Practical Activity 1

**Risk Assessment Plan**

* **Threats and Vulnerabilities:**

1. Using unsecured Public wi-fi networks are spots for malicious parties to spy on the internet traffic.
2. Not using VPN when accessing Company Information System Remotely
3. Use of weak passwords when working on Company Information system
4. Absence of Firewalls
5. Use of poor Antivirus Software
6. Workers device not secure for Operations.
7. Home Routers

* **Who will be Harmed and How?**

1. Company’s Security: The Company may lose confidential and intellectual property.
2. Worker’s Privacy: Employees privacy could be hampered due to the usage of personal computers
3. Damage to Company’s reputation

* **Precautions:**

1. Ensure wi-fi system at home is secured
2. Employees working at home should use VPN to improve online privacy. Employees must use VPN while working and accessing the company information system
3. All accounts must be protected with strong password because all it takes is one password for a criminal to access all accounts. Password functions should also be turned off when accessing company information system from personal device. Two step verification and Two step authentication should be done for extra protection.
4. Ensure hardware firewalls are enabled.
5. Ensure good anti-virus is in place and fully updated which can help in detecting and blocking malware.
6. If employees must work in public places, their device must be secured; they must ensure their devices are locked to avoid external parties from accessing confidential information.
7. Routers password should be changed when it is first installed. Firmware should be updated to patch security vulnerabilities.

* **Findings**

Using Home Computers is a Big Risk to the Company, if Employees must work from home the company must ensure that it has put in place security guidelines and policies to reduce exposure to cyber security Risk.