



Approval Date	04-12-2022
Periodical Review	Annual
Commencement Date	04-12-2022
Review Date	04-12-2023

**STANDARD OPERATING PROCEDURE: DEVELOP SYSTEM**

<b>TITLE OF SOP</b>	System Development Standard Operating Procedure	
<b>SOP Number</b>	CIO-SDM-SD-01	
<b>Purpose</b>	<ul style="list-style-type: none"> <li>To document the mandatory requirement of the System Development process at the Department of Social Development, in line with the adopted SDLC frameworks.</li> <li>To enforce application of effective Development and Design practices to ensure best fit of the solution to the business requirements.</li> </ul>	
<b>Scope</b>	<ul style="list-style-type: none"> <li>SOP for System Development for the Eastern Cape Department of Social Development (ECDSD)</li> </ul>	
<b>Definitions and Acronyms</b>	<b>ECDS</b> <b>Office Hours</b> <b>URS</b> <b>ERD</b> <b>DBA</b> <b>SDLC</b> <b>ICT</b> <b>UAT</b>	Eastern Cape Department of Social Development 8am to 4:30pm User Requirements Specification Entity Relationship Diagram Database Administrator Systems Development Life Cycle Information and Communications Technology User Acceptance Testing
<b>Performance Indicator</b>	Number of modernized business services rendered	

**STEP BY STEP**

**Develop System**

Nr	Task Name	Task Procedure	Responsibility	Time Frames	Systems and Supporting Documentation	Service Standard
1.	<b>Develop technical system design</b>	<ul style="list-style-type: none"> <li>• Prepare the project plan in joint with developers and DBAs.</li> <li>• Utilize the URS to develop a draft technical system design document that includes technical system flow charts, Class diagrams, Data models, ER Diagram and User Acceptance Checkpoints in joint with Senior DBA and lead Developer.</li> </ul>	Technical Manager (systems development)	1 month, depending to the size of the project	<ul style="list-style-type: none"> <li>• User Requirement Specification (input)</li> <li>• User Acceptance Checkpoints</li> <li>• Technical System Flow Chart.</li> <li>• Class Diagrams</li> <li>• Data Models</li> <li>• ER Diagram</li> <li>• Draft Technical System design document</li> <li>• Project plan</li> </ul>	Develop all the Department of Social Development requested systems approved by the ICT steering committee as defined in the Secure System Development and Maintenance policy Annexure A: SDLC process, within 1 year.
2.	<b>Design the application</b>	<ul style="list-style-type: none"> <li>• Develop screen design, Test cases and System Test plan in joint with lead Developer.</li> <li>• Edit the received Technical system design document to include the application design information.</li> </ul>	Technical Manager (systems development)	1 month depending to the size of the project	<ul style="list-style-type: none"> <li>• Draft System design document (input)</li> <li>• User Requirement Specification (input)</li> <li>• Data Models (Input)</li> <li>• ER Diagram (input)</li> <li>• Screen design</li> <li>• System Test cases</li> <li>• System Test Plan</li> <li>• Draft Technical System design document</li> </ul>	

**STEP BY STEP**

**Develop System**

<b>Nr</b>	<b>Task Name</b>	<b>Task Procedure</b>	<b>Responsibility</b>	<b>Time Frames</b>	<b>Systems and Supporting Documentation</b>	<b>Service Standard</b>
3.	<b>Design the database</b>	<ul style="list-style-type: none"> <li>• Develop the database logical design and database dictionary of the system in-joint with DBA.</li> <li>• Edit the received technical system design document to include the database design information.</li> <li>• Develop DB test cases, test plan.</li> </ul>	Senior DBA	1 month depending to the size of the project	<ul style="list-style-type: none"> <li>• Draft System design document (input)</li> <li>• User Requirement Specification (input)</li> <li>• Data Models (input)</li> <li>• ER Diagram (input)</li> <li>• Database logical design</li> <li>• Data dictionary design</li> <li>• Final Technical System design document</li> <li>• Database Test cases</li> <li>• Database Test plan</li> </ul>	
4.	<b>Develop the Database</b>	<ul style="list-style-type: none"> <li>• Develop the Database Entities (tables, relationships, indexes) to the highest normal form.</li> <li>• Review Database Schema for Quality in-joint with lead developer.</li> <li>• Perform Database testing.</li> </ul>	Senior DBA	2 months depending to the size of the project	<ul style="list-style-type: none"> <li>• Final System design document</li> <li>• Table design, Functions, Views and Stored procedure</li> <li>• DB Review Document</li> <li>• Database Test reports</li> </ul>	
5.	<b>Develop Application</b>	<ul style="list-style-type: none"> <li>• Setup the version controller environment for system development project.</li> <li>• Develop the system business logic (Packages, classes, functions, data queries through stored procedures) working with other developers.</li> </ul>	Lead Developer	2 months depending to the size of the project	<ul style="list-style-type: none"> <li>• Screenshot of system development project setup on Version controller</li> <li>• System design document</li> <li>• Test reports</li> </ul>	

**STEP BY STEP**

**Develop System**

Nr	Task Name	Task Procedure	Responsibility	Time Frames	Systems and Supporting Documentation	Service Standard
		<ul style="list-style-type: none"> <li>• Develop system data access logic working with other developers.</li> <li>• Develop the system user interface (e.g. pages, window, midlets etc.) working with other developers.</li> <li>• Create data validations working with other developers.</li> <li>• Perform unit tests working with other developers.</li> </ul>			<ul style="list-style-type: none"> <li>• System business logic</li> <li>• System data access logic</li> <li>• System user interface</li> </ul>	
6.	<b>Review Application Code</b>	<ul style="list-style-type: none"> <li>• Tests the application on the development environment against the specification.</li> <li>• Review code quality and processes in consultation with the Senior Developer.</li> <li>• Prepare draft of Deployment Document.</li> </ul>	<ul style="list-style-type: none"> <li>• Lead Developer</li> </ul>	1 month depending to the size of the project	<ul style="list-style-type: none"> <li>• URS document (input)</li> <li>• System design document (input)</li> <li>• Test results</li> <li>• Draft deployment document</li> </ul>	
7.	<b>Deploy Application to Test Server</b>	<ul style="list-style-type: none"> <li>• Get latest code version.</li> <li>• Run the code to verify if there are no errors.</li> <li>• Publish application to the test server</li> <li>• Deploy database to test server</li> <li>• Inform the both Functional support and Business analysis teams about the deployed application for proper quality testing.</li> </ul>	<ul style="list-style-type: none"> <li>• Lead DBA</li> </ul>	1 week depending to the size of the project	<ul style="list-style-type: none"> <li>• Draft Deployment document (input)</li> <li>• Deployed application</li> </ul>	
8.	<b>Fix the system bugs</b>	<ul style="list-style-type: none"> <li>• Receive the test report from the testing team</li> <li>• Share the report with lead DBA</li> <li>• Correct the bugs if there are any, DBA will correct if they are DB related or</li> </ul>	<ul style="list-style-type: none"> <li>• Lead developer</li> </ul>	1 day or depending to the size of the project	<ul style="list-style-type: none"> <li>• Test report</li> <li>• Closed system bugs report</li> </ul>	

**STEP BY STEP**

**Develop System**

<b>Nr</b>	<b>Task Name</b>	<b>Task Procedure</b>	<b>Responsibility</b>	<b>Time Frames</b>	<b>Systems and Supporting Documentation</b>	<b>Service Standard</b>
9.	<b>Prepare deployment document for the live environment</b>	<ul style="list-style-type: none"> <li>Update deployment document</li> <li>Submit the deployment document to the lead DBA</li> </ul>	<ul style="list-style-type: none"> <li>Lead Developer</li> </ul>	1 week or depending to the size of the project	<ul style="list-style-type: none"> <li>Functional Test report (input)</li> <li>User acceptance test report (input)</li> <li>Signed Live deployment document</li> </ul>	
10.	<b>Deploy application to the pre-live environment</b>	<ul style="list-style-type: none"> <li>Publish application to the pre-live server for training purpose.</li> <li>Deploy database to pre-live server.</li> <li>Test application on the pre-live server.</li> </ul>	<ul style="list-style-type: none"> <li>Lead DBA</li> </ul>	1 day	<ul style="list-style-type: none"> <li>Signed Live deployment document</li> <li>Published application</li> <li>Deployed database</li> </ul>	
11	<b>Deploy application to the live environment</b>	<ul style="list-style-type: none"> <li>Publish application to the live server</li> <li>Deploy database to live server</li> <li>Test application on the live server</li> <li>Inform Functional support</li> </ul>	<ul style="list-style-type: none"> <li>Lead DBA</li> </ul>	1 week depending to the size of the project	<ul style="list-style-type: none"> <li>Signed Live deployment document)</li> <li>Deployed application on live</li> </ul>	
12.	<b>Monitor and report the performance of the system</b>	<ul style="list-style-type: none"> <li>Convene meetings to report on progress throughout the project.</li> <li>Report on ICT Operational meeting on monthly basis.</li> </ul>	<ul style="list-style-type: none"> <li>Manager: System Development</li> </ul>	1 day	<ul style="list-style-type: none"> <li>Progress reports (input)</li> <li>Monitoring report</li> </ul>	

## LEGISLATION REFERENCES

Document Name	Description
<b>Constitution of the Republic of South Africa, 1996 (Act 108 of 1996)</b>	Section 32. Access to information states that ( 1) Everyone has the right of access to- (a) any information held by the state; and (b) any information that is held by another person and that is required for the exercise or protection of any rights.
<b>Minimum Information Security Standards (MISS), 1996</b>	Section 4 of Chapter 1 states that where information is exempted from disclosure, it implies that security measures will apply in full. This document is aimed at exactly that need: providing the necessary procedures and measures to protect such information. It is clear that security procedures do not concern all information and are therefore not contrary to transparency, but indeed necessary for responsible governance. Chapter 7 on Computer security indicates the allocation and use of passwords as prescribed.  The MISS seems to apply to both public and private bodies who handle sensitive or classified information. The definition of institution covers not only public bodies, but “any private undertaking that handles information classifiable by virtue of national interest” as well. Considering that private bodies seldom process classified information, the MISS mostly applies to public bodies. However, considering that the government does also outsource certain important national services to the private sector the MISS will certainly apply to private bodies as well.
<b>Public Service Regulations, 2016</b>	Chapter 6, section 93 states that the head of department shall ensure that the acquisition, management and use of information and communication technologies by the department as follows: (a) enhances direct or indirect service delivery to the public, including, but not limited to, equal access by the public to services delivered by the department; (b) improves the productivity of the department; (c) promotes an environmentally friendly public service; and (d) ensures cost efficiency for the department.  Section 97. Minimum interoperability standards states that 1) The Minister shall issue Minimum Interoperability Standards (herein referred to as the "MIOS") for the public service. (2) The MIOS shall include provision for standards and specifications for: (a) interconnectivity;

Document Name	Description
	<p>(b) data integration; and</p> <p>(c) information access.</p> <p>(3) Any new information and communication technology system developed or acquired or any upgrade of any existing information and communication technology system in the public service shall comply with the MIOS.</p> <p>(4) A head of department shall:</p> <p>(a) include compliance with the MIOS in the project approval procedure; and</p> <p>(b) ensure compliance to the MIOS in the acquisition or use of information and communication technology.</p>
<b>SITA Act 1998</b>	<p>Section 6 states that the objective of the Agency is to provide information technology, information systems and related services in a maintained information systems security environment to, or on behalf of, participating departments and organs of state and in regard to these services, act as an agent of the South African Government.</p> <p>Section 7 state the Powers and functions of Agency as follows:</p> <p>e. provide technical, functional and business advice and support regarding information technology;</p> <p>g. with regard to any of the above functions act as procurement agency in respect of information technology requirements, in accordance with State procurement policy; and</p> <p>h. perform any other function which the Minister may, from time to time, determine to give effect to the objective of the Agency.</p>
<b>ISO/IEC 17799:2005</b>	<p>Establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined provide general guidance on the commonly accepted goals of information security management. ISO/IEC 17799:2005 contains best practices of control objectives and controls in the following areas of information security management:</p> <p>System Development and Maintenance</p> <p>System Development and Maintenance control addresses an organization's ability to ensure that appropriate information system security controls are both incorporated and maintained, including:</p> <p>System security requirements – incorporates information security considerations in the specifications of any system development or procurement.</p>

Document Name	Description
	<p>Application security requirements – incorporates information security considerations in the specification of any application development or procurement.</p> <p>Cryptography – policies, standards, and procedures governing the usage and maintenance of cryptographic controls.</p> <p>System Integrity – mechanisms to control access to, and verify integrity of, operational software and data, including a process to track, evaluate, and incorporate asset upgrades and patches.</p> <p>Development security – integrates change control and technical reviews into development process.</p>
<p><b>National e-government strategy and roadmap 2017</b></p>	<p>Section 7 of Guiding Principles for E-Government Services states the following:</p> <p>7.1 Interoperability</p> <p>Government ICT systems (including networks, platforms, applications and data) must have the capacity to ‘talk’ to each other, allowing for architected sharing and exchange of electronic messages and documents, collaborative applications, distributed data processing and report generation, seamless transaction services, ‘whole-of government’ search and queries, integrated ICT systems management etc.</p> <p>Of note is that Government has the ability to correct the situation, as well as manage the related aspects of the development of ICT infrastructure, because government consumes more than half of South Africa’s ICT goods and services. The ideal state of interoperability is to have machine-to-machine communication, in essence, removing manual intervention in as many steps as possible. Once this aspect is controlled, citizens will start to experience seamless government service.</p> <p>7.2 ICT Security</p> <p>Government operates in an environment where electronic documents, data and ICT systems must be protected from unauthorised access, malicious code and denial-of-service attacks.</p> <p>Interoperability should be achieved without compromising vital ICT security concerns.</p>




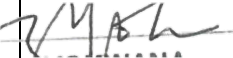

Document Name	Description
<b>Control Objectives for Information Technology (COBIT 5)</b>	<p>Chapter 7 of Implementation Guidance on Creating the Appropriate Environment states the following:</p> <ul style="list-style-type: none"> <li>• It is important for implementation initiatives leveraging COBIT to be properly governed and adequately managed.</li> <li>• Major IT-related initiatives often fail due to inadequate direction, support and oversight by the various required stakeholders, and the implementation of governance or management of IT enablers leveraging COBIT is no different.</li> <li>• Support and direction from key stakeholders are critical so that improvements are adopted and sustained.</li> <li>• In a weak enterprise environment (such as an unclear overall business operating model or lack of enterprise-level governance enablers), this support and participation are even more important.</li> </ul> <p>Chapter 7 of Implementation Guidance on Recognizing Pain Points and Trigger Events indicates that there are a number of factors that may indicate a need for improved governance and management of enterprise IT.</p> <p>Examples of some of the typical pain points for which new or revised governance or management of IT enablers can be a solution (or part of a solution), as identified in <i>COBIT 5 Implementation</i>, are:</p> <ul style="list-style-type: none"> <li>• Significant incidents related to IT risk, such as data loss or project failure</li> <li>• Regular audit findings about poor IT performance or reported IT quality of service problems</li> <li>• Duplication or overlap between initiatives or wasting resources, such as premature project termination</li> <li>• Insufficient IT resources, staff with inadequate skills or staff burnout/dissatisfaction</li> <li>• IT-enabled changes failing to meet business needs and delivered late or over budget</li> </ul>
<b>Department of Social Development Secure System Development and Maintenance policy 2021</b>	<p>To provide a policy guiding framework on processes and procedures for a security consideration at stages or phases of the Departmental systems.</p> <p>To ensure that security is an integral part of Departmental systems development, maintenance, use, retirement and disposal.</p>
<b>Prince 2</b>	<p>Sets out clearly defined roles, responsibilities, processes and stages. It does this while remaining versatile and scalable.</p>

Document Name	Description
<b>ITILV4</b>	<p>The ITIL service value system (SVS) is a model demonstrating how all the components and activities of an organization work together to facilitate value creation through IT-enabled services. Some of these components include:</p> <ul style="list-style-type: none"> <li>• <b>ITIL service value chain</b> is a set of interconnected activities that an organization performs in order to deliver a valuable product or service to its consumers and to facilitate value realization.</li> <li>• <b>The ITIL practices</b> are sets of organizational resources designed for performing work or accomplishing an objective.</li> <li>• <b>Continual improvement</b> is a recurring organizational activity performed at all levels to ensure that an organization's performance continually meets stakeholders' expectations.</li> </ul>
<b>Electronic Communications and Transactions Act 2002 (ECTAct2002)</b>	<p>Section 8 of <b>Development of human resources</b> in clause (3) Subject to subsections (1) and (2), states that the Minister must promote skills development in the areas of information:</p> <p>(a) Information technology products and services in support of electronic transactions;</p> <p>(c) Sectoral regional, national, continental and international policy formulation for electronic transactions;</p> <p>(d) Project management on public and private sector implementation of electronic transactions;</p> <p>(h) Technology and business standards for electronic transactions;</p> <p>Section 10 of <b>Electronic transactions policy</b> states the following:</p> <p>(2) (b) (ii) the nature, scope and impact of electronic transactions;</p> <p>(3) The Minister must publish policy guidelines in the Gazette on issues relevant to 20 electronic transactions in the Republic.</p> <p>(4) In implementing this Chapter, the Minister must encourage the development of innovative information systems and the growth of related industry.</p>

## RISKS

Risk Name	Risk Description	Probability (H/M/L)	Impact (H/M/L)	Control Description	System/Manual
Unclear or changing business requirements.	<ul style="list-style-type: none"> <li>Unclear or changing business requirements result to delay in system automation development completion or delay in delivery of the system.</li> </ul>	H	H	<ul style="list-style-type: none"> <li>Business Analyst need to ensure that business requirements are clearly defined and understood by Business or client.</li> </ul>	Manual
Scope creep.	<ul style="list-style-type: none"> <li>Scope creep occurs when there are overlooked processes by the time of process documentation or there is no documented manual process in place and come up on delivery of the system which results to not meet project deadline or failure.</li> </ul>	H	H	<ul style="list-style-type: none"> <li>Established project committee that include client representation to meet more frequently from the project initiation to the end to ensure that the chance of having scope creep is minimized.</li> </ul>	Manual
Changing technology.	<ul style="list-style-type: none"> <li>Changing technology during project lifecycle may cause delays due to upgrades that would need to takes place before the change is implemented.</li> </ul>	M	M	<ul style="list-style-type: none"> <li>ICT staff to keep up to date with software provider announcements to prepare relevant equipment upgrades in advance.</li> </ul>	Manual
Delays in Supply Chain Management procurement processes.	<ul style="list-style-type: none"> <li>Delays in SCM procurement process while the developers do not have working tools to embark on requested business project result to project failure.</li> <li>Delay in SCM procurement of software licenses that will be used for system development can lead to delay or failure of the project.</li> </ul>	H	H	<ul style="list-style-type: none"> <li>Developers to be prioritized as critical staff to be considered for high ICT equipment specification.</li> <li>Prioritize the purchase of required software licenses.</li> </ul>	Manual

## AUTHORIZATION

Designation:	Name:	Comments	Signature:	Date:
Recommended by Acting CIO	M.E.Gazi			22/11/22
Recommended by: DDG	N.Z.G Yokwana			01/12/2022
Approved by: HOD	M. Machedemba	Approved		04/12/2022
Distribution and Use of SOP	All Departmental staff			