



Approval Date	9 May 2022
Periodical Review	Annually
Commencement Date	9 May 2022
Review Date	9 May 2023

**STANDARD OPERATING PROCEDURE: PATCH MANAGEMENT**

<b>TITLE OF SOP</b>	PATCH MANAGEMENT
<b>SOP Number</b>	CIO-ICT-PM -01
<b>Purpose</b>	This document provides the procedure for windows server update services and antivirus updates.
<b>Scope</b>	This SOP apply across the Eastern Cape Department of Social Development on areas relating to patch management
<b>Definitions and Acronyms</b>	SCCM - System Centre Configuration Manager AD - Active Directory CPU - Central Processing Unit DP – Distribution Points POPIA - Protection of Personal Information Act OS - Operating System POC - Proof Of concept
<b>Performance Indicator</b>	Number of rendered ICT infrastructure services

**STEP BY STEP GUIDE  
PATCH MANAGEMENT**

Nr	Task Name	Task Procedure	Responsibility	Time Frame	Supporting Documentation	Service Standard
1.	Identify patches to be Downloaded.	<ul style="list-style-type: none"> <li>Classify and synchronize updates that are Critical Updates, Security Updates, Definition Updates, Service Packs, Updates and Update Rollups.</li> <li>Ensure that the SCCM Primary Site Server has been configured to only download the updates that our organization requires.</li> </ul>	System Administrator	2 hours	<ul style="list-style-type: none"> <li>Network</li> <li>Server</li> <li>System Centre Configuration Manager</li> <li>Identified patches to be Downloaded</li> </ul>	Tol ensure that all network devices, are deployed with the correct patches within acceptable intervals for maximum security
2.	Configure Windows Server Update Services	<ul style="list-style-type: none"> <li>Ensure that System Centre Configuration Manager is used to deploy software updates.</li> <li>Ensure that one Primary Site Server is located at the Head Office.</li> <li>Indicate ten additional servers configured as Distribution Points are located throughout the Province.</li> <li>Ensure that the Primary Site Server at the Head Office is where the updates are tested before they are deployed.</li> <li>All DSD computers/Notebooks and Servers have the System Centre Configuration Manager Client installed.</li> </ul>	System Administrator	24 hours	<ul style="list-style-type: none"> <li>Network</li> <li>Server</li> <li>System Centre Configuration Manager</li> <li>Configured Distribution Point Servers</li> </ul>	
3.	Perform Patch and distribution Process	<ul style="list-style-type: none"> <li>Ensure that the server at head office has been configured as the SCCM Primary Site Server where Management operations occur.</li> <li>Ensure that Software Updates are downloaded from the Microsoft Update Servers</li> <li>The Software Updates are then only deployed to a group of computers that have been setup for testing the updates.</li> <li>Once the Software Updates have been tested, they are then distributed from the SCCM Primary Site Server to the rest of the Distribution Points.</li> </ul>	System Administrator	48 hours	<ul style="list-style-type: none"> <li>Network</li> <li>Server</li> <li>System Centre Configuration Manager</li> <li>Confirmation of distributed Software Update Packages to Distribution Points.</li> <li>Confirmation of deployed updates to client computers</li> </ul>	

**STEP BY STEP GUIDE  
PATCH MANAGEMENT**

Nr	Task Name	Task Procedure	Responsibility	Time Frame	Supporting Documentation	Service Standard
		<ul style="list-style-type: none"> <li>The updates are then deployed to the client computers that have been configured to get updates from the Distribution point in their area.</li> </ul>				
4.	Configure Server to Create and Download Updates.	<ul style="list-style-type: none"> <li>In Configuration Manager, click the Software Library Workspace, click All Software Updates.</li> <li>In the results pane, search for the desired updates of a specific product.</li> <li>Select all the updates, click Create Software Update Group, type a name for the update group and click create.</li> <li>In the Software Library Workspace, click Software Update Groups, select the group and click download.</li> <li>On the Download Software Updates Wizard, click Create a new deployment Package, type in a name, indicate the source of the package and click next.</li> <li>Click Add and select Distribution Point. Then select the Distribution Point where the updates will be downloaded to, click OK and then Next.</li> <li>Select Automatically download content when packages are assigned to distribution points and click next.</li> <li>Select Download software updates from the Internet and click Next.</li> <li>Select English as the Update language and click next.</li> <li>Review the Summary, click Next and then Close.</li> </ul>			<ul style="list-style-type: none"> <li>Network</li> <li>Server</li> <li>System Centre Configuration Manager</li> <li>Configured Server for the creation and downloading of updates.</li> </ul>	

*MA*

**STEP BY STEP GUIDE  
PATCH MANAGEMENT**

Nr	Task Name	Task Procedure	Responsibility	Time Frame	Supporting Documentation	Service Standard
5.	Configure Server for Deploying Updates to the Test Lab	<ul style="list-style-type: none"> <li>• In the Software Library Workspace, click Software Update Groups, select the group and click Deploy.</li> <li>• On the Deploy Software Updates Wizard, type in a name for the Deployment.</li> <li>• Next to Collection, click Browse, expand the Software Updates folder, select Workstation Updates, select the Test Lab collection, click OK and then Next.</li> <li>• On the Deployment settings page select required next to Type of deployment and then click next.</li> <li>• On the scheduling page, select the following and click next. Schedule Evaluation : Client Local Time Software Available Time : As soon as possible Installation Deadline : As soon as possible.</li> <li>• On the User Experience page, select Display in Software Centre and show all Notifications next to user notifications and then click next.</li> <li>• On the Alerts page click Next.</li> <li>• On the Download Settings page, select Download software updates from distribution point and install, then click Next.</li> <li>• On the Summary page click Next.</li> <li>• On the Completion page, click Close.</li> </ul>	System Administrator	2 hours	<ul style="list-style-type: none"> <li>• Network</li> <li>• Server</li> <li>• System centre configuration Management</li> <li>• Configured Server for Deploying Updates to the Test Lab</li> </ul>	

**STEP BY STEP GUIDE  
PATCH MANAGEMENT**

Nr	Task Name	Task Procedure	Responsibility	Time Frame	Supporting Documentation	Service Standard
6.	Configure Server for Deploying Updates to All the Computers.	<ul style="list-style-type: none"> <li>• In the Software Library Workspace, click Software Update Groups, select the group and click Deploy.</li> <li>• On the Deploy Software Updates Wizard, type in a name for the Deployment.</li> <li>• Next to Collection, click Browse, expand the Software Updates folder, select Workstation Updates, select the Broad Deployment collection, click OK and then Next.</li> <li>• On the Deployment settings page select required next to Type of deployment and then click next.</li> <li>• On the scheduling page, select the following and click next.  Schedule Evaluation : Client Local Time  Software Available Time : As soon as possible  Installation Deadline : Select Specific time of 7 Days from date of deployment.</li> <li>• On the User Experience page, select Display in Software Centre and only show notifications for computer restarts next to user notifications, then click next.</li> <li>• On the Alerts page, click Next.</li> <li>• On the Download Settings page, select Download software updates from distribution point and install, then click Next.</li> <li>• On the Summary page click Next.</li> <li>• On the Completion page, click Close.</li> </ul>	System Administrator	2 hours	<ul style="list-style-type: none"> <li>• Network</li> <li>• Server</li> <li>• System Centre Configuration Manager</li> <li>• Configured Server for Deploying updates to all computers.</li> </ul>	
7.	Configuration Manager Client Manual Installation.	Run the ccmsetup.exe to install the Configuration Manager Client Software.	ICT Technician	1 hour	<ul style="list-style-type: none"> <li>• Network</li> <li>• Server</li> <li>• System Centre Configuration Manager</li> <li>• Configured Client computer</li> </ul>	

**STEP BY STEP GUIDE  
PATCH MANAGEMENT**

Nr	Task Name	Task Procedure	Responsibility	Time Frame	Supporting Documentation	Service Standard
8.	Deploy the Configuration Manager Client Software by Using Client Push Installation	<ul style="list-style-type: none"> <li>On the Navigation Pane of Configuration Manager, click Assets &amp; Compliance and then click Device Collections.</li> <li>Select All Desktop and Server Clients and then click Install Client from the Collection drop down menu.</li> </ul> <p>On the Install Configuration Manager Client Wizard, click Next on all the pages and Close on the Completion page.</p>	System Administrator	1 hour	<ul style="list-style-type: none"> <li>Network</li> <li>Server</li> <li>System Centre Configuration Manager</li> <li>Deployed Configuration Manager Client</li> </ul>	
9.	Schedule server to run updates	<ul style="list-style-type: none"> <li>The Primary Site Server's synchronization schedule is set to run after the Microsoft regular security update release on the second Tuesday of each month at 8pm.</li> <li>Deployment to the Test Lab is done every Wednesday after the Primary Server's synchronization.</li> <li>Distribution of the updates to the Distribution Points is done when updates are available on the Primary Site Server and are only deployed to computers according to the schedule of seven days after testing is completed.</li> </ul>	System Administrator	1 hour	<ul style="list-style-type: none"> <li>Network</li> <li>Server</li> <li>System Centre Configuration Manager</li> <li>Server update synchronization and distribution schedule</li> </ul>	
10.	Test the installed patches	<ul style="list-style-type: none"> <li>Verify that the updates have been installed.</li> <li>Restart the computer and run the applications to check stability.</li> </ul> <p>Run the computer for 24hrs to check stability.</p>	System Administrator	4 hours	<ul style="list-style-type: none"> <li>Network</li> <li>Server</li> <li>Reliability monitor Report</li> </ul>	
11.	Monitor Patch updates	<ul style="list-style-type: none"> <li>Monitor the machines that were tested on patches for inconsistency or malfunction.</li> </ul>	System Administrator	1 hour	<ul style="list-style-type: none"> <li>Network</li> <li>Server</li> <li>System Centre Configuration Manager</li> <li>Reliability monitor Report results</li> </ul>	

**STEP BY STEP GUIDE  
PATCH MANAGEMENT**

Nr	Task Name	Task Procedure	Responsibility	Time Frame	Supporting Documentation	Service Standard
12.	Report on patches	<ul style="list-style-type: none"> <li>• Review status of installation and the rate of successful patches against failed install and resubmit the failed installations</li> <li>• Compile patch management report on monthly basis and submit to Deputy Director- Network administration</li> </ul>	System Administrator	3 hours	<ul style="list-style-type: none"> <li>• Network</li> <li>• Server</li> <li>• System Centre Configuration Manager</li> <li>• Reliability monitor status Report</li> </ul>	

## PROCESS RISKS

Risk Name	Risk Description	Probability (H/M/L)	Impact (H/M/L)	Control Description	System / Manual
Windows operating system security	Windows operating systems that are not patched with the latest security updates are most vulnerable to exploitation by attackers.	H	H	System administrator must ensure that the Windows operating system is updated with the latest security updates so that exploitation from attackers can be detected and prevented.	Manual
Application Security	Applications that are not patched with the latest security updates could result to the applications being vulnerable to attacks	M	L	System administrator must ensure that patch management at application level is done to protect applications from attackers	Manual

*MA*



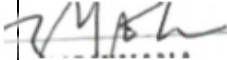



**REFERENCES (LEGISLATION, POLICIES, PROCEDURES, LEGISLATION & OTHER DOCUMENTATION (i.e. SOPs))**

Document Name	Section Description or Document Description
<b>ISO27000</b>	According to ISO 27000, which provides the overview and vocabulary for ISO Information Security Management Systems, a vulnerability is “a weakness of an asset or control that could potentially be exploited by one or more threats.” It also defines a threat as any “potential cause of an unwanted incident, which may result in harm to a system or organization.”
<b>The Promotion of Access to Information Act, 2000 (PAIA) (Act No. 2 of 2000)</b>	The Promotion of Access to Information Act, 2000 (Act No. 2 of 2000) (hereinafter referred to as “PAIA”) is the national legislation which was enacted to give effect to the constitutional right of access to information. PAIA gives all South Africans the right to have access to records held by the state, government institutions and private bodies.
<b>Minimum Information Security Standards (MISS 1996)</b>	The Minimum Information Security Standards (or MISS) is a standard for the minimum information security measures that any institution must put in place for the protection of sensitive or classified information.
<b>Protection of Personal information (POPIA) Act (No 4 of 2013)</b>	Section 19. (1) states that a responsible party must ensure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent - a) loss of, damage to or unauthorised destruction of personal information;
<b>Information Security Policy 2016</b>	Implementation Guideline for Corporate Governance of Information and Communication Technology.
<b>Microsoft Update catalogue</b>	A website from Microsoft that provides a listing of updates that can be distributed over a corporate network.

*MA*

## AUTHORISATIONS

Designation:	Name:	Comments:	Signature:	Date:
Recommended By: Director-ICT Engineering	T.M. Vazi			13/04/2022
Recommended by: Acting CIO -	M.E.Gazi			25/04/2022
Recommended by: DDG	Dr.N.Z.G Yokwana			06/052022
Approved by: Head of the Department	M. Machedemba			09/05/2022
Distribution and Use of SOP	All CIO Directors, All CIO Deputy Directors, All CIO Assistant Directors, All CIO Administration support staff, All CIO Personal Assistance			

*MA*