**Risk Management Policy Notes**

|  |  |  |
| --- | --- | --- |
| **Policy Section** | **Recommended Change(s)** | **Reasoning** |
| Access Control | Employees must lock their workstations, and configure their devices to lock automatically when unattended. | When employees leave their workstations unattended it becomes vulnerable to threat actors as anyone can access the said workstation which may result in a data breach. |
| Awareness and Training | New employees should be trained on current cyber threats, and they must be trained for their specific roles.  Training is also recommended when there are system changes that training is often necessary. | Cybersecurity changes everyday, the threat landscape also changes everyday, so employees must learn to adapt to these new threats and be trained regularly. Employees have specific roles and they must be trained for that specific role, since they have different roles they have access to specific information. |
| Configuration Management | Users can install specific applications that the company uses, any other application other than the company applications would not be allowed. | Installing any other application other than the company application may result in potential damages because of Malware or Ransomware. |
| Identification and Authentication | User password should be allowed spaces and punctuation. | Allowing user passwords to have spaces and punctuations will result in stronger passwords that can prevent threat actors from access, which otherwise may result in data loss. |

A screenshot of a quiz

Description automatically generated