Ministry of Digital Economy

Guidelines No. 01/2026

Interim Guidelines on Optimal Use of Digital Technologies in Remote Service Delivery by the Public Sector

21-04-2026

Context and Directive

The Government of Sri Lanka is taking several steps to mitigate the pressure on national fuel stocks due to the energy and overall fuel supply constraints currently affecting Sri Lanka in the face of unexpected global trends that emerged after February 28, 2026.

Accordingly, the Committee on the Systematic Maintenance of Public Service, chaired by the Prime Minister, directed the Ministry of Digital Economy to explore the possibility of resorting to remote work as much as possible, in consultation with the Ministry of Public Administration, Provincial Councils and Local Government, and to provide recommendations on the optimal use of digital technologies.

Heads of departments are encouraged to take necessary measures to improve the digital technology skills of officers and other staff members at each workplace and to strictly safeguard the security of information related to their duties, in order to contribute to the optimization of public sector services in the Digital Economy Plan, which is a major development approach of the current government.

Accordingly, this set of guidelines outlines several approved methods for performing key administrative tasks from home or office/workplace using digital technologies.

For further clarifications regarding this set of guidelines, please contact Ms. Chanaki Mallikarachchi, Director (Information Technology), Ministry of Digital Economy (Email: dir_it@mode.gov.lk / Telephone: 0777710253).

1. Meetings and Virtual Collaboration

To effectively minimize physical commuting and align with national efforts to conserve fuel, all internal and external government meetings are strongly encouraged to be conducted through digital means. This proactive measure is essential to eliminate the requirement for participants to travel, thereby significantly reducing the strain on national fuel supplies.

1.1. Guidelines for Effective and Secure Virtual Meetings

Officers at all levels are encouraged even if they present at their desk/seat. This will help preventing unnecessary inter-office commute by large numbers of participants)

To ensure efficient communication and maintain strict information security protocols, government employees are directed to adopt the following guidelines when conducting virtual meetings.

A. Mandatory Access Control:

i. **Guidance for Chair or nominated convenor** - e.g. roll call, participant validation and liveliness test
ii. Always enable **"Waiting Rooms"** to screen and verify the identity of participants before allowing them to enter the virtual meeting.
iii. Never share meeting links on public forums or social media. Distribute them exclusively via **official calendar invites, email, or secure direct messages**.
iv. Use your **official government email address** for sending all meeting invitations and related documents.

B. Data Confidentiality and Handling:

i. **Never send classified or highly sensitive government data** over consumer messaging apps.
ii. All sensitive documents or presentations shared during or before the meeting **must be password-protected** before transmission.
iii. For password-protected files, use **out-of-band password sharing** by sending the document and the password through separate communication channels (e.g., file via email, password via a secure direct message).

C. Endpoint and Network Security:

i. Ensure that the devices used for remote work have **up-to-date antivirus software** installed.
ii. **Avoid using unsecured public Wi-Fi networks** when accessing or transmitting official government documents or participating in sensitive meetings.

D. **Preparation & Effectiveness:**

i. **Test Your Connection and Hardware:** Before joining, make sure your internet connection is stable and that your camera and microphone are connected and functioning.
ii. **Share Materials in Advance:** Attach necessary documents, spreadsheets, or presentations to the calendar invite so participants can preview relevant files and come prepared to contribute. Guidance by a focal pointy officer/ facilitator is recommended for this purpose
iii. **Effective Use of AI tools:** There are AI tools for voice recognition (in English) that enables transcription and to support effective Meeting Minutes taking / summarizing.
iv. **Confidential Environment:** Use due care to ensure confidentiality when participating in meetings by utilizing a headset / headphones or by conducting the meeting from a dedicated, private space where confidentiality is guaranteed.

1.2. Proposed Platform - meet.gov.lk

The primary and recommended platform for large-scale and highly sensitive government meetings is **https://meet.gov.lk**, the government's dedicated digital platform designed to conduct virtual meetings securely and without time restrictions.

To obtain a login for their agency or division to access this platform, government officers/employees must contact the helpdesk of GovTech Sri Lanka:

i. Helpdesk Number: 0112 497900
ii. Helpdesk Email: helpdesk@noc.gov.lk

Alternatively, government officers/employees are allowed to make use of free-to-use video conferencing solutions or any other commercially procured web conferencing solutions for official meetings:

i. Google Meet: Free for meetings up to 60 minutes.
ii. Microsoft Teams: Free for meetings up to 60 minutes.
iii. Zoom: Free for meetings up to 40 minutes.
iv. Cisco Webex: Free for meetings up to 40 minutes.

Respective Heads of Departments are advised to obtain the services of its Information & Communication Technology officers at various levels to ascertain the appropriate communication methodology depending on the nature and sensitivity of the meetings.

2. Guidelines for Use of Electronic Documents and Signatures for Remote Work

2.1. Purpose

In order to facilitate continuity of government operations during periods of restricted travel or remote work arrangements, public officers are encouraged to utilize electronic communication and electronic document authentication methods in accordance with the **Electronic Transactions Act No. 19 of 2006 amended by Act No 25 of 2017)**.

2.2. Legal Basis

The following provisions of the Electronic Transactions Act No. 19 of 2006 enable electronic processing of official documents:

Section 4 – Legal recognition of electronic records
Section 5 – Electronic records satisfying writing requirements
Section 7 – Legal recognition of electronic signatures

Accordingly, documents shall **not be denied legal validity solely because they exist in electronic form**.

2.3. Use of Electronic Documents

Public officers may create, circulate, and store official documents electronically through:

i. Official email systems
ii. Government collaboration platforms
iii. Document management systems
iv. Secure cloud services approved by the government

Examples include:

i. Internal memos
ii. Approvals
iii. Meeting minutes
iv. Reports
v. Administrative correspondence

2.4. Electronic Authentication of Documents

Where a document requires the approval or signature of an officer, authentication may be performed using electronic methods including:

Acceptable methods

I. Scanned signature image inserted into the document
II. Digital signatures using approved signing tools
III. Typed signature block with designation
IV. Approval communicated through official government email

Example:

> Approved
>
> **[Signature Image]**
>
> A. B. Perera
> Director – Finance
> Ministry of XXX
> Date: 15 March 2026

2.5. Requirements for Valid Electronic Authentication

To comply with **Section 7 of the Electronic Transactions Act**, the authentication method must:

i. Identify the officer approving the document
ii. Indicate the officer's intention to approve the document
iii. Be reliable and appropriate for the purpose of the document

2.6. Recommended Best Practices

Officers are encouraged to follow the following practices:

i. Identity clarity

Include:

- Full name
- Designation
- Department
- Date – Maintain a standard format such as YYYY-MM-DD

ii. Document integrity

Documents should preferably be shared in PDF format to prevent modification after approval. Respective officers should be advised to add appropriate watermarks if so requires (e.g. Confidential, For Official Purposes Only etc.)

iii. Official Communication Channels

Documents should be transmitted using:

- Official government email addresses (e.g. at least one official email facility to receive and send communications electronically, such as info@<orgname>.gov.lk)
- Approved collaboration platforms (accessed through appropriate user credentials)

iv. Record Keeping

Record keeping must be carried out in accordance with the provisions of the Right to Information Act, Act No. 12 of 2016 and the National Archives Act, Act No. 48 of 1973 as amended by Act No. 30 of 1981.

v. Documents Requiring Physical Signatures

Where other laws explicitly require physical signatures, notarization, or sealing, the traditional process must still be followed.

Examples may include:

- Notarized legal instruments
- Land transactions
- Statutory declarations

vi. Security Considerations

Officers shall ensure:

- Electronic signatures are not shared with others
- Signature images are stored securely
- Official documents are not approved through personal email accounts

2.7. Physical-to-Digital Alternative

If e-signing platforms cannot be used, employees should follow this manual digitization process:

1. Print the required document at your remote location.
2. Sign the document clearly using a blue pen.
3. Scan the signed document using a secure scanning application (such as Adobe Scan) to convert it back into a high-quality PDF. Officers may use desktop or mobile scanners for this purpose.
4. Re-share the finalized PDF via Official Email or WhatsApp, strictly adhering to the security protocols outlined in Section 3.

3. Document Sharing and Transfer

To ensure the seamless continuation of administrative duties, employees are to utilize secure digital channels for document sharing.

i. **Official Email:** Use your official government email address (@xxx.gov.lk or similar) as the primary method for sharing scanned or digitally generated PDFs and official documents.
ii. **Encrypted Messaging:** End-to-end encrypted messaging applications like WhatsApp may be used for rapid communication and transferring non-classified documents.
iii. **Information Security Protocols:** Never send classified or highly sensitive government data over consumer messaging apps.
iv. **Password Protection:** All sensitive PDFs and documents must be password-protected before transmission.
v. **Out-of-Band Password Sharing:** Send the document password through a different communication channel than the document itself (e.g., send the file via email, and the password via a direct WhatsApp message).
vi. **Hardware and Network Security:** Ensure that the devices used to work from home have up to date antivirus software installed. Avoid using unsecured public Wi-Fi networks when accessing or transmitting official government documents.

4. General

1. Make sure to optimize digital resources for respective workload depending on the nature of the assignment. A prior work plan for each officer would be helpful in case the officers who work remotely are not assigned with a device for their own and should be provided with shared resources (laptop computers etc.)

2. All Heads of Departments should ensure that proper mechanism when assets are permitted to move out of office for remote work, including of physical safety of devices and security of software and data stored in them.

Waruna Sri Dhanapala
Secretary
Ministry of Digital Economy

www.mode.gov.lk