibilities shall include but are not limited to reviewing and approving all information security controls, action plans, risk management strategies, incident response plans and disaster recovery plans and other activities carried out by the ISO in implementing the Policy.

c. The Head of the Organization shall chair the Committee. The Committee shall consist of the ISO, AISO, officer in charge of the subject of IT, the (Chief) Internal Auditor, and assets custodians (refer Policy for their roles and responsibilities).

d. The Head of the Organization shall provide leadership to implement the Policy, allocate necessary resources, and ensure regular ISC meetings with proper monitoring and record-keeping of cyber security activities.

e. (Chief) Internal Auditor shall be assigned the responsibility of assessing the progress of adopting the Policy at the organization.

f. The ISC shall ensure that identified cyber security risks, incidents, vulnerabilities, and non-compliance issues are reported, addressed, monitored, and escalated appropriately in a timely manner.

g. The ISC shall take necessary steps to connect with the National Cyber Security Operations Center (NCSOC), based on the criticality of the organization's services, and obtain other relevant services offered by Sri Lanka CERT to ensure the protection and resilience of organizational information systems and digital infrastructure.

### b. Appointment of Information Security Officer (ISO)

*Reference: Section 4.1.2 (b) of the National Cyber Security Policy*

**Experience and Qualifications**

a. Shall be a senior officer representing the first or second tier management level of the organization with adequate authority to coordinate organization-wide cyber security and information security initiatives.

b. Shall possess sound knowledge and understanding of the organization's information systems, IT infrastructure, digital services, networks, and operational processes.

c. Possession of academic or professional qualifications in Information Technology (IT), Information Security (IS), Cyber Security, Computer Science, Networking, Systems Administration, Digital Governance, or related fields shall be considered as a significant advantage.

d. A minimum qualification of a Diploma in IT, IS, or Cyber Security is desirable. Preference shall be given to officers possessing Bachelor's or Master's Degrees in IT, IS, Cyber Security, Computer Science, or related disciplines.

**Annex 2: Nomination of ISO and AISO**

1. **Details of the organization**

| | | | |
|---|---|---|---|
| Name of the Ministry/ Name of the Department | | | |
| Name of the line ministry (If applicable) | | | |
| Address | | Email | |
| | | Telephone | |
| | | Fax | |

2. **Details of the ISO (Nomination of ISO should be done as per the qualification and experience criteria defined in the Annex 1)**

| | | |
|---|---|---|
| ISO's Name with Initials | | |
| Designation | | |
| Experience | | |
| Educational Qualifications | | |
| Contact details | Fixed | |
| | Mobile | |
| | Official e-Mail | |
| | Fax | |

3. **Details of the AISO (Nomination of AISO should be done as per the qualification and experience criteria defined in the Annex 1)**

*Priority shall be given to officers possessing qualifications, certifications, and hands-on experience*

**Annex 3: List of Government Organizations to Implement the Policy in the First Round**

1. Department of Pensions
2. Department of Irrigation
3. Medical Supplier Division
4. Department of Examinations
5. Department of Inland Revenue
6. Department of Motor Traffic
7. Department of Immigration and Emigration
8. Department of Auditor General
9. Department of Registration of Persons
10. Registrar General's Department
11. Department of Fisheries and Aquatic Resources
12. Import and Export Control Department
13. Sri Lanka Customs
14. Sri Lanka Ports Authority
15. National Water Supply and Drainage Board
16. Sri Lanka Police
17. Employees' Trust Fund Board
18. Employees provident Fund
19. Airport & Aviation Services Limited
20. Mahaveli Authority
21. Civil Aviation Authority of Sri Lanka
22. LGII/ ICTA
23. Telecommunication Regulatory Commission
24. Ceylon Electricity Board
25. Ceylon Petroleum Corporation
26. Ceylon Petroleum Storage Terminal Limited (CPSTL)
27. Central Bank of Sri Lanka
28. LTL Holdings
29. Ministry of Disaster Management (Mitigation)
30. Ministry of Finance
31. Ministry of Foreign Affairs
32. Ministry of Defense
33. President's Office
34. Cabinet Office
35. Election Commission of Sri Lanka
36. Prime Minister's Office
37. Sri Lanka Parliament