



Province of the  
**EASTERN CAPE**  
SOCIAL DEVELOPMENT

Approval Date	1 December 2021
Periodical Review	Annual
Commencement Date	1 December 2021
Review Date	1 December 2022

**STANDARD OPERATING PROCEDURE: PERSONNEL VETTING**

<b>TITLE OF SOP</b>	PERSONNEL VETTING
<b>SOP Number</b>	2/5/5/11
<b>Purpose</b>	The purpose of the SOP is to indicate the implementation process of Personnel Security Vetting in the Department.
<b>Scope</b>	This SOP is applicable to all members of the management, employees, consultants, contractors and any other service providers of the Department. It is further applicable to all visitors and members of the public visiting premises or may officially interact with the Department.
<b>Definitions and Acronyms</b>	<p>"Critical service" means a service identified by an institution as a critical service through a Threat and Risk Assessment and the compromise of which will endanger the effective functioning of the institution.</p> <p>"Security clearance" means a certificate issued to a candidate after the successful completion of a security screening investigation, specifying the level of classified information to which the candidate may have access subject to the need to know.</p> <p>"Security Competence" Means a person's ability to act in such a way that he/she does not cause classified information to fall into unauthorized hands there by harming/endangering the security/interests of the state (it is measured against a person's susceptibility to extortion/blackmail, amenability to bribes and susceptibility behavior of compromise, loyalty to the state and the relevant organ of state/institution.</p> <p>"State Security Agency (SSA)" means the Agency as defined in section 1 of the Intelligence Services Act, 2002 (Act No 65 of 2002) as amended by the General Intelligence Laws Amendment Act, 2013 (Act No 11 of 2013);</p> <p>MISS – Minimum Information Security Standards, 1996</p>
<b>Performance Indicator</b>	Number of Security Practices coordinated to create a secure environment.

**STEP BY STEP**

**PERSONNEL VETTING**

Nr	Task Name	Task Procedure	Responsibility	Time Frames	Systems and Supporting Documentation	Service Standard
1.	<b>Distribute Z204 form</b>	<ul style="list-style-type: none"> <li>Supply Z204 to the incumbent of a post where sensitive/classified information is handled, critical services rendered.</li> </ul>	<ul style="list-style-type: none"> <li>Supervisor</li> </ul>	14 Days	<ul style="list-style-type: none"> <li>Critical service or sensitive information</li> <li>Security management policy</li> <li>Letter to appointed official to submit Z204</li> </ul>	<p>Vetting all personnel that are handling Departmental sensitive or classified information and rendering critical service as defined in section 1 of the Intelligence Services Act, 2002 (Act No 65 of 2002) as amended by the General Intelligence Laws Amendment Act, 2013 (Act No 11 of 2013 ) within 60 days</p>
2.	<b>Submit Z204 form</b>	<ul style="list-style-type: none"> <li>Official submit completed Z204 and supporting documents to District Security Management Unit in sealed envelope.</li> </ul>	<ul style="list-style-type: none"> <li>Official</li> </ul>	30 Days	<ul style="list-style-type: none"> <li>Letter to appointed official to submit Z204</li> <li>Completed Z204 form and supporting documents as per checklist</li> </ul>	
3.	<b>Conduct District Evaluation for Z204 form</b>	<ul style="list-style-type: none"> <li>Capture receipt of the Z204 in the District database.</li> <li>Evaluate Z204 form for completeness and to ensure that required supporting documentation is attached.</li> </ul>	<ul style="list-style-type: none"> <li>Asst. Dir Security Management</li> </ul>	7 Days	<ul style="list-style-type: none"> <li>Completed Z204 form and supporting documents as per checklist</li> <li>Complete Z204 form</li> <li>Incomplete Z204 form</li> </ul>	
4.	<b>Submit/Return Z204 form</b>	<ul style="list-style-type: none"> <li>If found correct, consolidated Z204s will be forwarded to Provincial Office under cover memo signed by the District Manager.</li> <li>If not correct, Z204 to be returned to relevant official to address identified areas of concern with a cover letter and steps 2 – 4 will again be followed.</li> </ul>	<ul style="list-style-type: none"> <li>Asst. Dir Security Management</li> </ul>	1 Day	<ul style="list-style-type: none"> <li>Evaluated Z204 form</li> <li>Cover letter</li> <li>Signed acknowledgement of receipt</li> <li>Email</li> </ul>	

5.	<b>Conduct Provincial Evaluation for Z204 form</b>	<ul style="list-style-type: none"> <li>• Capture receipt of the Z204 in the Provincial database.</li> <li>• Evaluate Z204 form for completeness and to ensure that required supporting documentation is attached.</li> </ul>	<ul style="list-style-type: none"> <li>• Asst. Dir. Information Security</li> </ul>	7 Days	<ul style="list-style-type: none"> <li>• District evaluated Z204 form</li> <li>• Cover letter</li> <li>• Complete Z204 form</li> <li>• Incomplete Z204 form</li> </ul>
6.	<b>Submit / Return Z204</b>	<ul style="list-style-type: none"> <li>• If found correct, consolidated Z204s will be forwarded to State Security Agency under cover letter signed by the Head of Department.</li> <li>• Inform the Vetting applicant when Z204 form is submitted to SSA to expect engagement.</li> <li>• If not correct, Z204 to be returned to the relevant District/official to address identified areas of concern with a cover letter and steps 2 – 4 will again be followed.</li> </ul>	<ul style="list-style-type: none"> <li>• Asst. Dir. Information Security</li> </ul>	2 Days	<ul style="list-style-type: none"> <li>• Evaluated Z204 form</li> <li>• Cover letter</li> <li>• Signed acknowledgement of receipt</li> <li>• Email</li> </ul>
7.	<b>Request progress of submitted Z204s</b>	<ul style="list-style-type: none"> <li>• Request progress from SSA on submitted Z204s through letter signed by Head of Department.</li> </ul>	<ul style="list-style-type: none"> <li>• Asst. Dir. Information Security</li> </ul>	Monthly	<ul style="list-style-type: none"> <li>• Request letter</li> <li>• Signed acknowledgement of receipt</li> <li>• Competence certificate</li> </ul>
8.	<b>Administer competence Certificate on receipt</b>	<ul style="list-style-type: none"> <li>• Update Provincial database</li> <li>• Send copy to District to inform official with cover memorandum</li> <li>• Submit copy to Human Resource Administration for processing on PERSAL.</li> </ul>	<ul style="list-style-type: none"> <li>• Asst. Dir. Information Security.</li> </ul>	3 Days	<ul style="list-style-type: none"> <li>• Competency Certificate</li> <li>• Request letter</li> </ul>
9.	<b>Process competence certificate</b>	<ul style="list-style-type: none"> <li>• Record competence certificate on PERSAL function #4.3.6 <ul style="list-style-type: none"> <li>○ File competence certificate on personal file of applicable official.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Deputy Director: HRA</li> </ul>	3 Days	<ul style="list-style-type: none"> <li>• Competency Certificate</li> <li>• Cover letter</li> <li>• Persal printout</li> </ul>

10. Reporting on personnel vetting	<p>Approve Personnel vetting report for strategic planning submission with the following:</p> <ul style="list-style-type: none"> <li>• Report on number of Z204s received from districts <ul style="list-style-type: none"> <li>○ Name of official</li> <li>○ Occupational Category</li> <li>○ Classification Level</li> </ul> </li> <li>• Report on number of Z204s submitted to SSA for administration <ul style="list-style-type: none"> <li>○ Name of official</li> <li>○ Occupational Category</li> <li>○ Classification Level</li> </ul> </li> <li>• Report on Database captured and recorded competence certificate on PERSAL</li> </ul>	<ul style="list-style-type: none"> <li>• Deputy Director: Security Management</li> </ul>	<p>Monthly Quarterly</p>	<ul style="list-style-type: none"> <li>• Districts personnel vetting reports</li> <li>• Provincial personnel vetting reports</li> <li>• Monthly report</li> <li>• Quarterly report</li> </ul>	
------------------------------------	---	--	------------------------------	---	--

## LEGISLATION REFERENCES




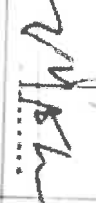

Document Name	Description
Constitution of the Republic of South Africa, 1996 (Act 106 of 1996)	Chapter 2 (Bill of Rights) Section 14 – Everyone has the right to privacy. Section 36 – Limitation can be placed on individuals rights, if reasonable, justifiable and taking into account: nature of the right; importance of the purpose of the limitation; nature and extent of the limitation; relationship between the limitation and its purpose; and there are no less restrictive means to achieve the purpose
Minimum Information Security Standards (MISS), Second Edition March 1998	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 (such as social grants, for example), the MISS will certainly apply to private bodies as well.
Public Service Regulations, 2016 (Chap. 4 Part 4)	Section 57(1)(C) – An executive authority— (c) shall subject an employee or a candidate for employment to personnel suitability checks as directed by the DPSA Circular 14/1/1/P dated 2019-01-11 – HRP Circular 3 of 2017
Public Service Act, 1994 (R103 of 1994)	Section 3(4) - Public Service Commission may issue mandates with regard to security requirements with which officers and employees shall comply - To be included in collective bargaining agreements for Public Sector.
National Strategic Intelligence Amendment Act, 2002	National Strategic Intelligence Amendment Act, 2002, Section 2A, Sub-Section 1-3 – Responsibility of SSA to conduct security screening investigations of any person who: is employed by or is an applicant to an organ of state; or is rendering a service or has given notice of intention to render a service to an organ of state; which service may: Give him or her access to classified information and intelligence in the possession of the organ of state.  Sub-Section 4-5 – SSA in performing the security screening investigation make use of a polygraph to determine reliability of information gathered May gather information relating to Criminal records, Financial records, personal information or any other information considered relevant to determine security clearance.  Section 2A, Sub-Section 6-7 -The DG of SSA may after evaluating the gathered information, issue, degrade, withdraw or refuse to grant a security clearance. The DG of SSA may establish a security screening Advisory Board to assist in determining the security competency of a person.

Document Name	Description
Protection of Personal Information Act, 2013	<p>Sub-Section 8 - If the DG of SSA refuse a persons security clearance, withdraw or degrade it may appeal to the Minister of State Security. Such shall be lodged within 60 days from the date of the decision be made known.</p> <p>Sub-Section 9-10 - The DG of SSA may issue functional directives on: Usage and application of polygraph; Criteria for determining security competence; and Levels of security clearance. - These directives shall be issued with the approval of the Minister.</p> <p>Section 4(1) Conditions for the lawful processing of personal information by or for a responsible party.</p>

**RISKS**

Risk Name	Risk Description	Probability (H/M/L)	Impact (H/M/L)	Control Description	System / Manual
Unauthorized disclosure / unauthorized access	Unauthorized disclosure of sensitive/classified information or unauthorized access to critical infrastructure or systems contribute to espionage and system / infrastructure failure.	H	H	Implementation of Security Management Policy Security Awareness program Information Brochure	Manual

# AUTHORIZATION

Designation:	Name:	Comments	Signature:	Date:	
Recommended By: Deputy Director: Security Management	J. Van Vuuren	Business Management Process will enable management to action participation in the Vetting process as part of their management function.		2021-09-28	
Recommended by Acting CIO	M. E. Gazi		Recommended		29/09/2021
Recommended by: Chief Director: Corporate Service	P. Mwandia -Tali				15/11/2021
Recommended by: DDG	N.Z.G Yokwana	Recommended		15/11/2021	
Approved by: Acting HOD	M. Macheмба	Approved		01/12/2021	
Distribution and Use of SOP	All Departmental staff				