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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **By** | **Date** | **Section Affected** | **Reason** |
| 1.0 | Chandira Deshan | 01-10-2024 | Process and risk owner added | ISO27001:2022 change |
| 1.1 | Chandira Deshan | 01-10-2024 | Company name changed | Company name change and documentation review |

At Walpita Enterprises Pvt Ltd, we have identified assets based on each process and certain common assets that are used across all processes. These have been assigned values of between 1-3 for the criteria of Confidentiality, Integrity and Availability. We have obtained the asset value pertaining to each identified asset and have categorized the asset value as follows;

|  |  |  |
| --- | --- | --- |
| **Asset Value** | **Asset Category** | **Value for Risk Assessment** |
| 1 - 3 | Low | 1 |
| 4 - 6 | Medium | 2 |
| 7 - 9 | High | 3 |

We have then identified the possible threats that relate to each asset and assigned a value for the impact and probability of occurrence.

Level of threat = (Impact x Probability of occurrence)/ 3

Impact

1. Not critical (Minor impact)
2. Medium impact
3. High impact will lead to loosen in revenue

Probability of occurrence

1. Low
2. Medium
3. High

The resulting threat value has been categorized as follows;

Level of threat

1- Low

2- Medium

3- High

Vulnerability

We have then assigned ratings for vulnerability based on the following conditions.

1 Low – System is not weak

2 Medium - Chance in exploit

3 High – High vulnerability

Based on the Asset Value, Threat Value and the Vulnerability, we have obtained the risk rank for each asset.

Risk rank = Asset value x Level of threat x Vulnerability

All the possible outcomes are put in to following table:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Level of Threat** | **Low** | | | **Medium** | | | **High** | | |
|  | **Level of Vulnerability** | **L** | **M** | **H** | **L** | **M** | **H** | **L** | **M** | **H** |
| **Asset Value** | **Low** | 1 | 2 | 3 | 2 | 4 | 6 | 3 | 6 | 9 |
| **Medium** | 2 | 4 | 6 | 4 | 8 | 12 | 6 | 12 | 18 |
| **High** | 3 | 6 | 9 | 6 | 12 | 18 | 9 | 18 | 27 |

Risk Rank

1 – Lowest

27 – Highest

Once the risk rank has been ascertained, we have identified the controls that need to be present as per ISO 27001 and compared them with the existing controls. Based on the results of the existing controls and the acceptable risk level, it has been decided if additional actions/controls would be required.

The acceptable level of Risk is “9” and has been approved by the management on 3rd OCT 2023. Accordingly, the following table indicates beyond the tolerate risk level.

|  |  |  |
| --- | --- | --- |
| **Asset Value** | **Level of Threat** | **Level Vulnerability** |
| Medium | Medium | High |
| Medium | High | Medium |
| Medium | High | High |
| High | Medium | Medium |
| High | Medium | High |
| High | High | Medium |
| High | High | High |

If a risk value exceeds “9” after the risk treatment, it should be escalated to CISO and seek for necessary remediation.

Process and Risk Owner

In addition to assets process which is relevant assets is also identified in the Risk Assessment report in accordance with ISO 27001:2022 version.

Further, assets owner is renaming as Risk owner and risk owner is accepting the identified risks of risk assessment report.