To ensure the consistent implementation of cybersecurity standards across all remote work arrangements, it is hereby required that all government officers who are performing official duties from home utilize only government-issued laptops or devices beginning 30 April 2025. The use of personal devices for accessing, storing, or processing internal documents is strictly prohibited due to the significantly increased risk of data leakage, malware infection, and potential compromise of sensitive information.

In addition to the device requirement, all officers must complete the Remote Work Cyber Hygiene Training Module prior to being granted clearance for system access. This training is designed to provide detailed guidance on best practices for secure handling of official data, safe network usage, password management, and response protocols in case of potential cybersecurity threats. Officers are required to demonstrate full understanding and compliance with the training content before they are permitted to access government systems remotely.

Failure to complete the mandatory training within the stated timeframe may result in temporary suspension of access to government networks and internal systems. Departments are advised to monitor compliance closely and to provide assistance to officers who encounter technical or procedural difficulties during the training process. Adherence to these requirements is critical to protecting the confidentiality, integrity, and availability of government information while maintaining secure and effective remote work operations.