LAW SOCIETY
OF SOUTH AFRICA

Information Security Guidelines for Law Firms

Drafted for the
Law Society of South Africa
by Mark Heyink

Information Security for South African Law Firms

LSSA Guidelines

VERSION 1.0

MARK HEYINK

Attorney, Notary & Conveyancer
Specialising in Information Law

Foreword

Please read this Foreword carefully.

This guideline has been compiled as a tool to assist attorneys in South Africa in understanding their information security obligations.

The guideline is not intended and must not be construed as establishing any legal obligation. Each practice is different and will have to apply the principles which have been developed to safeguard information as may be appropriate and in accordance with the nature of the information and of the firm. Neither is the guideline intended, nor must it be construed, as providing legal advice.

While guidelines to the implementation of information security practice have been developed which may differ from one another in form and emphasis, according to the profession or industry for which these standards have been developed, all credible information security practices are based on the principles which have been established and are documented in the ISO Standards. Three ISO Standards will be referred to in this guideline (ISO27001, ISO27002 and ISO27003). Two of the Standards have been accepted as South African Standards SANS27001 and SANS27002. ISO27003 was published in February 2010 and has not yet been adopted by the South African Bureau of Standards as a South African National Standard. These standards are sufficient to provide guidelines and a framework for the information security required by South African attorneys. There are additional guidelines which may assist attorneys in specific issues, for example record retention, ITC governance and digitisation of records.

Copyright

Chapter 1

1. INTRODUCTION

1.1 Attorneys are knowledge workers and information is the lifeblood of any attorney's practice. Not only does information assist the attorney in providing expert services to clients, but attorneys also have significant amounts of client information entrusted into their custody. The appropriate security of an attorney's information and that of the attorney's clients is simply good business practice and as importantly, the failure to safeguard information properly may also have legal consequences.

1.2 Over centuries, while information was predominantly in paper and text, the measures necessary to properly protect this information were well established and these are understood by practitioners and their staff. However, the information revolution has dramatically and exponentially increased the electronic processing and communication of information. It is trite that in most modern practices, despite the necessity to print some of the information in paper and text form, by far the preponderance of information is processed and communicated electronically.

1.3 The processing of information and communications electronically necessitates careful reconsideration of what attorneys must do to discharge their information security duties properly as the safeguards that apply to information in paper and text are simply not appropriate to information in electronic form. This is not to say that the safeguards relevant to information in paper and text are redundant. The discipline of information security encompasses all information in whatever form or media and therefore they remain an important component of the overall information security of a firm.

1.4 As has been pointed out by Judge Mervyn King:

> *"Willingly or unwillingly we are members of the information age. The ultimate light in regard to transparency and governance has become information technology. The use of IT in the business world is not only an enabler but has also become of strategic importance. Through this strategic role it has become pervasive."*[1]

The proper governance of information on which our practices are dependent is an undeniable obligation of every attorney.

1.5 At this time there is no research available as to how South African law firms safeguard information owned by or under their control. While some practices have embraced technology, many others fall into the category of "unwilling" participants alluded to by Judge King and have been slow to implement appropriate information management and security. Based on the writer's personal experience and interaction with law firms, their understanding of information security is poor. Even among those more progressive firms that have invested heavily in technology (some of these among our larger firms) information security is not high on most attorney's agenda.

[1] The Corporate Citizen: IT Governance Page 74

1.6 It is hoped that this guideline will assist practitioners in understanding what information security seeks to achieve, why it is important for attorneys to safeguard their own and their clients' information, who is responsible for information security and how an Information Security Management System ("ISMS") may be implemented. Finally, and most importantly, it is hoped that this will assist attorneys in deriving the enormous benefits that good information governance, management and security will yield in their practices.

Chapter 2

2. WHAT IS INFORMATION SECURITY?

The aim of this chapter is to assist the reader in understanding:

- What information security seeks to achieve; and
- The elements inherent in processing of information (technology, process and people) that need to be addressed to achieve appropriate information security.

2.1 The discipline of Information Security aims to protect the:

- **Confidentiality** of information, by ensuring that information is accessible only to those authorised to have access to the information;
- **Integrity** of information, by safeguarding the accuracy and completeness of information; and
- **Availability** of information, by ensuring that authorised users have access to information and information systems required to process information, as and when needed.

2.2 In order to establish an Information Security Management System ("ISMS") it is critical that an organisation addresses three primary components that are present in the processing of information. The three components are technology, process and people. Unless all three are addressed properly it is unlikely (probably impossible) that a credible ISMS may be established and maintained.

Technology

2.3 In our modern world, even in practices that do not have sophisticated networks or technologies, we still process significant amounts of information electronically. Stand alone computers, digital fax processors, digital copiers and of course cellphones process and store information electronically. Thus, even in practices which may not consider themselves technologically sophisticated or dependent upon networked information, information security is important. The nature of the technology used and the firm's dependency on the technology will determine the emphasis on the different control measures that may need to be implemented.

2.4 In addition to the technologies that we use to process information, there are many sophisticated technologies which may assist practices in enhancing their information security. Anti-virus software, intrusion detection devices and automatic backup applications are some examples of technologies which are of enormous assistance in structuring information security management. However, the danger of relying solely on the technology intended to enhance information security and believing that technology is the "silver bullet" to information security, is a fundamental error. It is nonetheless an error that is regularly repeated.

Process

2.5 The management of information and of information security is impossible without properly determined and documented processes. Unless there are clear processes relating to the generation, processing, communication and retention of information, the goals of confidentiality, integrity and availability of information will not be achieved.

2.6 The documentation of these processes is typically in the form of policies, supported by procedures and standards, all of which should be mandatory, and sometimes guidelines, which may not be mandatory but provide valuable assistance to users of information and information systems. Policy development is dealt with in more detail in Chapter 7 of this guideline.

2.7 In South Africa attorneys are still required in many context's to prepare documentation in paper and text form. South African institutions and administrative bodies with which attorneys interact on a daily basis (courts, Deeds Office, Master's Office, CIPRO) still typically require information to be presented in paper and text form. Therefore, the importance of managing and appropriately securing information in electronic form to ensure consistency with information printed on paper remains a vital aspect of information management and security for practitioners.

People

2.8 As attorneys are knowledge workers dependent on the integrity of the information they use, it is highly lamentable that the organised profession and our educational institutions have paid little attention to educating attorneys and law students in the importance of modern information and communications technologies, information management and information security. In view of this it is not surprising that typically practitioners and their staff lack adequate understanding of accepted information management and information security practice. The result of this is that consistently and persistently attorneys breach one of their fundamental duties in not ensuring that client information is safeguarded in a manner that protects its confidentiality. This is a duty (which also underpins the client's right to legal privilege) fundamental to the practice of law.

2.9 It is important that attorneys recognise their responsibility to establish and maintain appropriate information security, understand their governance duties in this regard, ensure that managers responsible for information systems are educated in their information management and security responsibilities and that users of the information systems under the attorney's control are educated in their information management and security responsibilities.

2.10 Education is a key element of all Information Security initiatives. Education must be tailored to suit the particular practice and that it is ongoing and sustainable. Threats to the safety of information change literally on a daily basis and the education required to combat these threats must be ongoing.

Chapter 3

3. WHY IS INFORMATION SECURITY IMPORTANT?

The aim of this chapter is to draw attention to:

- The attorney's professional duty to implement information security;
- The expanding legal obligation of information security;
- Recent legislation and regulation mandating the obligation to provide information security; and
- The good business sense of implementing information security.

Professional Duty

3.1 Before exploring the general obligations that have developed relating to information security, it is useful to examine the professional duty of an attorney to provide appropriate safeguards in protecting the confidentiality of his or her clients' information.

3.2 The International Code of Ethics governing the behaviour of attorneys provides that:

> *"Lawyers should never disclose, unless lawfully ordered to do so by the courts or as required by statute, what has been communicated to them in their capacity as lawyers, even after they have ceased to be the client's counsel. This duty extends to their partners, to junior lawyers assisting them and to their employees."*

3.3 This duty of confidentiality is echoed in rules governing attorneys' conduct in jurisdictions around the world and in South Africa.[2]

3.4 As has been indicated earlier in this Guideline, practices underlying the maintenance of confidentiality in electronic records and communications are vastly different to the practices which we have employed in the paper and text environment. It is interesting to note that the Canadian Bar Association guidelines for "Practicing Ethically with New Information Technology", a supplement to its "Code of Professional Conduct", makes the following comment:

> *"To meet the ethical obligation for competence in Rule 2 (perform any legal services undertaken on a client's behalf competently) lawyers must be able to recognise when the use of technology may be necessary to perform a legal service on that client's behalf and must use the technology responsibly and ethically.*
>
> *Lawyers must satisfy this duty by personally having a reasonable understanding of the technology and using it, or by seeking assistance from others who have the necessary proficiency."*

[2] Examples: In England and Wales the Solicitors Code of Conduct, published in 2007, provides that solicitors must keep affairs of clients and former clients confidential except when disclosure is required or permitted by law or by clients. A provision very similar to the international code of ethics is contained in Section 14 of that schedule of the rules of the KZN Law Society.

3.5 It is submitted that while there is no formal equivalent of the Canadian Bar Association's guideline in South Africa, attorneys are required to act reasonably and diligently in fulfilling their professional obligations. One of these obligations must be that in using modern technology they do not compromise the rights of their clients arising from the attorney/client relationship.

Information Security Obligation

3.6 Over recent years there has been an expansion of the obligations of entities holding information in electronic form to implement reasonable, organisational, physical and technical measures to safeguard information under its control. Even in the absence of legislation or case law obliging holders of information to safeguard their information, persons responsible for the governance or management of an organisation have a duty of care to the stakeholders of the organisation and to third parties on whose behalf they may hold information, to ensure that they exercise due diligence in properly safeguarding the information.[3]

Statutory Obligations to Provide Information Security

3.7 While it is beyond the scope of this Guideline and unnecessary to deal with all legislation which either expressly or impliedly requires the implementation of information security, it is useful to highlight recent legislative developments which address this responsibility.

3.8 The new **Companies Act** specifically mandates that a director must perform the functions of a director with a degree of care, skill and diligence that may be reasonably expected of the director and having the general knowledge, skill and experience of the director.[4] In exercising the necessary degree of care, skill and diligence relating to the use of information and communications technology, directors should take heed of the provisions of the **King III Code of Governance Principles for South Africa**. These specifically define the obligations of directors relating to IT Governance and expressly address the obligation to implement information security.[5]

3.9 Even in instances where attorneys may not be directors of incorporated practices (or perhaps hold directorships in companies subject to King III) they would do well to read and understand what is entailed in exercising proper information and communications technology governance.

3.10 The **Protection of Personal Information Bill** expressly requires in addressing Security Safeguards as a condition of lawful processing of personal information that:

> *"18.(1) A responsible party must secure the integrity of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent -*

[3] Information Security Law – Thomas J Smedinghof October 2005 (www.bakernet.com)

[4] Section 76(3) of the Companies Act, No. 71 of 2008

[5] King Report on Governance Principles for South Africa 2009. Principle 5.6 expressly requires that information assets are managed effectively. Principle 5.35.1 includes in management of information assets the protection of information. Principle 5.4 requires that an ISMS is implemented in an appropriate and applicable information security framework.

(a) loss of, or damage to, or unauthorised destruction of personal information; and

(b) unlawful access to or processing of personal information.

(2) In order to give effect to subsection (1) the responsible party must take reasonable measures to -

(a) identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;

(b) establish and maintain appropriate safeguards against the risk identified;

(c) regularly verify that the safeguards are effectively implemented; and

(d) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

(3) The responsible party must have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations."

Once the Bill is enacted this will be the first instance in South African law that there is an express statutory stipulation for the implementation of information security to protect information.

3.11 While information security is not an express requirement of certain legislation it is nonetheless a critical element in being able to comply with certain of the provisions. For instance **Chapter III of the Electronic Communication and Transactions Act** (which provides for the facilitation of electronic communications and transactions), the **Promotion of Access to Information Act**, the **Consumer Protection Act**, and the **National Credit Act**. It is simply inconceivable how the requirements of information management and safeguarding the confidentiality of information in terms of these acts can be achieved without appropriate information security.

3.12 An information management and security obligation imposed on most persons, whether natural or juristic, is that of **record retention**. The obligation to retain records is provided for in a significant number of instruments of legislation and regulation in South Africa. Implicit in this obligation to retain records is the necessity that records remain accurate during their retention. In the case of paper and text we have tried and tested mechanisms to ensure that records are not tampered with. However, in dealing with the retention of electronic records most attorneys firms have not developed proper protections to ensure the integrity of these records. This is a failure that needs to be addressed by many attorneys in order to fulfil their obligations to retain records properly.

Security Laws

3.13 As countries and the international community become more dependent on the Internet and other electronic communications infrastructure, governments are increasingly enacting laws aimed at securing the infrastructure and imposing general obligations to implement

appropriate information security. Not only is this occurring at national level but there is an increasing move to internationally ensure that the safety of the Internet is not compromised.

3.14 In South Africa the Minister of Communications gave notice on the 19th February 2010 of the intention to develop the South African National Cyber Security Policy[6]. This is in line with international developments.

Good Business Practice and Common Sense

3.15 The information security standards and practices that have been developed globally have at their core good business practice in the processing of information. While, as with any form of security, there may be an overhead in implementing and practising information security, the implementation of information security generally highlights deficiencies in information management which are extremely costly to many businesses. One of the recognised dividends of an investment in information security is the streamlining of business practices to unlock the benefits held in electronic processing and communication of information as opposed to merely using the technology as a mechanism of perpetuating old information management methodologies more appropriate to paper and text.

3.16 Aside from the motivation of Good Business Practice it is important in any business to assess the potential risk of liability in its actions or omissions. Given the duty of attorneys to safeguard the information that they use, including the information of their clients, it makes good business sense to assess these risks and determine what controls are appropriate to the management of the risks.

3.17 Attorneys should also note that the provisions of Chapter 6 of King III expressly require compliance with the law and consideration with the adherence of non-binding rules, codes and standards.[7] In the context of information security the ISO Standards referred to in this guideline are examples of non-binding codes and standards that should be adhered to in establishing appropriate information security.

Contractual Obligation

3.18 The draft Protection of Personal Information legislation requires responsible parties, where they appoint operators to process information, to enter into written agreements with the operators obliging operators to ensure that they safeguard personal information appropriately in terms of Generally Accepted Information Security Practice.

3.19 This requirement will necessitate that many of the larger institutions, from which South African attorneys source their work, enter into the written agreements required by the legislation. In this regard at least one major South African institution has already required attorneys to provide information to it as to their information security and protection of personal information status. There are several more who are in the process of planning similar interventions.

[6] Government Gazette No. 32963 dated 19 February 2010

[7] King Report on Governance for South Africa 2009 (Principle 6.1)

3.20 In the future, a failure to comply with the obligation to safeguard personal information and to enter into the written agreements required, may disqualify an attorney from receiving work.

Chapter 4

4. WHO IS RESPONSIBLE FOR INFORMATION SECURITY?

The aim of this chapter is to provide the reader:

- With a background to information and communications technology governance as it applies to an attorneys practice;
- Reference to new legislative and regulatory instruments regulating ICT Governance; and
- Practical guidelines relating to the delegation of information management and security responsibilities.

Background

4.1 As has already been stated, attorneys and their staff are knowledge workers and accurate information is the lifeblood of an attorneys practice.

4.2 Writing in "Management Challenges for the 21st Century", Peter Drukker stated:

> *"The diffusion of technology and the co-modification of information transforms the role of information into a resource equal in importance to the traditionally important resources of land, labour and capital."*[8]

4.3 Given the importance of information to an attorney's practice where (as a resource) information has always been at least as important as labour and capital, the importance of proper governance of information and the information and communications technologies used to process information cannot be underestimated.

4.4 This is recognised in more general terms in the new Companies Act (No. 71 of 2008), the King III Report (effective from the 1st March 2010) and the Protection of Personal Information Bill (currently before Parliament), which bring with them significant change to the ICT Governance landscape in South Africa.

New Legislation and Regulation

4.5 The reshaping of governance obligations in the legislation and regulation referred to acknowledges that to achieve effective and sustainable information management and security in today's complex interconnected world that governance (as the word implies) has to be exercised at the highest levels of an organisation and not relegated, as a technical speciality, to the IT department. King III expressly stipulates that the board of directors is responsible for information technology governance. The board may delegate the management of information and of information technologies to management. However, this delegation must be appropriate and must not be an abdication of the responsibility of governance.

[8] Peter Drukker "Management Challenges for the 21st Century"

4.6 Management, in terms of its mandate from the board, will in most cases become response for the implementation of structures, processes and mechanisms to execute its tasks within the IT governance framework.[9]

4.7 King III also expressly requires boards and management to distinguish between the governance of information from the governance of information technology.[10] While IT plays a critical role in providing appropriate technologies and support in managing information appropriately, the responsibility for assessing and establishing the appropriate controls of access to information and the security safeguards for the information, remains with the owner, or the person responsible, for the information and is not an IT responsibility.

4.8 For those legal practices that are incorporated, the obligations of the Companies Act, informed as they are by King III, may be of immediate application. For those that are not, the distinction between the governance of information and the governance of information technology dealt with in King III should resonate loudly when the responsibilities set out in Chapter 3 of this guideline are considered. It is simply not acceptable in dealing with the practice's information and that of its clients that decisions in this regard be delegated to persons responsible for IT (in many cases to third parties who provide technical IT assistance) who have no understanding of the attorney's responsibilities to safeguard information or the importance of the information to the practice.

4.9 It should be noted that the Protection of Personal Information Bill and in the Promotion of Access to Information Act (in the case of private bodies) stipulate that the head of the private body is, absent a delegation of the responsibility to an information officer, responsible for the obligations of the private body in terms of the Bill and the Act respectively. Where the head of a private body delegates this duty the person discharging the responsibility must know and understand what his/her obligations are. The proper delegation (and not abdication) of information security and management is key to discharging this obligation.

Responsibilities

4.10 While it is appreciated that it is difficult for busy practitioners in small practices to do everything that is required to safeguard information properly, the obligations that attorneys owe to their clients demand that they apply their minds to safeguarding of information in the practice and ensure that proper oversight is established and maintained on an ongoing basis. Whatever the size or nature of the practice it is the responsibility of attorneys who control the operation of the practice, or have been designated by their colleagues to fulfil this executive role, to ensure that the appropriate information security framework and mechanisms are established and maintained.

4.11 Unless users of information systems and information are educated in their information security responsibilities and made aware of information security risks they cannot perform this important function and will themselves become a significant information security risk.

[9] King III paragraph 5.1.1 and paragraph 5.3.15

[10] 5.1.7 King III Code of Governance Principles

Chapter 5

5. WHEN IS IT APPROPRIATE TO IMPLEMENT INFORMATION SECURITY?

The aim of this chapter is to persuade the reader:

- That information security is an immediate requirement;
- Information security is an ongoing process which must become a core competency within the organisation; and
- Each day without information security, places the organisation at risk.

5.1 Some 40 years ago Alvin Toffler observed that "information is the currency of the future". The future that Toffler predicted has rushed to meet us, and we are now in a time where indeed information has increased exponentially in value. Unfortunately, most people, while embracing the benefits of the information economy, have done little to evaluate the risks that new mechanisms of processing information has heralded. Among these are the facts that because of its increased value, information has become increasingly subject to abuse and theft.

5.2 In view of the reasons provided for implementation of information security in Chapter 3, not least of which are the professional duties of attorneys, the implementation of information security is overdue. Attorneys who have not already done so owe it to their clients and to their business to immediately take steps to implement appropriate information security.

5.3 It must be recognised that information security is an ongoing and continuous process. Technology, the application of technology and threats change constantly and the need to monitor, review and improve information security is an intrinsic characteristic of the discipline.

5.4 There are many examples of how the information revolution has enhanced the value of information. It is generally recognised that more than ever before information generally and personal information in particular are the subject of improper uses and because of its enhanced value, of theft.

5.5 From the perspective of information held by an attorney, not only may the information have commercial value but in many circumstances the information is of particular value to clients and clients rely on the confidentiality obligations of attorneys as well as the attorney and client privilege (where appropriate and applicable) in protecting their information. To believe that this information might not be of value to third parties and susceptible to information security threats is pure folly.

5.6 As has been indicated earlier, with legislation protecting personal information likely to be enacted in the foreseeable future, those practices who do not create the core competencies within their organisation to deal with information security on a continuous and ongoing basis will become disadvantaged and find that certain clients will be reluctant to do business with

them. Those practices that take information security seriously and can demonstrate an inherent ability to protect information (particularly personal information) properly will gain an important advantage in the market place.

Chapter 6

6. HOW TO IMPLEMENT INFORMATION SECURITY?

The aim of this chapter is to provide the reader with a basic understanding of:

- What an Information Security Management System is;
- The steps to take in implementing an Information Security Management System;
- How to maintain an Information Security Management System

Introduction

6.1 An Information Security Management System ("ISMS") is an integrated part of the overall management of a business, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security.[11]

6.2 The establishment of an ISMS and the nature of the ISMS will vary according to what may be appropriate to a particular practice. There are many diverse and complex characteristics that will influence the shape and nature of each individual ISMS. Thus there is no silver bullet or one-size-fits-all example that can be applied, however, the following structured approach will hopefully assist attorneys, however large or small their practices, in understanding how to go about establishing an appropriate ISMS.

6.3 This guideline is intended as a starting point and is not exhaustive. If more detail is required attorneys are referred to ISO27001-2005 and ISO27003-2010.

Core Competency

6.4 Information security is not something that can be purchased or outsourced. Certain functions relating to the processing of information may be outsourced, for instance the provision of IT and communications services, retention of backup media, or even the storage and destruction of dead-files (all elements of processing information). Ultimately the establishment, maintenance and ongoing review of information security is the responsibility of each practice. With regard to an attorney, because of the professional duty owed to clients, it is incumbent on an attorney to ensure that the firm within which he or she practices implements appropriate information security.

6.5 While reliance on experts in the field of information security may be necessary (perhaps essential) for the purposes of establishing an ISMS and to deal with extraordinary information security issues and incidents, attorneys should not rely on third parties to maintain and improve information security in their practices. The discipline of information security should become a core competency in all attorney's practices.

[11] Definition of Information Security Management System : Paragraph 3.7 ISO27001-2004

Initiation of an Information Security Management System

6.6 The first step is to identify and assign to a person/s who has/have the appropriate authority the responsibility for gathering the necessary information to define and plan what is necessary for the establishment of an ISMS in a particular practice. The importance of assigning appropriate authority to this person and ensuring that all persons within the practice recognise this authority is critical to the success of the investigation and initiation of an ISMS.

6.7 The objective of this investigation is to obtain approval at the highest level of the organisation for the establishment of an ISMS.

6.8 In conducting the investigation the following issues should be addressed (this list is not exhaustive but provides a good starting point):

- What are the critical business objectives of the practice?
- What organisational or support areas (eg. IT, HR, financial) allow the critical business of the practice to be conducted?
- What client relationships and agreements exist?
- What third party support relationships and agreements exist?
- What information is critical to the practice and its business?
- What are the consequences of a compromise of this information?
- What law is the practice required to comply with?
- What agreements are or may be required by clients or other third parties?
- What are the practice's professional obligations?
- What are the threats to information?
- What are the different categories of information that require protection?
- What are the minimum market requirements for information security?
- What information security controls would provide a competitive advantage for the practice?
- For how long can the practice tolerate interruption to its critical business processes?

6.9 Against this background the persons assigned the responsibility of this investigation should prepare a document outlining the characteristics of the practice, its management organisation, its location/s, the technologies employed by the practice and a high level list of its information assets (information and information and communications technologies).

6.10 The document should summarise the business objectives of the practice, how information security will benefit these objectives, what resources there are to properly organise an ISMS and identify or recommend priorities (by way of information or business elements within the practice) for the implementation of information security.

6.11 The document should also discuss the professional, statutory and regulatory and contractual obligations of the practice.

6.12 This will allow the development of a preliminary ISMS scope and a definition of roles and responsibilities within that scope. It will inform the documentation of a business case and a plan for the implementation of an ISMS for approval by the directors, partners or executive committee, as the case may be.

6.13 In smaller practices, particularly where persons conducting the investigation will be part of the approval process, some of the high level investigation described above may be conducted in more detail in these initial stages. In larger practices it is suggested that this initial high level investigation and the approval of decision-makers within the organisation is obtained to ensure that appropriate authority for more detailed work is obtained before embarking on a detailed definition of the ISMS scope, boundaries and policy.

Defining ISMS Scope, Boundaries and ISMS Policy

6.14 This step contemplates defining how information security is to be organised, which may include the establishment of an information security committee (where the size of the practice makes this appropriate), defining the information security roles and responsibilities within the practice, and establishing a hierarchy for decision-making within the information security management system.

6.15 It is also necessary to define information and communications technologies employed by the practice as well as how and by whom the hardware, network and software comprising these technologies is controlled.

6.16 The physical scope ie. premises, locations or facilities of the practice which should be governed by the ISMS must be defined. It is important to include in this consideration not only technology but for instance the warehousing of paper-based information such as deadfiling and procedures for the retrieval of deadfiles.

6.17 With these investigations complete, the findings should be integrated, which will allow for the development of an ISMS policy for approval by the practice's decision-makers. This policy should be a relatively brief document which, at a minimum:

- Establishes the information security objectives and the ISMS objectives of the practice;
- Provides focus to the practice to achieve the information security objectives;
- Identifies the practice's legal obligations (statutory and contractual) to provide information security;
- Indicates how risk is identified, evaluated and managed within the practice.

6.18 Once the ISMS policy has been approved by the practice's decision-makers the framework defining the boundaries of the ISMS and roles and responsibilities, a framework for the investigation of information security requirements, the implementation of controls and the ongoing monitoring and review of information security can commence.

6.19 A draft copy of an ISMS policy which may be adopted by attorneys and/or executive committees within practices is provided as A to this Chapter.

Defining Information Security Requirements

6.20 With the organisation infrastructure in place, the next step is to identify the:

- Processes, information systems and communication networks within the practice;
- Information assets of the organisation;
- Critical processes;
- Information security obligations;
- Identification of key information security policies, procedures and standards to be developed;
- Information security training and education requirements of the practice

Conduct an Information Security Assessment

6.21 The assessment should be aimed at comparing the status of information security of the practice to the desired objectives of the practice relating to information security. It is advisable, in looking at specific areas within the practice, that participants in the processing of information in those areas are included in the assessment.

Risk Assessment

6.22 Generally accepted information security practice and jurisprudence developing in this area indicate that in addressing information security a thorough assessment of the potential risk to the organisation's information and its information systems should be made. Only once the risk is understood can appropriate safeguards be implemented.

6.23 There are many risk management methodologies and in the case of larger practices more complex risk management methodologies may be required. However, there are certain fairly straight forward methodologies that may be used and indeed have been used by attorneys in the past. With regard to paper and text we typically keep sensitive information (original documents, confidential documents and documents which may have extrinsic monetary value) in fireproof safes, housed in strong rooms. Not all information is safeguarded to this extent, so somewhere along the line a risk assessment has been made relating to what information should be kept in the fireproof safe in the strong room. Similar principles will need to be applied to the retention of electronic information.

6.24 The simple principles which need to be applied in assessing risk are:

- Identifying potential threats to information;
- Considering the likelihood that the threat will materialise;
- Evaluating the potential damage that would occur if the threat materialises;
- Assessing the adequacy of the safeguards (technical, procedural and knowledge based) which safeguard against the threat materialising.

6.25 Guidance as to risk management which may be applied to information security can be obtained from ISO27005.

Security Measures

6.26 Once the information assets have been identified and a risk assessment concluded it is necessary to determine what controls are appropriate to treat the risk.

6.27 If it is established that the risk is remote or the consequences of the risk being realised of low impact, the practice may decide to accept the risk without implementing any control measures.

6.28 In certain instances it may be decided that the risk can be transferred (insured against or the liability transferred to a third party by agreement).

6.29 If it is determined that the risk needs to be controlled, appropriate control measures need to be established. In some instances the threats will be capable of being controlled by the implementation of appropriate technologies, but care must be taken to ensure that processes relating to the use of these technologies are established, and where necessary people using the technologies are properly trained in their use. It must be borne in mind that in themselves technologies, while very useful tools, do not without the framework of appropriate process and training of people in the process establish appropriate security.

6.30 In this regard reference to ISO27002 is very useful. This document is titled "Information Technology – Security Techniques – Code of Practice for Information Security Management". This Standard provides a framework and describes 11 different categories, the control objectives that are necessary in respect of each category and one or more controls that may be applied to achieve the control objective.

6.31 These categories are:

- Security Policy;
- Organising information security;
- Asset Management;
- Human resources security;
- Physical and environmental security;
- Communications and operations management;
- Access control;
- Information systems acquisition, development and maintenance;
- Information security incident management;
- Business continuity management;
- Compliance.

6.32 These controls are fully explored in Chapter 7 of this guideline.

Information Security Management System Policy (Framework)

6.33 Once the initial investigation has been undertaken a policy or a framework for the establishment of an ISMS should be documented. This should address the nature of the practice (different services provided by the practice), the organisation of the practice,

physical location, its information management and technologies used in information management and a broad categorisation of the information processed by the practice.

6.34 This policy or framework will provide parameters for setting objectives and establishing an overall sense of direction for the establishment of information security disciplines within the practice.

6.35 It should also indicate how the risk of different categories of information will be evaluated to enable what safeguards are required for information processed by the practice. This should include consideration of the contractual or regulatory requirements which the practice is obliged to fulfil.

6.36 Even with larger practices, this policy or framework which defines the establishment of the ISMS should be brief and in time will be replaced by more comprehensive policies, procedures and standards.

6.37 The document should also expressly include information and technologies or facilities that would not be subject to the ISMS and provide reasons for this.

6.38 Once completed the ISMS defining the scope and boundaries of information management of the practice should be provided to the directors, partners or executive committee of the practice, as the case may be, for approval.

The establishment of the organisational infrastructure for information security

6.39 In smaller firms this function can be carried out by one person. However, in larger firms it will be necessary and it is recommended that an information security committee be established. This should comprise of persons responsible for:

- The main business divisions within the practice;
- Human resource;
- Compliance;
- Training;
- Communication;
- Information technology;
- Physical security;
- Any other element within the organisation that may provide input or be responsible for information security (eg. Record retention, deadfiling, eMail archiving, etc.).

6.40 These persons will be responsible for the initial planning of the implementation of an ISMS and thereafter for its oversight.

6.41 In some instances with larger firms it will be appropriate to appoint an information security officer who will attend to the day-to-day responsibilities relating to information security. It is suggested that the person appointed to the role of information security officer may also fulfil the roles of information officer as contemplated in the Protection of Personal Information Bill (once enacted) and in the Promotion of Access to Information Act.

6.42 In smaller firms it may be that the role of information security officer becomes an extension of the statutory appointment of information officer in terms of the Protection of Personal Information Bill (once enacted) and the Promotion of Access to Information Act. Once established, the person/s who fulfil the information security roles need to consider the following issues.

6.43 The scope of the information security effort needs to be defined.

- What information needs to be protected?
- What information and communication systems are used to process and communicate information?
- Where are they located?
- Are these systems internally supported or is reliance placed on external third parties?
- What laws will the firm have to comply with?
- What agreements exist with service providers?

6.44 Some of this information will probably already be available from the ISMS policy or framework and may form the foundation for more in-depth investigation.

6.45 Once the organisational framework within which information security is to be governed and managed has been documented the next step is to consider appropriate controls for information security appropriate to the practice. This is dealt with in Chapter 7.

Chapter 7

7. INFORMATION SECURITY CONTROLS

The aim of this chapter is to:

- highlight information security controls that need to be implemented as part of the ISMS; and
- approaches to the implementation of the controls.

General

7.1 Having established the organisational framework for an ISMS, the next task is to determine what information security controls are necessary.

7.2 This chapter is not an exhaustive exposition of the controls that may be required and implemented, but summarises some of the more important controls which may need to be considered by attorneys in addressing information security.

7.3 The Standard ISO27002:2005 titled "Information Technology – Security Techniques – Code of Practice for Information Security Management" provides a comprehensive guideline to information security controls which may need to be considered. While the controls discussed in this Chapter provide a starting point for information security establishment and implementation, attorneys may also wish to consider the provisions of this Standard.

Statement of Applicability

7.4 In determining which controls are appropriate it is recommended that a "Statement of Applicability" be prepared.[12] This statement correlates information security objectives and controls selected. It must also provide a reason for the selection of the controls.

7.5 To the extent that controls are not necessary, their exclusion and a justification for their exclusion should also be provided. An example of a Statement of Applicability is provided as Appendix A to this chapter.

7.6 The King III report is based on the principle that its recommendations must be applied or an explanation provided where non-applicable. The principles underlying the Statement of Applicability reflect this. Thus, in establishing a Statement of Applicability, the principles in King III in so far as they relate to information security will be complied with.

7.7 Generally Accepted Information Security Practice requires continuous and ongoing reviews of the management of information, information technologies and information security controls that are applied. The Statement of Applicability should also be reviewed and may be used as an important tool in the review process itself.

Information Security Policies

[12] Paragraph 4.2.1(j) ISO27001:2005

7.8 The objective of information security policies is that they provide management direction and support for the information security function in accordance with the professional duties, business requirements and relevant laws and regulations governing an attorney's practice.

7.9 A major failure of information security policies are that they are far too lengthy. Further, that they address issues which apply to a limited number of persons within an organisation and are irrelevant to the majority of the readers. It is recommended that information security policies are not addressed in a single omnibus policy but that they are carefully divided to address specific information security issues and that only the persons responsible for particular information security interventions need read and understand that policy. A brief guideline addressing policy development is provided as Appendix B to this chapter.

Policy Structure

7.10 **Policies** are high level statements of intent that stipulate the information security objective and controls which are to be implemented. The policies should also address the consequences of a breach, including but not limited to, remedial actions that may be necessary and disciplinary procedures against persons responsible for the breach.

7.11 **Procedures** are set out step-by-step specifics of how the policy and the supporting standards will actually be implemented in an operating environment.

7.12 **Standards** are mandatory activities, actions, rules or regulation designed to provide policies with the support structure and specific direction they require to be meaningful and effective. A standard usually defines a specific product or mechanism that it selected for universal use throughout a practice in order to support the policy objectives. Among the tools used in achieving information security objectives are Standard Agreements.

7.13 **Guidelines** are discretionary recommendations to be followed by managers and users of information. While policies, procedures and standards are mandatory, guidelines are not and they will often be in the form of documentation addressing awareness and education programmes.

7.14 The importance of documenting policies, procedures and standards cannot be underestimated in the overall implementation and maintenance of information security within a practice. They should provide clear evidence of governance requirements and the intent of the owners of the practice relating to information security. They should define general and specific responsibilities for the management of information, the safeguards relating to the information and the protection of personal information.

7.15 Generally Accepted Information Security Practice requires that information security policies are regularly reviewed and where necessary that they are amended to accommodate changes in the information environment, new threats to the security of information and changes in the business application of information.

7.16 Policies are the most important tools in changing the culture of an organisation. However, they will only be successful if there is demonstrable management commitment to the policies being implemented, maintained and reviewed. Further, in the event of breaches of the policies, that appropriate remedial measures are taken by management and that

perpetrators of breaches are appropriately disciplined. Failure to provide this commitment will inevitably lead to a failure of any information security initiative.

Organisation of Information Security

7.17 The objective of having a clear organisational infrastructure is to ensure that information is securely and properly managed within a practice.

7.18 Some of the issues of establishing an information security structure have been dealt with in the previous chapter which addresses initiating an ISMS. An ISMS should provide a management framework which will determine and approve information security policies, assign roles and coordinate the review of security throughout the practice. As previously stated, the framework may vary from practice to practice but the underlying principle that must be observed is that information management and security should become a core competency within the practice.

7.19 While the skills necessary to exercise information management and security should be developed and encouraged within a practice, it may be necessary initially for practices to obtain specialist advice or assistance. However, this should be viewed as an interim measure until these core competencies are developed.

7.20 Among the controls that establishing an ISMS should provide is that management's commitment to information security is demonstrated, information security is coordinated and information security responsibility properly defined.

7.21 **Confidentiality agreements** are one of the tools necessary to manage information within an organisation. While at first blush this may seem simple for attorneys, in many instances careful consideration needs to be given to the nature of the confidentiality agreement and how they address the processing of information within a practice. It needs to be borne in mind that because we manage, use and apply information differently by using electronic technologies, some of the protections afforded by traditional confidentiality agreements have been lost. The "cut and paste" mentality afforded to these "standard clauses" must be avoided and proper consideration to the protection required provided. In this regard it may be helpful to replace confidentiality agreements with information security agreements which incorporate confidentiality clauses.

7.22 In the case of employees information security clauses should form part of employment agreements. In the case of third parties who may have access to information owned by or under the control of the practice, they should be subject to information security agreements.

7.23 **External Parties** may have access to an attorney's information processing facilities and information processed by an attorney. The information security of an attorney's practice should not be compromised in any way by providing access to external parties.

7.24 It is important in allowing external parties access to premises, information systems or information, that the access is properly controlled and the external party is subject to express requirements and prohibitions as a condition of the grant of such access.

7.25 Many information security compromises arise from access which is authorised but not controlled. There are an abundance of recorded cases of external cleaners and maintenance personnel stealing information (in many instances at the behest of third parties), access to which is made easier through their physical presence.

7.26 While in some instances physical access allows the opportunity to steal information, in our interconnected information economy the problem is exacerbate considerably by a necessity to allow third parties access (logical or electronic) to information systems and information.

7.27 In all instances whether physical or logical access to information is granted to third parties, the access should be subject to appropriate controls and should not be granted prior to the third parties signing information security agreements.

7.28 It must also be noted that the remedies available against employees will not necessarily apply to third parties. Therefore remedies flowing from a breach of information security obligations may include immediate removal from physical premises, immediate revocation of access to networks or databases, the immediate return of or destruction of information in the possession of third parties (including information which may be contained in backups held by the third party) and cancellation of agreements need to be considered.

Information Asset Management

7.29 In order to control and secure information assets it is critical that the assets are identified and that a person is assigned the responsibility for the management and security of the information asset. In information security speak this person is called an "information owner".

7.30 Information assets are not confined to technologies that process information. They include all information in whatever media. King III specifically requires the governance and management of information as well as the governance of technology.[13]

7.31 Turning to information systems: Due to the pervasive and increasing use of mobile computer devices and media it is important to address their acceptable use within the context of the practice. While mobile technologies provide considerable advantages and flexibility in the processing of information and persons working outside the physical confides of the practice, they also pose significant risks. Firstly, the use of mobile technologies outside of the physical and technological controls within the practice must be taken into account. In addition, unless properly controlled the provision of remote access to servers within a practice may result in unauthorised access being obtained through the less secure channels of communication. Users of a practice's information assets outside of the control of its physical parameters must be educated in their information security responsibilities and appropriate agreements concluded between a person granted the privilege of processing information outside of the practice or remotely accessing information from outside of the practice.

7.32 **Information Classification.** A framework should be established describing how information must be classified within the practice. A scheme that would work for most practices would be:

[13] 5.1.7 King III Report

- **Confidential Information.** Access to this information must only be granted to persons authorised by the owner of the information;
- **Restricted Information.** All employees of the practice are authorised to have access to the information. Third parties engaged by the practice and who are subject to an information security agreement may have access to the information;
- **Public Information** – This information is information which, through a mechanism of approval, has been declared to be public information by the practice.

7.33 In the normal course a proper classification would find that the vast majority of the information processed within an attorney's practice (at least 90%) would be "restricted". This information should nonetheless, by the nature of attorney's practices and their confidentiality obligations, still be strictly controlled to ensure the preservation of confidentiality and, where appropriate, attorney and client privilege.

7.34 The classification of information should be made by the designated owner of the information. The owner must determine who would be entitled to access the information and what controls should be established to ensure the information integrity is maintained.

7.35 Clients are entitled (indeed it is a right protected by the Constitution) to have access to their own information. Appropriate controls in ensuring that access to this information is provided only to the specific client entitled to access the information must be established.

Human Resources Security

7.36 The objective to dealing with human resources security issues is to ensure that persons dealing with information understand their responsibilities, are suitable to the roles that they may be considered for and that their security responsibilities are addressed prior to employment in terms of appropriate agreements.

7.37 All employees should understand their information security responsibilities. This will in the normal course be achieved by documenting information security responsibilities in employment contracts and in Acceptable Use Policies which must be accepted by the employee prior to being granted access to the practice's information systems or its information.

7.38 **Prior to engagement** it may be appropriate to screen employees and third parties who may be granted access to sensitive information.

7.39 **During their engagement** employees must be subject to information security policies, must receive appropriate awareness, education and training and breaches should be subject to disciplinary procedures. Third parties should be subject to commensurate arrangements contained in third party agreements.

7.40 **Changes of engagement** must be subject to proper change control mechanisms which revoke employees rights to information which they will no longer require in the course of their engagement and formally authorise and grant access to information that the new engagement requires.

7.41 On **termination of engagement** controls must be in place to remove access privileges to physical premises, the revocation of rights of access to information and the return or destruction of information in the possession of the person whose engagement is terminated.

7.42 Particularly as electronic technologies have made vast amounts of information extremely portable, the barriers which previously existed to the removal of information on paper have disappeared. It is therefore critical that appropriate exit policies and procedures are formulated and properly implemented.

Physical and Environment Security

7.43 The object of ensuring physical and environmental security from an information security perspective is to prevent unauthorised physical access which may lead to the unauthorised access to damage of or interference with the practice's information.

7.44 An obvious corollary to this is that physical premises in which critical or sensitive information is processed should receive appropriate security attention. They should be protected by defined security perimeters, physical barriers and entry controls where necessary. In all cases the protection should be commensurate with the identified risks.

7.45 It is also important that information systems (eg. hardware, cabling, routers and hubs) on which information is processed receive appropriate protection. The protection provided should be commensurate with the identified risks.

7.46 The practice's reception areas should be manned at all times save when the business is closed and access to the premises secured. Access to areas in the practice's premises where information is processed, should only be granted to clients or third parties on the basis that they are accompanied by a person authorised to do so. Where possible, meeting rooms should be separated from any operational areas of the practice.

7.47 Where areas are secured and access restricted (eg. Computer rooms), appropriate controls to entry should be implemented to ensure that only authorised personnel are allowed access and where necessary, records or registers of persons granted access must be kept.

7.48 While it is beyond the scope of this guideline to deal with this in any detail, issues of environment security need to be considered, including controls against damage from fire, flood, earthquake, explosion and other forms of natural and manmade disasters. Equally, protections which include backup facilities and the retention of information off-site (in both physical and electronic form) should be dealt with.

7.49 In dealing with electronic information the establishment of uninterrupted power supplies and, where necessary, backup generators may be a consideration.

7.50 An issue which is often lost sight of is that controls must be established to ensure that sensitive data (and possibly licensed software) has been removed or securely overwritten prior to the disposal of computer equipment. These principles apply equally to media on which information may have been stored. Prior to removing equipment or media from the premises of the practice, proper steps need to be taken to ensure that information is secured, or deleted in a manner that it cannot be reconstructed.

Governance and Management of Information Processing and Communications Facilities

7.51 In ISO27002 this is referred to as "Communications and Operations Management". I have changed the heading for this section as I believe it more accurately describes the issues at hand.

7.52 For many practices in South Africa the management of their information system is in the hands of third parties. Many attorneys rely on technology vendors and technology support companies to manage their information systems. As is evident from King III, these functions may be delegated but must not be abdicated, particularly with regard to information, the responsibility of management rests with attorneys, their appointed executive committee or staff to whom this responsibility has been properly assigned.

7.53 The objective of control measures relating to communications and operations management are to ensure that the information processing facilities of the practice operate correctly and securely. To the extent that responsibilities are delegated to third parties there should be written agreements which record and govern the third party's obligations.

7.54 In many instances in South African practices the management of the technologies facilitating information processing and communication is assigned to an external third party. The following responsibilities of the third party will provide some guidance as to important issues to be addressed in agreements with third parties. Where the necessary management is provided by technologists employed by the practice these responsibilities may be included in an employment agreement.

- Operating procedures must support the practice's information security policies;
- Operating procedures must be properly documented;
- Changes to technologies facilitating information processing and communication must be made with due care for the security of information and avoidance of disruptions to the practice;
- Where they support information security, duties of the persons managing information systems must be segregated;
- Access to information systems and information must only be granted against appropriate authority of the owners of the information systems and/or information;
- The development and acquisition of all new technologies must take into consideration and ensure information security capability in the developed or newly acquired technologies;
- Information and communications technologies must be tested prior to implementation in the operational environment to avoid unnecessary disruption;
- Protections against malicious and mobile code (viruses) must be implemented;
- Appropriate backup of information and information systems must be implemented;
- Records, including but not limited to audit trails and logs of usage of information must be retained;
- All media on which the practice's information may be stored (particularly where removed from the physical protection afforded by the practice) must be appropriately controlled;
- Where computer equipment is to be disposed of or destroyed the information must either be removed from the equipment or destroyed in a manner that it cannot be reconstructed;
- Where appropriate intrusion detection and monitoring must be facilitated;

- Generally best practice supporting the establishment and maintenance of information security must be applied.

7.55 There may be numerous practice specific considerations which also have to be addressed and some of the issues already addressed relating to the screening of information technologists and their confidentiality obligations must also be included in these agreements.

7.56 In dealing with agreements with a service provider it must be borne in mind that the provision of information system services is highly dependent on creating a cooperative relationship. This requires persons within a practice responsible for information systems and information security to work closely with the service provider, regularly review the service provision and ensure that the services are being provided in terms of the agreement and information security principles inherent in that agreement. This cooperation will also facilitate the planning of changes to systems, upgrading of systems and implementation of third party systems which may need to integrate with existing systems.

7.57 Extremely important to some practices is the monitoring of communications with third parties (not the content of the communications but the communications traffic). Persons responsible for the administration of communication systems should ensure that proper logs of communications are retained, a monitoring system used to ensure that capacity is adequate, faults and the rectification thereof are logged, adequate backup is available at all times, in the event of system failures these can be rectified with the least possible disruption and generally administering the information system in line with good practice and generally accepted information security practices.

7.58 Care must be taken in using vendor agreements. Often the vendors of technology do not have appropriate vendor support agreements and where they do they tend to be very biased towards the vendor. Typically, they do not address issues of information security. Attorneys need to ensure that where third parties are employed to manage information processing and communications facilities, appropriate agreements are concluded. For attorneys who might not have the necessary background or expertise to do this, it would be a worthwhile investment to engage a person with the appropriate expertise to assist them in ensuring the agreements address all relevant issues, including information security.

Access Control to Information

7.59 The objective is to control access to information.

7.60 In the same manner that the control of access to physical areas is a key security control, the proper control of access to information systems and information will limit the risk of their compromise.

7.61 In determining who should be granted access, the principle that should be followed is that access to information is only granted on a “need to know” basis. Access should generally be forbidden unless expressly permitted.

7.62 Procedures need to be developed for the authorisation of access to information and identified owners of information should be the persons authorising the grant of access.

Information owners need to take into account the classification of information principles, dealt with earlier, in doing so.

7.63 The grant of access to information must be reviewed on a regular basis by information owners authorising access.

7.64 Once the grant of access has been authorised, access to information systems and information may be granted by system administrators responsible for the control of access. This is typically done by assigning a unique user registration ID and allowing the user to select a password to authenticate the user's identity. More sophisticated control mechanisms such as the use of digital certificates could also be implemented to authenticate identity.

7.65 Without mechanisms to authenticate the user (such as passwords or other authentication software) it is impossible to establish accountability for persons accessing information systems or information residing on those systems. It is unfortunate, but true, that access control to information systems is often lax and the control of passwords, where passwords are used, lamentably poor. Passwords are not a strong form of authentication, although it is true that strong passwords can be created and can be established through well-formulated and implemented password policies, procedures and standards.

7.66 In safeguarding confidential information, its retention and communication, it is recommended that attorneys consider the use of Encryption and Data Rights Management technologies. These technologies are extremely useful in restricting access to information at a document level and ensuring that even if the information is accessed without the necessary decryption keys, encrypted information cannot be read.

7.67 It should also be remembered that unauthorised access to information is a criminal offence in terms of the Electronic Communications and Transactions Act[14] and users should be reminded of the fact that unauthorised access (or attempts at access) information systems and information may not only be subject to the normal disciplinary procedures contained in the policy but also to criminal prosecution.

7.68 In order to control unauthorised access, unattended equipment should be controlled to prevent unauthorised access and "clear desk" and "clear screen" policies should be implemented.

7.69 Where access to information systems is granted to remote users special care needs to be taken to ensure that the authentication of the identity of the remote user is established before access is granted.

7.70 There are a number of technological tools that assist in the control of access. These should be investigated and where necessary implemented to assist the control of access.

7.71 In certain instances systems which process particularly sensitive information may be isolated from the general computing environment either as dedicated computers and servers or on isolated networks.

[14] Section 86 of the Electronic Communications & Transactions Act

7.72 It is a worthwhile investment to devote time to dealing with the control of access to information systems and information. Control procedures and standards should be carefully investigated and those most appropriate for the practice or for the information within the practice which needs to be protected should be implemented. While technologies are of great assistance in the control of access, equally important are the establishment, maintenance and regular review of access control policies, procedures and standards. It is critical to the success of access control that owners of information are properly trained in their responsibilities relating to the authorisation of access, system administrators in their responsibilities in granting access and users in their responsibilities to observe access controls.

7.73 Supplementary to the control of access must be the control of revocation of access. In all circumstances where a person no longer requires access to information (even if they remain engaged by a practice), access should be revoked.

Information Systems, Acquisition, Development and Maintenance

7.74 The objective of this control is to ensure security is an integral part of information systems used to process and communicate information.

7.75 In many instances attorneys will require assistance from technologists relating to the acquisition of new information systems or enhancements to existing information systems. Unfortunately, the issue of information security is often overlooked by the attorney and these issues are not adequately addressed by the technologists in making acquisition and development decisions.

7.76 One of the primary issues in the acquisition of new technologies or the development of technology must be the information security provided by the technologies. Questions should be asked as to whether the technologies are designed and incorporate appropriate information security features and, where possible, warranties in this regard should be obtained.

7.77 Often technologies have, inherent in their operation, information security features which are simply not used due to poor configuration. This can be avoided if the information security considerations are properly considered in the purchase, development or implementation of new technologies.

7.78 Cryptographic controls are increasingly being used to protect the confidentiality, authenticity and integrity of information. They are also the basis of electronic signatures in many instances. While they may be controlled internally, in many instances they will be subject to the control of a trusted third party.

7.79 As the emphasis on using cryptography as a security mechanism increases it is important that policies are developed relating to the use of cryptography and an understanding obtained as to how these technologies work and the allied management that is required to control the technologies properly. It is beyond the scope of this guideline to deal with this in any detail, but as encryption technologies provide some of the most promising tools to provide the degrees of security that attorneys require in the communication and retention of

information, it is recommended that attorneys investigate these technologies in considering their information security.

7.80 Another issue which does not necessarily entail acquisition of technologies but relates to systems acquisition is the attractiveness of outsourcing information facilities and the development of "cloud computing".

7.81 Cloud computing and outsourcing allow attorneys the commercial benefits of sophisticated information technologies at a fraction of the cost of the purchase of these technologies.

7.82 It must be appreciated that outsourcing and cloud computing by their nature may result in information entrusted to attorneys by clients and the practice's business information falling under the control of a third party. In the circumstances the attorney's obligations to clients and legislative obligations need to be borne in mind and if necessary, the appropriate assurances obtained from the providers of the facilities and documented in agreements governing the relationship.

Information Security Incident Management

7.83 The objective of implementing information security incident management is to ensure that when security incidents occur, timely corrective action can be taken.

7.84 Information security is seldom, if ever, one hundred percent foolproof. Breaches of security will occur and the ability to react appropriately is important in avoiding reputational risk and potential liability that may result from these breaches.

7.85 In dealing with security incidents the management team should be skilled in the investigation, gathering of the necessary evidence, remedial measures required, and, where necessary, communication of the incidents to the parties affected and possibly the media. There should be a clear definition of roles in this regard to enable a coordinated and coherent response to information security incidents.

Business Continuity Management

7.86 The objective of business continuity management is to counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

7.87 A process should be developed and maintained for business throughout the practice that identifies the information security facilities critical to the practice's business and addresses remedial measures in the event of failures of the information systems.

7.88 Business continuity management is far wider than incident response management. It is aimed to protect critical business processes from the effects of major failures of information systems and to ensure their speedy resumption. In the circumstances events that could cause interruptions to business should be identified along with the probability of the impact of such interruption and the consequences for information security.

7.89 It is beyond the scope of this guideline to deal with business continuity in any detail but it is an aspect of information security which should be addressed by all practices who have

become reliant on their information systems and information processed and retained by those systems.

Compliance

7.90 The objective is to avoid breaches of any law, statutory, regulatory or contractual obligation and breaches of any security requirements established by the practice.

7.91 Issues of licensing and intellectual property rights need to be properly controlled to ensure software used to process information is used legitimately.

7.92 Important records may require protection from loss, destruction and falsification in terms of statutory, regulatory, contractual and business requirements. Care needs to be taken to ensure that these records are maintained properly, particularly where these records have been digitised and the paper records destroyed.

7.93 The increasing importance of the protection of personal information demands careful consideration of legislation, regulation and provisions to be contained in agreements with data subjects as well as third parties processing personal information on behalf of attorneys.

7.94 From an internal perspective attorneys should demand compliance with security policies, procedures and standards. It is critical therefore that regular reviews of compliance with internal policies, procedures and standards are conducted.

7.95 In many instances information systems provide audit controls. These must be properly implemented and analysed by persons responsible for their analysis in auditing the information security status of the practice. It is advisable that auditors include in their audits the audit of information security. With regard to financial information this may already be in place for some practices, but for many practices audits of general information security would not be a routine audit issue. In particular in the light of existing and pending legislation, it is recommended that practices consider the inclusion of the audit of information security as a routine audit issue.

Special Issues to be Addressed

7.96 These issues are not within the scope of this guideline but are developments which have serious information security implications.

7.97 **eMail** is now pervasive in most practices. It has become the *de facto* mechanism of communication and even the most sensitive information is communicated using eMail. Unfortunately, eMail is a notoriously insecure mechanism of communication and it is suggested that careful consideration be given to establishing good eMail policies and practices that take into consideration the information security obligations of attorneys.

7.98 The use of **short message services (SMS)** instant messaging, some of which are provided in social networking services such as Facebook and Twitter and the use of cellphones to communicate by eMail are all recent phenomena which need consideration. It should be remembered that in certain instances the information system (eg. cellphones) will not be owned by the practice, nor will the communication be subject to control on servers within

the practice. Electronic communications policies may have to be reviewed in light of these developments if use of these technologies is to be allowed for business purposes. If not, then their use should be expressly prohibited.

7.99 **Mobile Computing and Teleworking** are two phenomenon that have become exponentially more important in the processing of information. It is important that proper controls are implemented to ensure that information on mobile computers or on computers which are accessed remotely and are outside of the normal physical security and information securities within an organisation, remain protected.

7.100 Mobile security devices should be encrypted so that their loss does not subject the information on those devices to unauthorised access.

7.101 Agreements with persons using mobile devices and teleworking, expressly establishing their obligations, must be concluded. These agreements must expressly address appropriate information security arrangements.

Chapter 8

8. REFERENCES

8.1 There are many references to particular areas of information security that are easily available on the Internet. The following Standards are useful but it must be understood that they are provided as guidelines and must be considered in the light of the practice, its information systems and information and compliance requirements in determining whether they are appropriate.

- ISO27001:2005 Information technology — Security techniques — Information security management systems - Requirements
- ISO27002:2005 Information technology — Security techniques — Code of practice for information security management
- ISO27003:2010 Information technology — Security techniques — Information security management system implementation guidance
- ISO27005:2008 Information technology — Security techniques — Information security risk management
- ISO38500:2008 Corporate Governance of Information Technology