

Offshore Data Hosting White Paper

MARCH 2008

The information contained in this White Paper (i) is based on our interpretation of current principles of South African law which may be subject to change occasioned by future legislative enactments (most notably the pending Protection of Personal Information Bill) and court decisions, (ii) is neither an endorsement of Iron Mountain Digital's products nor an independent assurance that its systems are reliable and operate without material errors, faults or failures and (iii) is not intended as legal advice. It has been prepared as a summary and opinion on general principles of law or other common law principles and is published for general information purposes only. Only specific professional advice should be relied upon as to what is herein contained may not be appropriate in particular circumstances. This is not a substitute for legal or other professional advice.

BACKGROUND

Iron Mountain Digital's Data Protection and Archiving Software as a Service (SaaS) is available to businesses in South Africa through its distributor, Channel Data (Pty) Limited, and its network of resellers and service providers. Client data for the different SaaS solutions offered to the South African market are hosted in either the United States of America¹, Belgium², the United Kingdom or Germany³. For further information on the different Iron Mountain Digital Services and Solutions offered see the Iron Mountain website at www.ironmountain.com/digital.

The purpose of this White Paper is to explain (i) how South African law, and in particular the provisions of pending data privacy law in the Protection of Personal Information Bill (PPIB) will impact on Iron Mountain Digital's SaaS solution offerings once it is enacted and (ii) the measures Iron Mountain Digital will take to ensure compliance with the requirements of South African law.

As the law currently stands, there is no legal bar to individuals and companies transferring personal information and data to the international offshore data centers from which Iron Mountain Digital SaaS solutions are offered. However, once the PPIB becomes law, obligations will be imposed on both Iron Mountain Digital and its customers. There will also be indirect requirements imposed. This is because one of the most vexing issues in trying to comply with privacy laws worldwide is being able to translate what the laws mean for everyday business use and IT practices. Compliance with the letter of the law can be extremely difficult, especially because the PPIB will be new and it will take some time before the Information Protection Commission (the Privacy Regulator) or South African Courts hand down definitive guidelines. See "Iron Mountain's Responsibilities" and "Your Responsibilities" below.

TYPES OF COMPLIANCE

In this White Paper, we deal with legal issues insofar as they pertain to legal compliance with regards to privacy, information security and records. It is important to note that the South African legislative landscapes in these areas are very different to the landscape in other countries, most notably the USA, where there are specific laws which regulate these activities. However, one must not be under the misapprehension that what is obligatory in the USA (e.g. compliance with the Sarbanes Oxley Act) is or will be obligatory in South Africa (for all companies). One must also be careful not to misinterpret best practice (for example the South African information security standard SANS 17799:2005/ISO/IEC⁴) as mandatory legal compliance. Moreover, one must be careful not to misinterpret international standards as *de facto* legislation in South Africa when South African individuals and companies are free to adopt whatever standards they choose.

TYPES OF INFORMATION

The types of information that can be transferred and hosted offshore to the data centers from which the Iron Mountain Digital SaaS solutions are offered include "**Personal Information**" (PI), "**Sensitive Information**" (SI) and "**Records**".

PI will be regulated by the PPIB, once enacted. PI has been specifically defined in section 2 of the PPIB⁵.

¹ Connected® Backup (for PC, Macintosh and File Servers), LiveVault® (for Servers) and DataDefense™.

² Connected® Backup (for PC, Macintosh and File Servers) and LiveVault® (for Servers).

³ Connected® Backup (for PC, Macintosh and File Servers), LiveVault® (for Servers) and Total Email Management Suite (TEMS).

⁴ Information technology – security techniques – code of practice for information security management (SANS 17799:2005).

⁵ "personal information" means information about an identifiable, natural person, and in so far as it is applicable, an identifiable, juristic person, including, but not limited to

a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, color, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

SI is defined by organizations according to the classification chosen by them (e.g. “secret”, “confidential” and “public”). *Sensitivity classifications in the private sector are not regulated by any law.* However, sensitivity classifications in the public sector are regulated by amongst other things the Protection of Information Act, 84 of 1982 (PIAA), soon to be replaced by the Protection of Information Bill which is currently before Parliament. PIAA deals with inter alia what constitutes “classified information”⁶ and who may have access to such information.

There is currently no definition of a “**record**” that is universally used by all organisations. The simple reason for this is that definitions serve the community that they are created by and each community has different needs. Whilst not in itself the law, the South African National Standard on records management (SANS 15489) defines a record as “information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business” (our emphasis). Each company needs to derive its own definition of a record and in so doing be able to “separate” the wheat from the chaff and identify what information constitutes a record or not.

It is your responsibility as an end user to determine what is PI, SI and what constitutes a “record” and to implement physical and logical security measures to protect such information and determine whether or not that information can be transferred to the offshore data centres from which the Iron Mountain Digital SaaS solutions are offered.

PRIVACY COMPLIANCE

In October 2005 the South African Law Commission published the PPIB. **The PPIB is not yet law.** It is expected that the Bill will be enacted during the course of 2008.

Pre-PPI

As the law currently stands, the right to privacy is protected in terms of both our common law and in section 14 of the Constitution of the Republic of South Africa Act, 108 of 1996 (“the Constitution”). The constitutional right to privacy is, like its common law counterpart, not an absolute right but may be limited in terms of law of general application and has to be balanced with other rights entrenched in the Constitution. Therefore, although individuals and organisations can institute legal proceedings alleging an infringement of the right to privacy at this point in time, complex legal arguments will have to be presented to prove the infringement. **Moreover, as the law currently stands, there are no express legal requirements that have to be complied with when it comes to storing personal information offshore.**

Post-PPI

The PPIB seeks to regulate the “processing”⁷ of PI. Inasmuch as PI will in all probability be transferred during the use of SaaS solutions, the PPIB will apply to the Iron Mountain Digital SaaS offerings once enacted, and Iron Mountain Digital will be legally required to (i) notify its customers and the Information Protection Commission of any security breaches which have resulted in the PI of its customers being accessed by an unauthorized person⁸ and (ii) obtain the consent of its customers to the transfer of their PI offshore⁹, which Iron Mountain Digital already does as part of its SaaS procurement and client registration procedures.

Consent

Section 94(b) of the PPIB permits Iron Mountain Digital, its resellers and managed service providers to transfer their clients personal information to the offshore data centres from which the Iron Mountain Digital SaaS solution are offered if their clients consent to the transfer. This consent is usually provided for in the Agreement which is entered into with you.

INFORMATION SECURITY COMPLIANCE

- b) information relating to the education or the medical, criminal or employment history of the person or information relating to financial transactions in which the person has been involved;
- c) any identifying number, symbol or other particular assigned to the person;
- d) the address, fingerprints or blood type of the person;
- e) the personal opinions, views or preferences of the person, except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual;
- f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- g) the views or opinions of another individual about the person;
- h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the person, but excluding the name of the other individual where it appears with the views or opinions of the other individual; and
- i) the name of the person where it appears with other personal information relating to the person or where the disclosure of the name itself would reveal information about the person;
- j) but excludes information about a natural person who has been dead, or a juristic person that has ceased to exist, for more than 20 years;

⁶ “State information that has been determined under this Act or the former Minimum Information Security Standards (MISS) guidelines to be either “Top Secret”, “Secret” or “Confidential” in order that such information may be afforded heightened protection against unauthorised disclosure” (per section 1(1) of the Protection of Information Bill).

⁷ The PPIB defines “processing” as the “collection, recording, organization storage, updating or modification, retrieval, consultation, use, dissemination by means of transmission, distributing or making available in any other form, merging, linking, as well as blocking, erasure or destruction of information”

⁸ In terms of section 20.

⁹ In terms of section 94(b).

There is no single law in South Africa that deals exclusively with information security. There are several pieces of legislation¹⁰ which impose information security obligations and various non-statutory sources of obligations¹¹. However, **none impose specific physical or logical security measures that have to be followed in order to keep information and records secure.**

What the lawmakers have done recently in the PPIB is to impose a general standard requiring “reasonable”¹² security or “appropriate” security, where companies will be required to take steps to protect PI. Previously this has been expressed in best practice (notably SANS 17799:2005) and in the King II Best Practice Guide for Information Security.

Section 17(2) (headed “Security Safeguards”) stipulates that an organisation must take measures to:

- “(a) identify all reasonably foreseeable internal and external threats 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.”

Thus, rather than telling companies what specific security measures they must implement, the law will require companies to engage in an ongoing and repetitive process that is designed to assess risks, identify and implement appropriate security measures responsive to those risks, verify that they are effectively implemented, and ensure that they are continually updated in response to new developments. It does not require the use of any specific security measures, instead leaving the decision up to the company.

Iron Mountain already has proper security safeguards in place to protect the PI of its customers. In this regard, Iron Mountain has achieved SysTrust™ certification from an outside, independent and reputable professional service firm who have audited Iron Mountain’s Information Technology Infrastructure Environment to ensure that Iron Mountain has appropriate internal controls in place for security, availability, processing integrity and confidentiality of the personal information that it hosts. Iron Mountain intends to renew this certification annually.

To review Iron Mountain’s certifications and to access a copy of the SysTrust™ audit report go to www.ironmountain.com/company/certification.asp.

The SysTrust™ security requirements inter alia require Iron Mountain to meet high standards for the protection of its system components from unauthorized access, both logical and physical. Additionally, Iron Mountain Digital’s SaaS offerings also makes use of secure transmission channels and encryption during Internet transfer of PI and SI and stores this data encrypted in digital vaults which further ensure its information security compliance.

RECORDS COMPLIANCE

Iron Mountain Digital’s Connected® Backup (for PCs, Macs and Servers), LiveVault® (for servers) and the Total Email Management Suite (for Microsoft Exchange) protect SI off-site. “Records” will in all likelihood be included in such SI.

There are several hundred statutes in South Africa which prescribe recordkeeping obligations, but none of them prescribe how the records must be kept and which technologies must be used.¹³ This is left up to the individual or company to determine.

Where the records are in electronic form, section 14 (original) and 16 (retention) of the Electronic Communications and Transactions Act (ECT Act) allows you to keep the record in electronic form, **provided that you implement a reliable, auditable process.** However, the ECT Act, unlike some foreign laws¹⁴, does not provide procedural or technological standards that have to be followed in order to ensure that a record will be legally valid. It does not prescribe any technical functional requirements and leaves it up to the end users and implementing technology companies to determine what is appropriate having regard to the technological requirements of their clients in conjunction with best practices and risk management.

¹⁰ See section 20 of the PPI Bill.

¹¹ E.g. The Information Security Best Practice Guide to King II, to be followed in 2008 by King III.

¹² In *Transnet Limited and Another v SA Metal Machinery Co. (Pty) Limited* 2006 (1) All SA 352 (SCA) the court interpreted the word “reasonable” in the context of that case to mean a **moderate** or **fair** probability.

¹⁴ E.g. the Gramm-Leach-Bliley (“GLB”) Act in the United States, which does not apply in South Africa, Securities Exchange Commission (“SEC”) Rules 17a-3 and 17a-4, the Fair and Accurate Credit Transactions Act (“FACTA”), the Sarbanes Oxley Act (“SOX”) and the Health Insurance Portability and Accountability Act (“HIPAA”).

Email Archiving (a sub-set of records compliance)

Iron Mountain Digital’s Total Email Management Suite (TEMS) Active Archiving Service for Emails (a managed service for email storage management, archiving and discovery)¹⁵ and its Connected® Backup for PC with EmailOptimizer™ (patented functionality to efficiently and effectively backup personal email folder files such as PST files), provides a solution to protect and/or archive emails off-site.

Email, in and of itself, is a transmission medium for content that may or may not constitute a record. If it constitutes a “record” it may have to be kept for a minimum period of time as determined by the business itself or as required by an act of Parliament.

It is up to the individual or company to “separate” the wheat from the chaff and identify which emails are records. The difficulty lies in giving practical effect to those laws which require that “records” be retained, as they focus on the need to retain the record based on its content and often do not (i) focus on the specific medium that is used to transmit or house the record (e.g. email, a Word document or paper), or (ii) identify precisely what the actual record is as this is often not apparent from the statute.

RESPONSIBILITIES AND RECOMMENDATIONS

YOUR RESPONSIBILITIES	IRON MOUNTAIN’S RESPONSIBILITIES
<ul style="list-style-type: none"> ▪ Establish what information you hold that supports your business activities and programs by way of an Information Inventory¹⁶. ▪ Determine your PI, SI and Records (including email records) from the Information Inventory. ▪ Draft and implement appropriate¹⁷ policies detailing <i>inter alia</i> the information handling criteria¹⁸ for PI, SI and Records together with clear rules on what PI, SI and Records can be transferred offshore. ▪ Implement logical and physical security measures to assess risks, identify and implement appropriate security measures responsive to those risks. ▪ Furnish written consent to your PI being transferred offshore. ▪ Companies to obtain written consent from employees whose PI will be transferred offshore. 	<ul style="list-style-type: none"> ▪ Provide the SaaS in a secure and efficient manner. ▪ Prepare for compliance by implementing proper security safeguards which it already does (see Iron Mountain’s most recent SysTrust™ certification)¹⁹. ▪ Prepare for compliance by implementing a proper incident response plan to notify customers of potential breaches of their PI as required by section 20 of the PPIB. It should be noted that Iron Mountain’s current processes already adhere to these requirements. ▪ Take all steps necessary to ensure that data centre locations (in the US, UK, Belgium and Germany) from which the Iron Mountain Digital SaaS solutions are offered upholds principles for PI similar to the PPIB.*

*** Cross border data transfers**

End users of the SaaS offerings are legally permitted to transfer PI offshore in several scenarios. One of those is where you have consented to the transfer. Another one is where Iron Mountain’s operations which host the data offshore are in countries which have laws which “effectively upholds principles for fair handling of the information that are substantially similar to the Information Protection Principles set out in Chapter 3 of” the PPIB.²⁰

Iron Mountain already incorporates key elements of data protection laws in the European Union into its operations and insofar as the USA is concerned, complies with the US Department of Commerce’s Safe Harbor Privacy Principles. **We are therefore confident that Iron Mountain currently already complies with the provisions of section 94(a) of the PPIB.**

¹⁵ Discovery (in court proceedings) is a procedure whereby a party can (i) require his opponent to specify on oath the documents in his possession or under his control which relate to the court case and (ii) inspect and copy such documents. Discovery helps each side understand the material facts and evident in advance of the trial. It also prevents anyone from being ambushed at the trial. An email archiving system with appropriate discovery capabilities can minimize the time and expense required to produce the required information. A company that receives a discovery request or subpoena *duces tecum* that calls for the production of emails, for example, is under a duty to make a proper effort to search for the email. The nature and extent of this search may be traversed in cross-examination where the request is not met. It is not an offence to fail to discover documents.

¹⁶ This must aim to be a complete and current reflection of information holdings required to support business processes and objectives which will ultimately be described in the information directory. The Inventory gives action and potential users of the information a greater understanding of what information is available.

¹⁷ E.g. Information and Records Retention and Destruction Policy, Email Archiving Policy, various Information Security Policies.

¹⁸ E.g. to shred paper that is classified “secret” versus only having to throw paper classified “public” in the rubbish bin.

¹⁹ www.ironmountain.com/company/certification.asp

²⁰ Section 94(a).

ABOUT MICHALSONS

Michalsons is a boutique IT law firm which offers a range of services aimed at assisting companies proactively address the challenges they face in the South African regulatory IT environment. Michalsons provides its services to organisations in both the private and public sectors.

Together with its consulting arm, i-Forest Information Management (Pty) Limited (an information management consultancy that enables organisations manage their information holdings in a compliant and operationally optimized manner), we assist companies compile Information Inventories, draft file plans, provide guidance on what information constitute records, identify what laws require you to retain records, how to classify information and records according to their sensitivity and write the necessary Policies to give effect to the foregoing.

Michalsons have been involved in the drafting of the ECT Act on the instructions of the Department of Communications and the King II Best Practice Guides on Information Security and Escrow on the instructions of the Institute of Directors. Lance Michalson is currently the chairman of the IT work stream for the chapter on Risk Management in King III and is one of the 267 lawyers in the world selected for inclusion in the forthcoming 2008 edition of the international Who's Who of Internet and e-Commerce Lawyers.

ABOUT IRON MOUNTAIN DIGITAL

Iron Mountain Digital is the world's leading provider of data backup/recovery and archiving software and storage as a service (SaaS). The technology arm of Iron Mountain Incorporated (NYSE: IRM) offers a comprehensive suite of data protection and archival storage software and services to thousands of companies around the world, directly and through a world-wide network of channel partners.

Iron Mountain Digital is based in Southborough, Massachusetts. with European headquarters in Frankfurt, Germany.

Founded in 1951, Iron Mountain Incorporated (NYSE: IRM) is a trusted partner to more than 100,000 corporate clients throughout North America, Europe, Latin America and the Pacific Rim.

ABOUT CHANNEL DATA

Channel Data (Pty) Limited is Iron Mountain Digital's authorized distributor for sub-Saharan Africa. It is a black empowered company based in Johannesburg with a regional office in Cape Town and has been involved in IT distribution since the late 1980s. The company specializes in supplying IT infrastructure products including Networking, Security, Storage and Power Solutions. Skilled and knowledgeable resources work with its channel partners to ensure complete and effective solution delivery to customers.

For further information please contact:

Michalson Attorneys

Contact: **Helaine Leggat**
 Tel: (011) 327-4540
 Cell: (082) 901-9500
 Email: helaine@michalson.com
 Web site: www.michalson.com

Iron Mountain Digital

Contact: **Amit Parbhucharan**
 Tel: (011) 235 7725
 Cell: (083) 400 3050
 Email: amit.parbhucharan@ironmountain.com
 Web site: www.ironmountain.com

www.michalson.com