ITO’s Circular No: 01/2022

IT Department,
SriLanka Telecom PLC,
Colombo 01.
28 February, 2022

To All Employees,

NEW Technology & Data Security Policy for Hybrid Work

1. Purpose

This circular introduces the new "Technology & Data Security Policy for Hybrid Work." This policy is mandatory for all employees participating in the new Hybrid Work Model (HRO’S CIRCULAR NO: 01/2022) and is designed to mitigate the security risks associated with a distributed workforce.

2. Scope

This policy is effective March 1, 2022, and applies to all employees (Hybrid, Fully Remote, and Full In-Office) who access company data, systems, or networks.

3. Relation to Other Policies

This policy is an **addendum** to the main "Hybrid Work Model Policy" (HRO’S CIRCULAR NO: 01/2022). It does **not** supersede HRO’S CIRCULAR NO: 01/2022. It provides the specific technology and security requirements that all employees must follow under the new model. This policy **supersedes** all older, pre-pandemic IT and "Acceptable Use" policies.

4. Key Policy Requirements for All Employees

- **Multi-Factor Authentication (MFA):** As of March 1, 2022, MFA will be mandatory for all remote access, including email, VPN, and cloud applications. Employees who have not yet registered will be locked out.
- **Company-Issued Equipment:** All work must be performed on company-issued and managed devices. The use of personal computers, tablets, or mobile phones to access or store *any* company data (including email) is strictly prohibited.

- **Data Storage:** All company documents and data must be stored on company-approved cloud storage (e.g., OneDrive, SharePoint). Saving sensitive data to a local desktop, "Downloads" folder, or personal cloud storage (like a personal Google Drive) is a violation of this policy.

5. Specific Requirements for Hybrid and Remote Employees

- **Secure Home Network:** Employees are responsible for ensuring their home Wi-Fi network is secure. This includes:
    - A strong, unique password (WPA2 or higher).
    - Changing the default router administrator password.
    - Enabling the router's firewall.
- **VPN Usage:** The company's VPN (Virtual Private Network) must be active at all times when working remotely, even when accessing standard applications like email.
- **Physical Security:** Employees must take reasonable steps to secure their company-issued equipment.
    - Laptops must be locked when not in use (Windows Key + L).
    - Equipment must be stored securely and out of sight when not in use.
    - Loss or theft of a device must be reported to the IT Help Desk and HR within one (1) hour of discovery.
- **Confidentiality:** Employees must ensure that confidential conversations (phone or video) cannot be overheard and that their screen is not visible to unauthorized individuals (e.g., family members, roommates).

6. Prohibited Activities

- Allowing non-employees (family, friends) to use company-issued equipment.
- Disabling or bypassing any company-installed security software (e.g., antivirus, endpoint management).
- Connecting company laptops to unsecured public Wi-Fi (e.g., at a coffee shop, airport) without using the company VPN.
- Installing any unauthorized or unlicensed software on a company device.

7. Policy Acknowledgement

All employees are required to read this policy in full and sign a digital "Remote Work Agreement" form by March 15, 2022. This form confirms you understand and agree to

adhere to these new security standards. Failure to sign the agreement will result in suspension of remote work privileges.

The full, detailed policy document is available on the intranet. Please direct any questions to the IT Help Desk.