Risk Management Policy Review Notes

|  |  |  |
| --- | --- | --- |
| **Policy Section** | **Recommended Change(s)** | **Reasoning** |
| Access Control | Employees should lock devices when leaving them. Devices should be configured to automatically lock after 2 minutes of inactivity. Devices should prompt user for credentials each time they log in again | If an employee leaves their device unlocked it is vulnerable to unauthorised access. Configuring devices to automatically lock and ask for credentials each time minimises this risk. |
| Awareness and Training | All employees should be trained on cyber threats. Training should be conducted on both a regular basis and in special cases such as system changes that make training necessary. Training should be specific for each employee’s role. | Regular training for all employees helps keep staff up- to-date on the best practices and emerging threats. Training staff according to their role also addresses the different kinds of risk the organisation faces, such as legal risk in case of data breach or availability issues in case of system outage. |
| Configuration Management | Adopt application whitelisting to allow users only to install/run approved software on workstations. | Allowing users to download and run unvetted software potentially leads to malware being introduced. If only approved applications can run, this minimises this risk. |
| Identification and Authentication | Passwords should be allowed to include special characters | Including special characters makes passwords more complex and harder for attackers to gain access. |
| Physical and Environmental Protection | Individuals must be removed from the server room authorisation list if they no longer require access | If an employee changes roles or departs the company, they no longer require access to the server room. The access list needs to be maintained with an accurate up-to-date list of individuals to minimise the risk of unauthorised access. |
| System and Information Integrity | Alerts and advisory information should be shared across the organisation, not just the security team | Alerts and advisory information regarding security should be broadly shared to help keep all employees informed. By sharing information, everyone can contribute to security outcomes. |