**ANNEXURE D**

**SENIOR MANAGEMENT PERFORMANCE AGREEMENT**

**NAME OF DEPARTMENT/PROVINCE (AS APPLICABLE)**

**BETWEEN**
**(Names and Designations of parties to agreement)**

**SMS MEMBER:**

**AND**

**HEAD OF DEPARTMENT (OR DELEGATED SUPERVISOR)**

**PERIOD OF AGREEMENT:**
**(indicate from when until when, i.e a full financial year (from 1 April 200__ to 31 March 200__ )**

## 1. JOB DETAILS

Persal number :

Component :

Location :

Salary level :

Notch (package) :

Occupational classification :

Designation :

## 2. JOB PURPOSE

Describe the purpose of the job (overall focus) as it relates to the Vision and Mission of the Department. Capture the overall accountability that the jobholder has in relation to her/his position.

## 3. JOB FUNCTIONS

Describe the key functions that the jobholder is required to perform, based on the job profile, and the departmental strategic/operational plan.

## 4. REPORTING REQUIREMENTS/LINES & ASSESSMENT LINES

4.1 The SMS member shall report to the . ……..as her/his supervisor on all parts of this agreement. The SMS member shall:

(1) Timeously alert the supervisor of any emerging factors that could preclude the achievement of any performance agreement undertakings, including the contingency measures that she/he proposes to take to ensure the impact of such deviation from the original agreement is minimised.
(2) Establish and maintain appropriate internal controls and reporting systems in order to meet performance expectations.
(3) Discuss and thereafter document for the record and future use any revision of targets as necessary as well as progress made towards the achievement of performance agreement measures.

4.2 In turn the supervisor shall:

(1) Create an enabling environment to facilitate effective performance by the SMS member.
(2) Provide access to skills development and capacity building opportunities.
(3) Work collaboratively to solve problems and generate solutions to common problems within the department that may be impacting on the performance of the SMS member.

## 5. PERFORMANCE APPRAISAL FRAMEWORK

Performance will be assessed according to the information contained in the work plan (attached as Appendix A) and the Core Management Criteria (CMC) framework (attached as Appendix B). The specific KRAs and CMCs together with their weightings are, for example, as follows:

5.1 The KRAs and CMCs during the period of this agreement shall be as set out in the table below.

5.2 The SMS member undertakes to focus and to actively work towards the promotion and implementation of the KRAs within the framework of the laws and regulations governing the Public Service. The specific duties/outputs required under each of the KRAs are outlined in the attached work plan. KRAs should include all special projects the SMS member is involved in. The work plan should outline the SMS member's specific responsibilities in such projects.

| KEY RESULT AREAS (KRAs) | Batho Pele Principles | Weight |
|---|---|---|
| 1. | | |
| 2. | | |
| 3. | | |
| 4. | | |
| 5. | | |
| **TOTAL** | | **100%** |

5.3 The SMS member's assessment will be based on her/his performance in relation to the duties/outputs outlined in the attached work plan as well as the CMCs marked here-under. CMCs should be selected (✓) from the list that are deemed to be critical for the SMS member's specific job.

| CORE MANAGEMENT CRITERIA | Batho Pele Principles | Weight | CORE MANAGEMENT CRITERIA | Batho Pele principles | Weight |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | **TOTAL** | | **100%** |

## 6. DEVELOPMENTAL REQUIREMENTS

Provide details on the areas in which development is required. These may relate to the attainment of specific objectives or standards specified for Key Result Areas (KRAs), as well as to the CMCs.

The plan for addressing developmental gaps is attached as Appendix C.
(Each manager should identify her/his involvement in the Senior Management Service Delivery Challenge – i.e. deployment to the coalface of service delivery for at least 5 days per performance cycle).

## 7. TIMETABLE AND RECORDS OF REVIEW DISCUSSIONS AND ANNUAL APPRAISAL

Specify the dates when progress reviews and feedback sessions will take place, as well as the annual evaluation session:

## 8. MANAGEMENT OF PERFORMANCE OUTCOMES

Identify and specify what actions will be taken in recognition of superior performance or to address poor/non-performance: (These should be based on Chapter 4 of the SMS Handbook).

## 9. DISPUTE RESOLUTION

9.1 Any disputes about the nature of the senior manager's PA, whether it relates to key responsibilities, priorities, methods of assessment and/or salary increment in this agreement, shall be mediated by:

9.2 If this mediation fails, the dispute-resolution procedure referred to in the SMS Handbook and/or the prescribed grievance procedures will apply.

## 10. AMENDMENT OF AGREEMENT

Amendments to the agreement should be in writing and can only be effected after discussion and agreement by both parties.

## 11. SIGNATURES OF PARTIES TO THE AGREEMENT

The contents of this document have been discussed and agreed with the SMS member concerned.

Name of SMS member:

Signature: ……..

Date: ……

*AND*

Name of supervisor of SMS member:

Signature: ……..

Date: ……

## APPENDIX A: PERFORMANCE WORK PLAN

Two examples of work plans are described here. Managers would select the appropriate form based on the nature of their job.

**EXAMPLE 1**

| KEY RESULT AREA | PERFORMANCE STANDARDS INCORPORATING BATHO PELE SERVICE DELIVERY STANDARDS | RESOURCE REQUIREMENTS | ENABLING CONDITIONS |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

OR

**EXAMPLE 2**

| KEY RESULT AREA | KEY ACTIVITIES/ OUTPUTS | PERFORMANCE MEASURES | | RESOURCE REQUIREMENTS | ENABLING CONDITIONS |
|---|---|---|---|---|---|
| | | TARGET DATE | INDICATOR | | |
| | | | | | |
| | | | | | |
| | | | | | |

## APPENDIX B: GENERIC CORE SMS MANAGEMENT CRITERIA AND STANDARDS

This shows one example of a criterion and its standards. The same approach would apply to all others

| CRITERIA | STANDARDS – BATHO PELE PRINCIPLES INCORPORATED | | WEIGHTING |
|---|---|---|---|
| | GENERIC | DEPARTMENT SPECIFIC | |
| Strategic Capability and Leadership | ◊ Gives direction to team in realising the organisation's strategic objectives;<br>◊ Impacts positively on team morale, sense of belonging and participation;<br>◊ Develops detailed action plans to execute strategic initiatives;<br>◊ Assists in defining performance measures to evaluate the success of strategies;<br>◊ Achieves strategic objectives against specified performance measures;<br>◊ Translates strategies into action plans;<br>◊ Secures co-operation from colleagues and team members;<br>◊ Seeks mutual benefit/win-win outcomes for all concerned;<br>◊ Supports stakeholders in achieving their goals;<br>◊ Inspires staff with own behaviour – "walks the talk";<br>◊ Manages and calculates risks;<br>◊ Communicates strategic plan to the organisation; and<br>◊ Utilises strategic planning methods and tools. | ◊ | (as percentage – indicated in paragraph 5 of this Annexure) |

APPENDIX C: PERSONAL DEVELOPMENT PLAN

| Competency to be addressed | Proposed actions | Responsibility | Time-frame | Expected outcome |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |

**APPENDIX D: CORE RESPONSIBILITIES AND OUTPUTS ON THE IMPLEMENTATION OF THE NATIONAL INFORMATION SECURITY POLICY**

| NR | CORE RESPONSIBILITY | KEY OUTPUTS | TARGET DATES | REVISED DATES / STANDARDS |
|---|---|---|---|---|
| 1. | Overall accountable for security at the institution and to implement the national information security policy (currently the "*Minimum Information Security Standards*" - MISS, as approved by Cabinet on 4 December 1996). | 1.1 **Designate a senior staff member (in the case of a government department, at least at the level of director) as security manager for that institution to manage the security function at the said institution; provided that the head of the institution may, with the approval of the Agency, appoint a staff member at a lower level as security manager.**<br>• The profile, post and job description should comply with the criteria as given in the NIA position paper "*Security Managers in Government* Bodies" and NIA guidance document "*Guideline – Profile of a Security Manager*".<br>• The following disciplines of security must be covered by the responsibilities of a security manager:<br>o Security administration (including record keeping, reporting and investigation of security breaches, etc.)<br>o Information security (including document security, implementation of a classification system, etc.)<br>o Physical security<br>o Personnel security (including security screening and security awareness)<br>o Information and communication technology (ICT) security.<br>• Inform NIA of the name of the security manager so appointed, to serve as a nodal point for liaison on security issues with NIA.<br>• Ensure that the Security Manager attends and passes the security management course, which is arranged or offered by NIA.<br>• The security manager should report directly to the Director General / Head of the Institution on line functional (security) and related matters. | | |

| NR | CORE RESPONSIBILITY | KEY OUTPUTS | TARGET DATES | REVISED DATES / STANDARDS |
|---|---|---|---|---|
| | | 1.2 Establish a security component or support structure for the Security Manager.<br>• **Determine the size and functions of the security component in consultation with NIA** | | |
| | | 1.3 **Establish a security committee for the institution, comprising**:<br>• the security manager of the institution (chairperson);<br>• the senior manager of the institution responsible for the management, integration and implementation of the system security architecture and maintenance of the information and communication technology system of the institution; and<br>• representatives (on senior management level) from all main business functions or structures of the institution. | | |
| | | **1.4** Ensure that a security threat and risk assessment is conducted of the institution by the security committee (according to NIA guidelines in this regard). The threat and risk assessment must include:<br>• **identification of all critical assets, systems and services of the institution;**<br>• **identification of the categories of information held by the institution that require protection against disclosure;**<br>• **identification of security threats against the institution;**<br>• **identification of security vulnerabilities;**<br>• **recommendations to address the identified vulnerabilities.** | | |

| NR | CORE RESPONSIBILITY | KEY OUTPUTS | TARGET DATES | REVISED DATES / STANDARDS |
|---|---|---|---|---|
| | | 1.5 **Ensure and oversee the development, implementation and maintenance of an internal security policy, as well as directives in connection therewith, for that institution that complies with all the requirements of the Minimum Information Security Standards.**<br>• Assign the responsibility to draft the security policy and directives to the security manager and the security committee.<br>• Ensure that the security policy assigns pertinent security responsibilities and/or duties to specific officials, and that it provides for disciplinary and remedial steps in cases of transgressions or non-compliance.<br>• Ensure that the policy and directives covers all security disciplines effectively and sufficiently. | | |
| | | 1.6 **Ensure that Staff Members and Contractors with Access to Sensitive Information are Security Cleared**<br>• Determine and list the posts/positions for which incumbents need security clearances.<br>• Determine the levels of security clearances for each post (Confidential, Secret or Top Secret).<br>• Provide the above-mentioned information to NIA.<br>• Request NIA to subject incumbents and applicants for posts (which require a security clearance) to a security competence investigation in terms of the MISS.<br>• Ensure that prospective contractors are security cleared before awarding the contract or before allowing access to the premises of the institution. | | |

| NR | CORE RESPONSIBILITY | KEY OUTPUTS | TARGET DATES | REVISED DATES / STANDARDS |
|---|---|---|---|---|
| | | 1.7 **Ensure that security training and awareness programmes are implemented in the institution to sensitise employees and relevant contractors and consultants of the institution, about the security policy and directives of the institution and the need to protect confidential information against disclosure. These programmes must, as a minimum,**:<br>• ensure that every manager and supervisor briefs his or her subordinates on the particular types of information that will be handled by them in that department, division, component or section that should be treated as confidential or secret and repeats this briefing at regular intervals;<br>• ensure that individuals who have specific security duties receive appropriate training related to those duties;<br>• empower employees and contractors to evaluate information that they come into contact with, to be able to recognize to which category it belongs, and to handle it accordingly. | | |
| | | 1.8 **Ensure that employees and contractors, to whom the institution may have to disclose sensitive or classified information are informed on a need-to-know basis and are contractually bound to keep such information secret. This must include**:<br>• directing of the legal advisers of the institution, when requested to peruse or to draw up a contract with a supplier, to consider the necessity or otherwise of including a clause into the particular contract, that would place a contractual obligation on the said contractor and his or her employees to keep secret any sensitive information of the institution that may be supplied to the supplier;<br>• requiring staff members, who negotiate contracts on behalf of the institution, not to disclose sensitive information to would-be contractors during the negotiation phase, except where this is necessary for the purposes of the negotiations. | | |

| NR | CORE RESPONSIBILITY | KEY OUTPUTS | TARGET DATES | REVISED DATES / STANDARDS |
|---|---|---|---|---|
| | | 1.9 **Consider the recommendations made in the threat and risk assessment and implement security measures in the most efficient and cost effective manner that will ensure that identified security risks will be reduced to an acceptable level**. **This must also include**:<br>• reporting to the Agency, on an annual basis, on the risks identified and the implementation of security measures to address the risks;<br>• reporting to the Agency, on an annual basis, on the categories of information held by the institution that require protection and the measures implemented to protect such information. | | |
| | | 1.10 **Implement measures to ensure the continuous monitoring of the compliance by that institution with the Minimum Information Security Standards, the internal security policy of the institution and any directives issued in connection therewith. Such measures include**:<br>• conducting of internal security audits at the institution (by the security manager of the institution);<br>• conducting of security audits by NIA;<br>• addressing security vulnerabilities identified during such audits. | | |