|  |  |
| --- | --- |
| **Walpita Enterprises Pvt Ltd**  **Walpita Enterprises Pvt Ltd,**  **HORANA,**  **Sri Lanka.** | **APPROVED BY: ISSC**  **Date: 03-10-2024** |
| **VERSION NO : 1.0**  **Distribution: Internal** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **By** | **Date** | **Section Affected** | **Reason** |
| 1.0 | Chandira Deshan | 01-10-2024 | 3.0 | Review |
| 1.2 | Chandira Deshan | 01-10-2024 | Full document | Company name change and documentation review |
| 2.0 | Chandira Deshan | 01-10-2024 | No change | ISSC review |

# 1.0 Purpose

The purpose of this policy is to define standards for connecting to **Walpita Enterprises Pvt Ltd’s** network from any host. These standards are designed to minimize the potential exposure to Walpita Enterprises Pvt Ltd from damages which may result from unauthorized use of resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical internal systems.

# 2.0 Scope

This policy applies to all Walpita Enterprises Pvt Ltd employees, contractors, vendors. This policy applies to remote access connections used to do work on behalf of Port City Airport, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

# Policy

1. Employees, contractors, and suppliers with remote access privileges to the corporate network are responsible for ensuring that their remote access connection receives the same attention as the user's on-site connection.
2. The Walpita Enterprises Pvt Ltd employee is responsible for ensuring that the family member does not break any Walpita Enterprises Pvt Ltd policies, engages in unlawful activity, or uses the access for personal gain. If the access is exploited, the SBC Hospital employee is responsible for the repercussions.
3. Please study the following policies for information on how to protect data when using remote access methods to access the corporate network, as well as permitted corporate network usage:

* 1. Virtual Private Network (VPN) Policy
  2. Wireless Communications Policy
  3. Acceptable Use Policy

1. No third party shall be granted remote access to any computer on the business network. If this is absolutely essential, written permission from the MD should be acquired, and such sessions should be ‘monitored' by a member of the relevant project team.
2. SBC Hospital users can remotely connect to the corporate network in one or more of the following methods (based on the privileges granted):

|  |  |  |  |
| --- | --- | --- | --- |
| **Device** | **Network** | **User Group** | **Description** |
| Walpita Enterprises Pvt Ltddomain computer | Office dongle | All users with dongle access (APN Users) | This is to facilitate users to work from outside locations. The APN dongle will provide a connection identical to that in office locations (with the same policies and restrictions). |
| Walpita Enterprises Pvt Ltd domain computer | Free internet (wired/wireless)  e.g. Public networks, mobile hotspots | Direct Access Users | This is to facilitate users who need to access the corporate network resources via public/external internet connections (NOT the corporate internet connection). These can be users who are primarily based outside of office locations or need to access the internet via external internet connections as the corporate internet policies provide minimal support for their daily work. |
| Personal computer/computer outside Walpita Enterprises Pvt Ltd domain | Free internet (wired/wireless)  e.g. Public networks, mobile hotspots | VPN Users (Global Protect) | This is to facilitate users who perform the majority of their daily operations COMPLETELY outside of the SBC Hospital Corporate network. The computers, although provided by SBC Hospital, reside outside the Walpita Enterprises Pvt Ltd domain (not recognized as an office computer). However, such users may need to occasionally access corporate network resources (e.g. Service Desk system). Such users also have the option of connecting to the corporate network from their personal computers. |

*IT Operations shall maintain user lists for the above User Groups and ensure it is updated.*

# 4.0 Enforcement

Walpita Enterprises Pvt Ltd reserves the full right to ensure enforcement and compliance of this policy. In the event of violation of the said policy, appropriate corrective and disciplinary action will be taken, up to and including termination of employment and/or criminal liability if required by law of the country.