



the dr&pw

---

Department:  
Roads and Public Works  
NORTHERN CAPE PROVINCE  
REPUBLIC OF SOUTH AFRICA

**TERMS OF REFERENCE OF THE  
DEPARTMENTAL SECURITY AND  
INFORMATION AND COMMUNICATION  
TECHNOLOGY COMMITTEE (SICTC)**

Version 1  
(March 2015)

**1. PURPOSE OF THE SECURITY AND INFORMATION AND COMMUNICATION TECHNOLOGY COMMITTEE (SICTC)**

The Security and Information and Communication Technology Committee (SICTC) is a committee of the Department charged with the responsibility to oversee the development, implementation, monitoring and review of the Department's policies, procedures, practices, and guidelines aimed at assisting the Head of Department (HOD) to ensure that there is a continuous monitoring of the compliance with Minimum Physical Security Standards as well as realizing the Department's goals and objectives on the provision and support of Information Technology Security Infrastructure and services.

- 1.1. The SICTC is the principal departmental forum focusing on Physical Security and Information and Communication Technology (ICT) Security Management in the Department of Roads and Public Works.
- 1.2. The SICTC is established in order to enable the HOD to respond to his/her overall accountability for the overall physical security of the Department under his/her control; to oversee the development, implementation and maintenance of internal security and information technology security policies in terms of relevant legislation; and to ensure that employees and service providers (contractors/consultants) are subjected to reliability record checking processes conducted by the State Security Agency (SSA).
- 1.3. The SICTC furthermore provides strategic direction and operational oversight as far as the Department of Roads and Public Works' ICT security and security related matters in terms of the Management Information Systems (MIS) policies and procedures are concerned, whilst guiding the Department in executing its mandate.
- 1.4. Day-today operational oversight of divisions supplying Security, Information and Communication Technology services or administrative support services through the medium of Security and Information technology is NOT a role or responsibility of the SICTC; this is affected through the management reporting structures of the Department.

## **2. STRATEGIC FOCUS OF THE SICTC**

The SICTC is strategically focused on maximizing the value of Public Service Security and ICT investment by:

- 2.1. Making recommendations on the Physical Security and ICT Security policies of the Department after having taken into account the advice provided by the South African Police Services (SAPS), the State Security Agency (SSA), the State Information Technology Agency (SITA) and the Government Communication and Information System (GCIS).
- 2.2. Making recommendations to the HOD and Senior Management of the Department regarding the implementation and maintenance of Physical Security and ICT Security measures.
- 2.3. Regularly reviewing the Physical Security and ICT Security policies of the Department, the prioritisation thereof as well as information and advice provided by the institutions as mentioned in 2.1 above.
- 2.4. Forwarding the abovementioned draft security policies and reviews thereof to the institutions as mentioned in 2.1 above.
- 2.5. Circulating the draft Physical Security and ICT Security policies or any review thereof in the Main and Regional Offices of the Department for comments and inputs.
- 2.6. Submitting the Physical Security and ICT Security policies or any review thereof to the HOD for approval.
- 2.7. Ensuring the communication of the approved Physical Security and ICT Security policies to all departmental staff members, relevant consultants and contractors.

- 2.8. Making recommendations to the HOD regarding directives to be issued by the HOD to ensure the implementation of the Physical Security and ICT Security policies or any review thereof.
- 2.9. Leveraging economies of scale in Physical Security and ICT Security solution provision, maintenance and support.
- 2.10. Eliminating duplication in Physical Security and ICT Security functions, projects, resources, and information.
- 2.11. Enforcing interoperability of Departmental and Governmental Physical Security and ICT Security systems, including networks, platforms, applications and dSata compatibility.
- 2.12. Aligning the improvement of the security of electronic documents and data, personal computers (PC's), laptop computers, information systems, networks and user access from other users and viruses.
- 2.13. Aligning the respective Physical Security, MIS and ICT Security strategies with government priorities and business strategies.
- 2.14. Improving the practices of the Department on matters of the utilization and sharing of resources as far as Physical Security, MIS and ICT Security matters are concerned.
- 2.15. Make recommendations for the department's MIS and ICT security resources, management, policy, procedure, norms, standards, guidelines and best practices.
- 2.16. Identify opportunities for co-operation within the Department and between the public and private sector in providing access to and using information and ICT Security resources.
- 2.17. Identify common solutions for common requirements across the Department wherever possible.

- 2.18. Identify or recommend on lead agencies in promoting security automation initiatives in the Department, including e-Government.
- 2.19. Conceptualize, consolidate and co-ordinate IT Security related projects.
- 2.20. Position the Department in the forefront of e-Government initiatives within the Province.
- 2.21. Provide strategic direction for the security of the department's information technology and network related infrastructure and services.
- 2.22. Develop, monitor and review departmental policies, guidelines, procedures, and significant incidents relating to information security and information technology security, and renewal of the department's ICT Security infrastructure.
- 2.23. Ensure that policies and procedures so formulated are not in contravention of existing security policies and procedures established by Law.
- 2.24. Receive reports from, provide feedback and advice to, and take decisions relating to security policy and processes, of divisions supplying information technology services or administrative support services through the medium of information technology.
- 2.25. Assess operational and reputational risks to the Department associated with the use of ICT Security, and comment on or develop ICT Security strategy as it relates to the departmental institutional security strategy.
- 2.26. Comment on institutional level risk management issues relating to information security and information technology raised by the Audit Committee or reports of the appointed Auditors.
- 2.27. Be a sounding board for divisions with decision making mandates over aspects of the Department's use of ICT Security, in their design, development, acquisition, or establishment of procedures for the use of the ICT Security systems of the Department.

- 2.28. Act as think tank for the Department in terms of Physical and ICT Security matters, to brain storm new ideas, and to address such topics as might be relevant and requested by various stake holders within the Department.

### 3. SCOPE OF OPERATION AND REGULATORY FRAMEWORK

The SICTC focuses on all Security, ICT and MIS issues in the Department in terms of:

- The South African Constitution Act, Act No. 108 of 1996.
- The Public Service Act, Act No. 103 of 1994, as amended.
- The Public Finance Management Act (PFMA), Act No. 1 of 1999, as amended and Treasury Regulations.
- The Preferential Procurement Policy Framework Act (PPPFA), Act No. 5 of 2000.
- The Telecommunications Act, Act No. 103 of 1996.
- The Electronic Communications and Transactions Act, Act No. 25 of 2002 (the ECT Act).
- The Regulation of Interception of Communications and Provision of Communication-Related Information Act, Act No. 70 of 2002.
- The State Information Technology Agency Act, (SITA Act), Act No. 88 of 1998, as amended.
- The Control of Access to Public Premises and Vehicles Act, Act No.53 of 1985.
- The Criminal Procedure Act, Act No. 51 of 1977.
- The National Key Point Act, Act No. 102 of 1980.
- The Minimum Information Security Standards (MISS) policy as approved by Cabinet on 04 December 1996, as amended.
- The Minimum Information Security Standards (MISS), Second Edition March 1998.
- The Minimum Physical Security Standards (MPSS) of 2009.
- The Private Security Industry Regulations Act, Act No. 56 of 2001.
- The Protection of Information Act, Act No. 84 of 1982.
- The Promotion of Access to Information Act, Act No. 2 of 2000.
- The Promotion of Administrative Justice Act, Act No. 3 of 2000.
- The National Archives of South Africa Act, Act No. 43 of 1996.
- The Occupational Health and Safety Act, Act No. 85 of 1993, as amended.

- The Constitution of the Republic of South Africa, Act 108 of 1996.
- The Trespass Act, Act No.6 of 1959.
- The General Intelligence Law Amendment Act, Act No. 66 of 2000.
- The National Strategic Intelligence Act, Act No. 39 of 1994.
- The Fire-arms Control Act, Act No. 60 of 2000 and regulations.
- The Protected Disclosures Act, Act No. 26 of 2000.
- Prevention and Combating of Corrupt Activities Act, Act No. 12 of 2004.
- The South African Communication Security Agency, SACSA/090/1(4) Communication Security in the RSA.
- Proclamation No R 59 of 2009 – establishment of the State Security Agency (SSA).
- The Intelligence Service Control Act, Act No. 40 of 1994.
- The National Building Regulations and Building Standards Act, Act No. 103 of 1977.
- The Public Service Regulations, 2001, as amended in 2002: Chapter 1, Part iii, Regulation E, and Chapter 5, Part I, Part ii, Part iii.
- The Government Information Technology (Gito) Council, as approved by the Department of Public Service and Administration (DPSA): Information Technology Planning Framework, 2002.
- DPSA: Handbook on Minimum Information Security Standards (MISS), 2002: Chapter 6, Chapter 7, Chapter 8.
- DPSA: Handbook on Minimum Interoperability Standards (MIOS), 2002.

#### **4. THE COMPOSITION AND FUNCTIONS OF THE SECURITY AND INFORMATION AND COMMUNICATION TECHNOLOGY COMMITTEE (SICTC)**

##### **4.1 Composition of the SICTC**

Permanent staff members of the Department shall be formally appointed by the Head of Department to be members of the SICTC. The Committee members shall collectively possess the specialised skills, knowledge and expertise of the Department, including familiarity with the Physical Security and Information and Communication Technology Security fields in order to contribute meaningfully to the Committee.

The establishment of the SICTC for the Department is in accordance with the Minimum Physical Security Standards (MPSS) of 2009, which requires that this Committee comprise of the following officials:

- The Senior Manager of the Department responsible for the management, integration and implementation of the system security architecture and maintenance of the Department's information security infrastructure.
- The Security Manager of the Department. (For technical inputs and advice.)
- The Information Technology (IT) Manager of the Department. (For technical inputs and advice.)
- A representative from the Property Management unit.
- Representatives (on Senior Management level) from all main business functions or structures of the Department, namely Roads; Human Capital Management; Finance; EPWP and Public Works; Corporate Services; Policy and Planning; Monitoring & Evaluation and Organisational Risk; as well as Legal Services.
- Any other person who may be co-opted to provide specialised security skills, advice and counsel.

## **4.2 Duties and Powers of the various Committee Members**

### **4.2.1 The Chairperson of the SICTC**

- Has a casting vote as well as a deliberate vote.
- Retains all his/her rights as a member.
- May adjourn a meeting.
- May rule on points of order which will be final.
- May withdraw any proposal or other matters under discussion before it is put to the vote.
- Convene extraordinary Committee meetings on request.
- Maintain order during a meeting and ensure that business is conducted in an orderly manner.
- Before opening a meeting, ensure that it is properly constituted.
- Protects the rights of every Committee member.



- Will ensure that there is an agenda for the meeting and ensure that the minutes are ready for every meeting convened, except when the meeting is convened on an urgent basis.
- Must reprimand committee members for not attending meetings without any apology.

#### **4.2.2 The Vice-chairperson of the SICTC**

In the absence of the Chairperson the Vice-chairperson shall resume automatic responsibility for the Chairperson. The Vice-chairperson shall support the Chairperson.

#### **4.2.3 The SICTC Members**

- Participate in special Committee activities.
- Promote Committee decisions within the Department.
- Communicate Committee recommendations to their respective units, peers and users.
- Identify viable Physical Security and ICT (Information and Communication Technology) Security issues for presentation to the Committee, inclusive of supportive material and the facilitation thereof.

#### **4.2.4 Co-opted SICTC members**

- The SICTC may request advisors, specialists or any other persons, as deemed fit, to attend the meetings of the Committee.
- Attendance of any of these persons to the meetings shall be restricted to the area of concern as presented on the agenda.
- The Chairperson must approve the attendance of invited co-opted members to attend a Committee meeting or a consequent meeting(s) thereafter.
- A co-opted member cannot vote on any matters balloted by the Committee.
- The Committee, through the Chairperson, may request invitees to leave the meeting venue during the discussion of sensitive agenda items, as defined by the Committee.

#### **4.3 Functions of the SICTC**

The SICTC is responsible for the following:

- 4.3.1 Making recommendations on the Physical Security and Information and Communication Technology Security policies of the Department, after having taken into consideration the advice provided by the South African Police Services (SAPS), the State Security Agency (SSA), the State Information Technology Agency (SITA) and the Government Communication and Information System (GCIS).
- 3.3.2 Making recommendations to the Head of Department (HOD) regarding the implementation and maintenance of Physical Security and Information and Communication Technology Security measures.
- 4.3.3 Regular review of the Physical Security and Information and Communication Technology Security policies of the Department, the prioritisation thereof, as well as information and advice provided by the SAPS, the SSA, the SITA and the GCIS.
- 4.3.4 Forward the draft Physical Security and Information and Communication Technology Security policies of the Department and any reviews thereof to the SAPS, the SSA, the SITA and the GCIS.
- 4.3.5 After endorsement by the SAPS, the SSA, the SITA and the GCIS, to submit the security policies or any review thereof to the HOD for approval.
- 4.3.6 Ensure the communication of the approved security policies to all departmental staff members, relevant consultants and contractors.
- 4.6.7 Making recommendations to the HOD regarding directives to be issued by the HOD to ensure the implementation of the said departmental security policies or any review thereof.

#### **4.7 Meetings of the SICTC**

The Security and Information and Communication Technology Committee (SICTC) shall meet at least four times per annum. The Chairperson of the Committee or a majority of the permanent members of the Committee may convene additional meetings as circumstances may dictate.

#### **4.8 Administrative duties**

A permanent Committee member shall be appointed by the Chairperson of the Committee on the advice of the other permanent Committee members as the Secretary

of the Committee. The Secretary shall forward the notice of each meeting of the Committee to all members not later than ten working days prior to the day of the meeting. The notice shall confirm the venue, time, date and agenda, and shall include the documents for discussion.

**4.9 Quorum**

The total number of fifty per cent (50%) plus one (1) member constitutes a quorum. A permanent member may nominate a proxy on his/her behalf. This provision shall lapse in the event that the permanent member fails to attend three (3) or more Committee meetings held in that particular financial year in person.

**4.10 Reviewing of SICTC Performance**

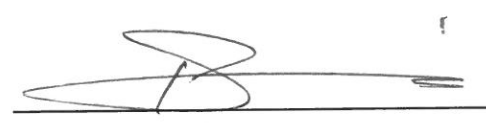
The SICTC shall review its performance annually and make recommendations to the HOD in this regard, before forwarding the review to the HOD for approval.

**5. APPROVAL OF THE TERMS OF REFERENCE OF THE SICTC**

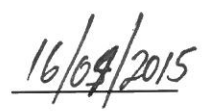
*Approved / Not Approved*

*Comments:*

.....  
.....  
.....  
.....



**HEAD OF DEPARTMENT**



**DATE**