1. Outdated OS/SW & security vulnerabilities

2. Is Microsoft providing any support for older windows versions

3. ESU (Extended Security Update) program, SEEP (System center End-point Protection)

4. Regularly we need to check for vulnerability updates

Risks:

1. Device/App exposure to internet is a major risk.
2. 3rd party components not getting update.
3. Vendor security tools becoming obsolete with EOL OS

|  |  |  |  |
| --- | --- | --- | --- |
| S.No | Responsibility | Detail of responsibility | Achievement of responsibility |
| 1 | Justification | Reason for not updating the current OS |  |
| 2 | Timeline | Road map/deadline of the product with current/EOL OS |  |
| 3 | Devices count | Approximate no.of field devices |  |
| 4 | Connectivity & Scope | Does all the devices restricted to communicate with intranet/Hospital LAN. |  |
| 5 | EOS/EOL | Patches availability to purchase after EOS |  |
| 6 | Microsoft Security Service Essentials (MSE) | Support after EOS |  |
| 7 | Alternatives | Suggested alternatives from vendor after EOS |  |
| 8 | Cloud support after EOS | Backup & disaster recovery with cloud support |  |
| 9 | Patches for latest OS | Evaluate the released patches for critical vulnerabilities and integrate if they are compatible with EOL OS |  |
| 10 | Tools | Tools to install in EOL OS for vulnerability monitoring |  |
| 11 | Hardening | Identify the vulnerable interfaces and implement the hardening for same |  |
| 12 | Case study/POC | Identify the components to protect the system from cyber attacks |  |
| 13 | Auditing | Regular monitoring audit logging to identify the vulnerability |  |
| 14 | Support from 3rd party components | 3rd party components support to EOS and our plan to update them |  |
| 15 | Regular scanning | Identify the tools to scan periodically and provide log |  |