Remote Work Policy: Given the increase in remote work, a policy that outlines security measures for employees working remotely is crucial. This might include requirements for secure home networks, using VPNs, and locking devices when not in use.

1. **Purpose**
    a. The purpose of this policy is to define the rules and requirements for connecting to TKH's network from any host (cell phones, tablets, laptops). These rules and requirements are designed to minimize the potential exposure from damages which may result from unauthorized use of company resources. Damages include the loss of sensitive or organization confidential data, intellectual property, damage to public image, damage to critical internal systems, and fines or other financial liabilities incurred as a result of those losses.
2. **Policy**
    a. It is the responsibility of TKH's employees, contractors, vendors, and agents with remote access privileges to our corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection.
    b. General access to the internet for recreational use through TKH's company network is strictly limited to our employees, contractors, vendors and agents (hereafter referred to as "Authorized users"). When accessing our network from a personal computer, Authorized users are responsible for preventing access to a company computer resources or data by non-Authorized Users.
    c. Performance of illegal activities through TKH's company network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User's access. Authorized

Users will not use TKH's networks to access the Internet for outside business interests.

3. **Connection Procedures**
    a. Secure remote access will be strictly controlled with encryption through TKH's Virtual Private Networks (VPNs) and strong pass-phrases.
    b. Authorized Users shall protect their login and password, even from family members
    c. While using our corporate owned computer to remotely connect to TKH's corporate network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party
    d. Use of external resources to conduct our company business must be approved in advance by the appropriate business unit manager
    e. All hosts that are connected to TKH's internal networks via remote access technologies must use the most up-to-date anti-virus software that includes personal computers.
4. **Compliance**
    a. TKH's IT team will verify compliance to this policy through various methods, including but not limited to periodic walk-throughs, video monitoring (if applicable), business tool reports, internal and external audits, and/or inspection.
    b. An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment

5. Exception to Policy

a. Any exception to the policy should be approved by IT department