ITO’s Circular No: 01/2025

IT Department and Chief Information Security Officer (CISO),

SriLanka Telecom PLC,

Colombo 01.
01 June, 2025

To All Employees,

REVISED Data Security & Acceptable Use Policy

1. Purpose

This circular introduces the comprehensively revised "Data Security & Acceptable Use Policy." This new policy is updated to reflect the security landscape of 2025 and our company's full return to in-office operations. It addresses new threats and technologies that were not prevalent when our previous policies were written.

2. Scope

This policy is effective June 15, 2025, and applies to all employees, contractors, and temporary staff who use any company equipment or access the company network.

3. Supersession of Previous Policy

This new policy is a complete replacement for our previous technology guidelines. This circular **supersedes and repeals** the following:

- **ITO’S CIRCULAR NO: 01/2022: "NEW Technology & Data Security Policy for Hybrid Work"**

The "Hybrid Work" policy (ITO’S CIRCULAR NO: 01/2022) is no longer relevant to our in-office model, and its focus on home network security and VPNs is outdated. All employees must now adhere to the new policies outlined in this document.

4. Key Policy Updates

While all employees must read the full policy, key changes include:

- **Personal Device Use (BYOD):** The use of personal mobile phones on the company's corporate Wi-Fi network is now subject to new rules.
    - Connecting a personal device (phone, tablet) to the "Innovate-Corporate" Wi-Fi network will require the installation of a Mobile Device Management (MDM) profile.
    - This profile allows IT to enforce security policies (like screen lock and remote wipe for lost devices) and ensure the device is not compromised.
    - Employees who do not wish to install the MDM profile must use the "Innovate-Guest" network, which has no access to internal company resources (like intranet, file shares).
- **Removable Media (USB Drives):** The use of all personal, removable media is now strictly prohibited.
    - Company-issued USB ports on all workstations will be disabled by default.
    - Transferring files must be done via approved cloud storage (OneDrive, SharePoint).
    - Exceptions for specific business needs (e.g., client deliverables) must be approved by both the manager and the IT Security team, and will use encrypted, company-owned drives.
- **Phishing and Incident Reporting:**
    - The "Report Phishing" button in Outlook is the *only* acceptable method for reporting a suspicious email. Forwarding the email to IT is no longer the correct procedure.
    - Failure to report a known security incident (e.g., clicking a link, downloading a strange file) will be considered a serious policy violation.
- **Password Policy:**
    - Password complexity requirements have been increased.
    - All employees will be required to change their password upon their next login after June 15, 2025.

5. Relation to RTO Policy

This policy is the new technology standard and works in conjunction with the "Return to Office" (RTO) policy (HRO'S CIRCULAR NO: 01/2024). All work is to be performed on company-issued equipment, in the office, and on the secure corporate network.

6. Exceptional Remote Work (ERW) Security

For the very few employees with an approved ERW arrangement (as defined in HRO'S CIRCULAR NO: 01/2024), the following *additional* rules apply:

- A company-issued firewall/router must be used as the primary connection to the internet.
- All home-based work must be performed in a room with a closed door, and the workstation must be locked at all times when not in use.
- These employees are subject to random, virtual security audits of their workspace.

7. Mandatory Training and Acknowledgement

All employees are required to complete the new "Data Security 2025" training module, which will be assigned on June 15, 2025. You will be required to digitally sign this new policy upon completion of the training. The deadline for completion is July 1, 2025.

We thank you for your partnership in protecting our company's data and our clients' trust.