



LOCAL MUNICIPALITY – UMKHANDLU WENDAWO

I.T SECURITY POLICY

PATCH MANAGEMENT

2021/2022

PATCH MANAGEMENT

- 1.1 All patch releases will follow a defined process for patch deployment that includes assessing the risk, testing, scheduling, installing and verifying.
- 1.2 Patch Prioritization and Scheduling
 - 1.2.1 Patches shall be managed based on their priority level.
 - 1.2.2 A patch cycle shall exist that guides the normal application of patches and updates to systems.
 - 1.2.3 Procedures to deal with the prioritization and scheduling of updates shall be established.
 - 1.2.4 System criticality shall be taken into consideration when scheduling and prioritizing patches
 - 1.2.5 Patches shall only be downloaded from OEM sources or vetted websites.
- 1.3 Patch Testing
 - 1.3.1 The patch testing process shall be implemented to avoid downtime.
- 1.4 Change Management
 - 1.4.1 Patch management shall be managed according to the ICT Change Management Process.
- 1.5 Auditing and Monitoring
 - 1.5.1 Post-patch audit scans shall occur after new critical security patches are released.
 - 1.5.2 Regular or pre-patch network-wide audit scans shall be performed.
 - 1.5.3 Audit reports and logs shall be maintained.
 - 1.5.4 In the event that a critical patch cannot be centrally deployed, it shall be installed in a timely manner manually.
 - 1.5.5 Failure to properly configure new workstations is a violation of this policy
 - 1.5.6 Disabling, circumventing or tampering with patch management protections and/or software constitutes a violation of policy.

RECOMMENDATIONS: