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.** • 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*". • The following disciplines of security must be covered by the responsibilities of a security manager: o Security administration (including record keeping, reporting and investigation of security breaches, etc.) o Information security (including document security, implementation of a classification system, etc.) o Physical security o Personnel security (including security screening and security awareness) o Information and communication technology (ICT) security. • Inform NIA of the name of the security manager so appointed, to serve as a nodal point for liaison on security issues with NIA. • Ensure that the Security Manager attends and passes the security management course, which is arranged or offered by NIA. • The security manager should report directly to the Director General / Head of the Institution on line functional (security) and related matters.		
		1.2 **Establish a security component or support structure for the Security Manager.** • Determine the size and functions of the security component in consultation with NIA		

NR	CORE RESPONSIBILITY	KEY OUTPUTS	TARGET DATES	REVISED DATES / STANDARDS
		1.3 **Establish a security committee for the institution, comprising**: • the security manager of the institution (chairperson); • 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 • 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:** • identification of all critical assets, systems and services of the institution; • identification of the categories of information held by the institution that require protection against disclosure; • identification of security threats against the institution; • identification of security vulnerabilities; • recommendations to address the identified vulnerabilities.		
		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.** • Assign the responsibility to draft the security policy and directives to the security manager and the security committee. • 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. • Ensure that the policy and directives covers all security disciplines effectively and sufficiently.		

NR	CORE RESPONSIBILITY	KEY OUTPUTS	TARGET DATES	REVISED DATES / STANDARDS
		1.6 **Ensure that Staff Members and Contractors with Access to Sensitive Information are Security Cleared** • Determine and list the posts/positions for which incumbents need security clearances. • Determine the levels of security clearances for each post (Confidential, Secret or Top Secret). • Provide the above-mentioned information to NIA. • Request NIA to subject incumbents and applicants for posts (which require a security clearance) to a security competence investigation in terms of the MISS. • Ensure that prospective contractors are security cleared before awarding the contract or before allowing access to the premises of the institution.		
		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,**: • 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; • ensure that individuals who have specific security duties receive appropriate training related to those duties; • 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.		

NR	CORE RESPONSIBILITY	KEY OUTPUTS	TARGET DATES	REVISED DATES / STANDARDS
		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**: • 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; • 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.		
		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**: • reporting to the Agency, on an annual basis, on the risks identified and the implementation of security measures to address the risks; • 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**: • conducting of internal security audits at the institution (by the security manager of the institution); • conducting of security audits by NIA; • addressing security vulnerabilities identified during such audits.		