

101104
ad hoc protect

REPUBLIC OF SOUTH AFRICA

**PROTECTION OF
INFORMATION BILL**

P I 2

[18-4-2010]

*(As introduced in the National Assembly (proposed section 75); explanatory summary of Bill
published in Government Gazette No. 32999 of 5 March 2010)*

(The English text is the official text of the Bill)

(MINISTER OF STATE SECURITY)

BILL

To provide for the protection of certain information from destruction, loss or unlawful disclosure; to regulate the manner in which information may be protected; to repeal the Protection of Information Act, 1982; and to provide for matters connected therewith.

PREAMBLE

RECOGNISING the importance of information to the national security, territorial integrity and well-being of the Republic;

ACKNOWLEDGING the harm of excessive secrecy;

AFFIRMING the constitutional framework for the protection and regulation of access to information;

DESIRING to put the protection of information within a transparent and sustainable legislative framework;

AIMING to promote the free flow of information within an open and democratic society without compromising the security of the Republic,

BE IT THEREFORE ENACTED by the Parliament of the Republic of South Africa, as follows:-

CONTENTS

Section

CHAPTER 1

DEFINITIONS, OBJECTS AND APPLICATION OF ACT

1. Definitions and interpretation
2. Objects of Act
3. Application of Act
- 4.

CHAPTER 2

GENERAL PRINCIPLES OF STATE INFORMATION

4. State information
5. Protected information
6. General principles of State information

CHAPTER 3

NATIONAL INFORMATION SECURITY STANDARDS AND PROCEDURES AND
DEPARTMENTAL POLICIES AND PROCEDURES

7. National standards and procedures
8. Departmental policies and procedures

CHAPTER 4

INFORMATION WHICH REQUIRES PROTECTION AGAINST ALTERATION,
DESTRUCTION OR LOSS

9. Process of determining information as valuable
10. Protection of valuable information

CHAPTER 5

INFORMATION WHICH REQUIRES PROTECTION AGAINST DISCLOSURE

*Part A**Sensitive Information*

11. National interest of Republic

*Part B**Commercial Information*

12. Nature of commercial information

CHAPTER 6

CLASSIFICATION AND DECLASSIFICATION OF INFORMATION

Part A

Classification

13.	Nature of classified information	
14.	Method of classifying information	
15.	Classification levels	10
16.	Authority to classify information	
17.	Directions for classification	
18.	Report and return of classified documents	
19.		15

Part B

Declassification

19.	Authority to declassify information	20
20.	Maximum protection periods	
21.		

CHAPTER 7

CRITERIA FOR CONTINUED CLASSIFICATION OF INFORMATION	25
--	----

21.	Continued classification of information	
22.	Regular reviews of classified information	30
23.	Requests for status reviews of classified information	
24.	Status review procedure	
25.	Appeal procedure	

CHAPTER 8

TRANSFER OF RECORDS TO NATIONAL ARCHIVES

26. Transfer of Public Records to National Archives

5

CHAPTER 9

RELEASE OF DECLASSIFIED INFORMATION TO PUBLIC

27. Release of declassified information to public
28. Request for classified information in terms of Promotion of Access to Information Act, 2000
29. Establishment of National Declassification Database

10

CHAPTER 10

IMPLEMENTATION AND MONITORING

30. Responsibilities of State Security Agency
31. Dispute Resolution

CHAPTER 11

OFFENCES AND PENALTIES

32. Espionage offences
33. Hostile activity offences
34. Harboursing or concealing persons
35. Interception of or interference with classified information
36. Registration of intelligence agents and related offences
37. Attempt, conspiracy and inducement
38. Disclosure of classified or related information

- 39. Failure to report possession of classified information
- 40. Provision of false information to national intelligence structure
- 41. Destruction of valuable information
- 42. Improper classification of information
- 43. Prohibition of disclosure of State security matter
- 44. Extra-territorial application of Act
- 45. Authority of National Director of Public Prosecutions for institution of criminal proceedings

CHAPTER 12

PROTECTION OF INFORMATION IN COURTS

- 46. Protection of State information before courts

CHAPTER 13

GENERAL PROVISIONS

- 47. Reports
- 48. Regulations
- 49. Transitional provisions
- 50. Repeal of laws
- 51. Short title and commencement

35

40

CHAPTER 1

DEFINITIONS, OBJECTS AND APPLICATION OF ACT

1. (1) In this Act, unless the context indicates otherwise-

Definitions and interpretation

"Agency" means the State Security Agency established in terms of Proclamation No. 59 of 2009 as published in Government Gazette No. 32566 of 11 September 2009, and includes the National Intelligence Agency, the South African Secret Service, Electronic Communications Security (Pty) Ltd (COMSEC), and the South African National Academy for Intelligence;

"archive" means any archive established in terms of a national or a provincial law;

"categories of information" means those groupings, types, classes, file series or integral file blocks of classified information that may be classified, declassified or downgraded together or in bulk;

"categorisation of information" means the process by which State information is placed into categories for purposes of classifying such information and for purposes of declassification and downgrading of information;

"classification authority" means the entity or person authorised to classify State information, and includes-

(a) a head of an organ of state; or

(b) any official to whom the authority to classify State information has been delegated in writing by a head of an organ of state;

"classification of information" means a process used to determine

(a) the level of protection assigned to certain information; and

(b) the manner in which such information may be accessed and classified in terms of section 15;

"classified information" means the State information that has been determined under this Act or the former Minimum Information Security Standards guidelines to be information that may be afforded heightened protection against unlawful disclosure;

"commercial information" means commercial, business, financial or industrial-

~~information held by or in the possession of an organ of state;~~

"confidential information" has the meaning assigned to it in section 15(1);

"Constitution" means the Constitution of the Republic of South Africa, 1996;

"declassification authority" means the entity or person authorised under section 19 to declassify classified information;

"declassification database" means the database which contains all declassified information considered by declassification authorities to be accessible by members of the public;

"declassification of information" means the authorised change in the status of information from classified information to unclassified information;

"department" means a department as defined in section 1 of the Public Service Act, 1994 (Proclamation No. 103 of 1994);

"downgrading of information" means a change of classified and safeguarded information from its status to be reclassified and safeguarded at a lower level;

"file series" means file units or documents that are arranged according to a filing system or kept together because they-

(a) relate to a particular subject or function;

(b) result from the same activity, instruction, document or a specific kind of transaction;

(c) take a particular physical form; or

(d) have some other relationship arising out of their creation, receipt, or use, such as restrictions on access or use;

"foreign State" means any State other than the Republic of South Africa;

"head of an organ of state" means-

(a) in the case of a department, the officer who is the incumbent of the post bearing the designation mentioned in Column 2 of Schedule 1, 2 or 3 to the Public Service Act, 1994 (Proclamation No 103 of 1994), or the person who is acting as such;

(b) in the case of a municipality, the municipal manager appointed in terms of section 82 of the Local Government: Municipal Structures Act, 1998 (Act No. 117 of 1998), or the person who is acting as such;

(c) in the case of any other institution, the chief executive officer or equivalent officer of that public body or the person who is acting as such; or

(d) in the case of a national key point declared as such in terms of the National Key Points (Act No. 102 of 1980), the owner of the national key point;

"identifiable damage" means significant and demonstrable harm;

"information" means any facts, particulars or details of any kind, whether true or false, and

contained in any form, whether material or not, including, but not limited to--

- (a) documents, records, data, communications and the like, whether in paper, electronic, digital, audio-visual format, DVD, microform C, microphone, microfilm and microfiche form or format or any other form or format; and
- (b) conversations, opinions, intellectual knowledge, voice communications and the like not contained in material or physical form or format;

"information and communication technology security" means the application of security measures to protect the design, development, implementation, support, management and use of-

- (a) computer-based information systems, including software applications, computer hardware and data; and
- (b) electronic and mobile communication systems and the transmission of data;

"information principles" means the principles that guide the protection of information as set out in Chapter 2;

"information security" means the safeguarding or protecting of information in whatever form and includes, but is not limited to--

- (a) document security measures;
- (b) physical security measures for the protection of information;
- (c) information and communication technology security measures;
- (d) personnel security measures;
- (e) continuity planning;
- (f) security screening;
- (g) technical surveillance counter-measures;
- (h) dealing with and reporting of information security breaches;
- (i) investigations into information security breaches; and
- (j) administration and organisation of the security function at organs of state to ensure that information is adequately protected;

"integral file block" means a distinct component of a file series that must be maintained as a separate unit to ensure the integrity of the records, and may include a set of records covering either a specific topic or a period of time;

"intelligence" means any information, obtained by a national intelligence structure, for the purpose of crime prevention, investigation and combating or for the purpose of informing any government decision or policy-making process carried out in order to protect national security or to further the national interest, and includes the following:

- (a) "Counter-intelligence", which means measures and activities conducted,

instituted or taken to impede and to neutralise the effectiveness of foreign or hostile intelligence operations, to protect intelligence and any classified information, to conduct security screening investigations and to counter sedition, treason and terrorist and -related activities;

(b) "crime intelligence", which means intelligence used in the prevention of crime or to conduct criminal investigations and to prepare evidence for the purpose of law enforcement and the prosecution of offenders;

(c) "departmental intelligence", which means intelligence about any threat or potential threat to the national security and stability of the Republic which falls within the functions of a department of State, and includes intelligence needed by such department in order to neutralise such a threat;

(d) "domestic intelligence", which means intelligence on any internal activity, factor or development which is detrimental to the national stability of the Republic, as well as threats or potential threats to the constitutional order of the Republic, the safety and the well-being of its people, on all matters relating to the advancement of public good and all matters relating to the protection and preservation of all things owned or maintained for the public by the State;

(e) "domestic military intelligence", which means intelligence required for the planning and conduct of military operations within the Republic to ensure security and stability for its people;

(f) "foreign intelligence", which means intelligence on any external threat or potential threat to the ~~national interests~~ national security of the Republic and its people, and intelligence regarding opportunities relevant to the protection and promotion of such ~~national interests~~ national security irrespective of whether or not it can be used in the formulation of the foreign policy of the Republic; and

(g) "foreign military intelligence", which means intelligence regarding the war potential and military establishment of foreign countries (including their capabilities, intentions, strategies and tactics) which can be used by the Republic in the planning of its military forces in time of peace and for the conduct of military operations in time of war;

"legitimate interest" means an interest that is consistent with the Constitution, applicable law and the mandate of an institution or organ of state;

"Minister" means the President or the member of the Cabinet designated by the President in terms of section 209(2) of the Constitution to assume political responsibility for the control and direction of the intelligence services established in terms of section 209(1) of the Constitution;

"MISS Guidelines" means the Minimum Information Security Standards document as approved by Cabinet on 4 December 1996;

"National Archives" means the National Archives and Records Service of South Africa established by section 2 of the National Archives and Records Service of South Africa Act, 1996 (Act No. 43 of 1996);

"national intelligence structures" means-

- (a) the National Intelligence Coordinating Committee (Nicoc);
- (b) the intelligence division of the National Defence Force;
- (c) the intelligence division the South African Police Service; and
- (d) the Agency;

~~"national interest of the Republic" has the meaning assigned to it in section 11;~~

"national security" means the

~~resolve of South Africans as individuals and as a nation, to live as equals, to live in peace and harmony, to be free from fear and want~~

~~and to seek a better life, and includes protection of the people and occupants of the Republic from hostile acts of foreign intervention, terrorist and related activities, espionage and violence, whether directed from or committed within the Republic or not, and includes the carrying out of the Republic's responsibilities to any foreign country in relation to any of the matters referred to in this definition;~~

"need-to-know" means a determination made by an authorised person that a person with a valid security clearance gains access to such classified information as may be necessary to enable him or her to perform his or her functions;

"organ of state" means-

- (a) any organ of state as defined in section 239 of the Constitution, including, but not limited to, any public entity as defined in section 1 of the Public Finance Management Act, 1999 (Act No.1 of 1999), and section 3 of the Municipal Finance Management Act, 2003 (Act No.56 of 2003);
- (b) any facility or installation declared as a National Key Point in terms of the National Key Points Act, 1980 (Act No. 102 of 1980);

"original classification authority" means the head of the organ of state that authorised the original classification, or the person or entity authorised by the head of the organ of state to do so;

"personal information" means any information concerning an identifiable natural person which, if disclosed, could reasonably be expected to endanger the life or physical safety or general welfare of an individual;

"physical security" means the use of physical measures to--

- (a) prevent or deter unauthorised persons from accessing protected information;
- (b) detect attempted or actual unauthorised access; and
- (c) activate an appropriate response;

"Promotion of Access to Information Act" means the Promotion of Access to Information Act, 2000 (Act No.2 of 2000);

"protected information" means State information which requires protection against destruction, loss or unlawful disclosure;

"public interest" means all those matters that constitute the common good, well-being or general welfare and protection of the people of South Africa, the promotion of which, are required by, or are in accordance with the Constitution;

"public record" means a record created or received by a governmental body in pursuance of its activities;

"record" means recorded information regardless of form or medium;

"regulations" includes regulations issued by the Minister in terms of this Act;

"secret information" has the meaning assigned to it in section 15(2);

"security" means to be protected against danger, loss or harm, and is a condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts;

"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;

"security committee" means the committee, comprising representatives from all the main functions or structures of an institution, charged with overseeing the development, implementation and maintenance of the institution's security policy;

"sensitive information" means information which must be protected from unlawful disclosure in order to prevent the ~~national interest~~ national security of the Republic from being harmed;

"State information" means information generated, acquired or received by organs of state or in the possession or control of organs of state;

"State operations" means any function, activity or process conducted by an organ of state which is authorised by law and is in accordance with the Constitution;

"State security matter" includes any matter which is dealt with by the Agency or which relates to the functions of the Agency or to the relationship existing between

any person and the Agency;

"technical surveillance countermeasures" means the process involved in the detection, localisation, identification and neutralisation of technical surveillance of an individual, an institution, a facility or a vehicle;

"this Act" includes regulations made in terms of section 48;

"top secret information" has the meaning assigned to it in section 15(3);

"valuable information" means-

(a) the information that should be retained for later use or reference; and

(b) that the alteration, loss or destruction of such information is likely to-

(i) impede or frustrate the State in the conduct of its functions; and

(ii) deny the public or individuals of a service or benefit to which they are entitled.

(2) This Act must be interpreted to give effect to its objects and to develop the information principles set out in Chapter 2.

(3) When considering an apparent conflict between this legislation and other information-related legislation, every court must prefer any reasonable interpretation of the legislation that avoids a conflict over any alternative interpretation that results in a conflict.

(4) For the purposes of this Act a person is regarded as having knowledge of a fact if-

(a) that person has actual knowledge of the fact; or

(b) the court is satisfied that-

(i) the person believes that there is a reasonable possibility of the existence of that fact; and

(ii) the person has failed to obtain information to confirm the existence of that fact,

and "knowing" shall be construed accordingly.

(5) For the purposes of this Act a person ought reasonably to have known or suspected a fact if the conclusions that he or she ought to have reached, are those which would have been reached by a reasonably diligent and vigilant person having both-

(a) the general knowledge, skill, training and experience that may reasonably be expected of a person in his or her position; and

(b) the general knowledge, skill, training and experience that he or she in fact has.

Objects of Act

2. The objects of this Act are to-

- (a) regulate the manner in which State information may be protected;
- (b) promote transparency and accountability in governance while recognising that State information may be protected from disclosure in order to safeguard the ~~national interest~~ national security of the Republic;
- (c) establish general principles in terms of which State information may be handled and protected in a constitutional democracy;
- (d) provide for a thorough and methodical approach to the determination of which State information may be protected;
- (e) provide a regulatory framework in terms of which protected information is safeguarded in terms of this Act;
- (f) define the nature and categories of information that may be protected from destruction, loss or unlawful disclosure;
- (g) provide for the classification and declassification of classified information;
- (h) create a system for the review of the status of classified information by way of regular reviews and requests for review;
- (i) regulate the accessibility of declassified information to the public;
- (j) harmonise the implementation of this Act with the Promotion of Access to Information Act and the National Archives and Records Service of South Africa Act, 1996 (Act No. 43 of 1996);
- (k) establish a National Declassification Database of declassified information that will be made accessible to members of the public;
- (l) criminalise espionage and activities hostile to the Republic and provide for certain other offences and penalties; and
- (m) repeal the Protection of Information Act, 1982 (Act No. 84 of 1982).

Application of Act

3.(1) This Act applies to

- (a) all organs of state; and
- (b) juristic and natural persons to the extent that the Act imposes duties and obligations on such persons.

(2) The Minister, on good cause shown and on such terms and conditions as the Minister may determine, may by notice in the *Gazette*-

- (a) exempt an organ of state or a group or class of organs of state from the application

of the duty to establish departmental standards and procedures in terms of section 8;

(b) restrict or preclude an organ of state or a group or class of organs of state from exercising the authority to classify information in terms of Chapter 6;

(c) grant to an organ of state an extension of the 18 months' period referred to in section 23(5);

(d) exempt an organ of state from declassifying information before such information is transferred to the National Archives or other archives in terms of section 26; or

(e) exempt an organ of state from section 30(1) insofar as the section authorises the Agency to carry out on-site inspections and reviews for the purposes of monitoring the protection of information programmes.

(3) The Minister, on his or her own accord or on a request made by an organ of state, may by notice in the *Gazette*-

(a) determine that an organ of state is to be regarded as part of another organ of state;

(b) determine that a category of organs of state is to be regarded as one organ of state with such head of organ of state as the Minister specifies; and

(c) if there is doubt as to whether an organ of state is a separate organ of state or forms part of another organ of state, determine that the organ of state-

(i) is a separate organ of state; or

(ii) forms part of another organ of state.

GENERAL PRINCIPLES OF STATE INFORMATION

State information

4. State information may, in terms of this Act, be protected against unlawful disclosure, destruction, alteration or loss.

Protected information

5. (1) State information which requires protection against unlawful alteration, destruction or loss, is referred to as "valuable information".

(2) State information in material or documented form which requires protection against unlawful disclosure may be protected by way of classification and access to such information may be restricted to certain individuals who carry a commensurate security clearance.

General principles of State information

6. The following principles underpin this Act and inform its implementation and interpretation:

(a) Unless restricted by law or by justifiable public or private considerations, State information

should be available and accessible to all persons;

(b) information that is accessible to all is the basis of a transparent, open and democratic society;

(c) access to information is a basic human right and promotes human dignity, freedom and the achievement of equality;

(d) the free flow of information promotes openness, responsiveness, informed debate, accountability and good governance;

(e) the free flow of information can promote safety and security;

(f) accessible information builds knowledge and understanding and promotes creativity, education, research, the exchange of ideas and economic growth;

(g) some confidentiality and secrecy is, however, vital to save lives, to enhance and to

protect the freedom and security of persons, to bring criminals to justice, to protect the national security and to engage in effective government and diplomacy;

(h) measures to protect State information should not infringe unduly on personal rights and liberties or make the rights and liberties of citizens unduly dependent on administrative decisions; and

(i) measures taken in terms of this Act must-

(i) have regard to the freedom of expression, the right of access to information and the other

rights and freedoms enshrined in the Bill of Rights; and

(ii) be consistent with article 19 of the International Covenant on Civil and Political Rights and

have regard to South Africa's international obligations;

(j) paragraphs (a) to (i) are subject to the security of the Republic, in that the national security of the Republic may not be compromised.

CHAPTER 3

NATIONAL INFORMATION SECURITY STANDARDS AND DEPARTMENTAL POLICIES AND PROCEDURES

National standards and procedures

7. (1) The Minister must, within 12 months of the commencement of this Act-

(a) prescribe broad categories and subcategories of information that may be classified, downgraded and declassified and protected against destruction, alteration and loss;

(b) prescribe categories and subcategories of information that may not be protected in terms of this Act; and

- (c) prescribe national information security standards and procedures for the categorisation, classification, downgrading and declassification of information.
- (2) The national information security standards referred to in subsection (1)(b) include, but are not limited to-
 - (a) organisation and administration of information security matters at organs of state;
 - (b) personnel security, including training, awareness and security screening;
 - (c) information and communication technology security;
 - (d) physical security for the protection of information in consultation with the Minister of Police; and
 - (e) continuity planning.
- (3) Before the Minister prescribes any categories of information in terms of subsection (1)(a), the Minister-
 - (a) must by notice in the *Gazette* provide an opportunity for organs of state and other interested persons to submit comments in respect of the categorisation in question; and
 - (b) may take into account any comments received as a result of the notice contemplated in paragraph (a).
- (4) Subsection (2) applies to any modification to the categories of information prescribed in terms of subsection (1).
- (5) No measure taken under this section may impede or prevent the National Archives or any other archive from preserving and managing public records in terms of the National Archives and Records Service of South Africa Act, 1996 (Act No. 43 of 1996), or other applicable law or ordinance.

Departmental policies and procedures

- 8. (1) The head of each organ of state must establish departmental policies, directives and categories for classifying, downgrading and declassifying information and protection against loss, destruction and unlawful disclosure of information created, acquired or received by that organ of state.
- (2) Departmental policies and directives must not be inconsistent with the national information security standards prescribed in terms of section 7.
- (3) Each organ of state must establish departmental policies, directives and

categories in terms of subsection (1) within 18 months of the commencement of this Act.

CHAPTER 4

INFORMATION WHICH REQUIRES PROTECTION AGAINST ALTERATION, DESTRUCTION OR LOSS

Process of determining information as valuable

9. (1) State information must be determined as valuable when that information is identified in terms of a prescribed procedure or policy as information that should be protected from destruction and loss.

(2) Items of valuable information and files, integral file blocks, file series or categories of valuable information must be entered into a departmental register of valuable information.

(3) Items of information, files, integral file blocks, file series or categories of State information may be determined as valuable in advance.

(4) When State information is categorised as valuable, all individual items of information that fall within a valuable category are automatically deemed to be valuable.

Protection of valuable information

10. (1) Valuable information warrants a degree of protection and administrative control and must be handled with due care and only in accordance with authorised procedures.

(2) Valuable information need not be specifically marked, but holders of such information must be made aware of the need for controls and protections as set out in the regulations.

(3) The destruction of public records is subject to the National Archives and Records

Service of South Africa Act, 1996 (Act No. 43 of 1996).

CHAPTER 5

INFORMATION WHICH REQUIRES PROTECTION AGAINST DISCLOSURE

Part A

Sensitive Information

National interest of Republic

11. (1) The national interest of the Republic includes, but is not limited to—
- (a) all matters relating to the advancement of the public good; and
 - (b) all matters relating to the protection and preservation of all things owned or maintained—
—for the public by the State.
- (2) The national interest is multi-faceted and includes—
- (a) the survival and security of the State and the people of South Africa; and
 - (b) the pursuit of justice, democracy, economic growth, free trade, a stable monetary system and sound international relations.
- (3) Matters in the national interest include—
- (a) security from all forms of crime;
 - (b) protection against attacks or incursions on the Republic or acts of foreign interference;
 - (c) defence and security plans and operations;
 - (d) details of criminal investigations and police and law enforcement methods;
 - (e) significant political and economic relations with international organisations and foreign governments;
 - (f) economic, scientific or technological matters vital to the Republic's stability, security, integrity and development; and
 - (g) all matters that are subject to mandatory protection in terms of sections 34 to 42 of the Promotion of Access to Information Act, whether in classified form or not.
- (4) The determination of what is in the national interest of the Republic must at all times

be-