Protection of Personal Information
Securing Unstructured Data

COMPLYING WITH THE KING REQUIREMENTS FOR THE PROTECTION OF PERSONAL INFORMATION

The King Committee on Corporate Governance in South Africa has emphasised the need for companies to ensure that there are systems in place for personal information to be treated by the company as an important business asset and that all ‘personal information’ processed by the company be identified. Soon the Protection of Personal Information Act will make this a law that every organisation must comply with, or face consequences of reputational risk to its brand.

Overview
The Protection of Personal Information (POPI) has become necessary as personal data in the possession of companies and other organisations is frequently used without consideration of the potential consequences to consumers and employees. Loss of personal data in the hands of public and private bodies and the resulting incidents of identity theft and fraud is just one example.

As a result, companies will have to redesign their IT infrastructure and business procedures to properly balance individual rights and the right of companies to use personal data for their business. Individuals will have the right to ask for information about the processing of their personal data. Companies will have the obligation of ensuring that personal data is properly protected at all stages of processing.

Locating Unstructured Data
The Protection of Personal Information requires organisations to locate all personally identifiable information (PII) and protect it from unauthorised access. This is not a trivial task in today’s highly distributed world where data is often duplicated and widely distributed – on users PC’s.

Solutions such as the Iron Mountain Connected® Backup with the Classify & Collect add-on enable organisations to unobtrusively inspect and gather unstructured data from across the organisation’s workstations and store copies in a central repository for recovery or export. Additionally, companies can locate and report on files and email on any PC containing personal information and ensure that it is properly protected, any unauthorised access is flagged and adequate steps taken to retain or dispose the files on the PC.

The Challenge of Securing Unstructured Data
Well-planned data storage and management has structure. The data is categorized, classified and tagged with meta-data that makes it easy to locate, manage and search efficiently.

In most organisations, 70-90% of business data is in an unstructured or semi-structured state. Recent research indicates that only 23% of organizations feel this data is properly protected. Unstructured data includes Word and Excel documents, PDF’s, email and instant messages.

Unstructured data must be protected in transit and when at rest. Frequently data is left vulnerable and without corporate oversight at the networks edge on devices such as PC desktops and mobile laptops - these being two of primary distributed repositories of unstructured data.

User Experience
Not everyone is a technology guru. Most users concentrate on getting their work done, not on the underlying technology powering that work. When a security solution is deemed too difficult to use, most users will circumvent the solution as well as the security.

The Iron Mountain Connected® for PC suite is designed to provide a secure, lightweight and robust solution with the least amount of discomfort to the user.

Companies can implement automated, efficient and secure backup and recovery capabilities for their important PC data using solutions from vendors like Iron Mountain which leverages data reduction and can perform indexing for improved data discovery and reporting for compliance.

Protecting Unstructured Data
Almost every organisation is using some form of encryption for data in transit – SSL being the most common for secure transactions on the web and VPNs, and deployed by businesses for over a decade.

While there are a number of options for securing unstructured data at rest on the company’s PCs, full hard disk encryption is a popular option but meets only a quarter of the need.

Before implementing full hard disk encryption companies need to plan how they will manage the distributed unstructured environment. Policies, classification schemes and naming conventions will be important components. Crucial to the protection of personal information is making sure there is no storage of data which is legally not allowed.

Iron Mountain Digital Archiving
Beyond the distributed desktops and laptops in organisations today, Microsoft Exchange®, SharePoint® and Windows® File Shares are other primary stores of unstructured and semi-structured data. The Iron Mountain NearPoint™ software solution provides organisations with an on-site unified indexed archive repository with integrated fine-grain restore of email items, mailboxes and SharePoint objects.

With NearPoint™, all data is globally single-instanced and de-duplicated no matter which system sent it to the archive and long term storage needs can be accommodated with the Iron Mountain Virtual File Store™ service!

The NearPoint™ solution provides rich functionality for retention, storage management and eDiscovery. One key feature is that this solution is agent-less and therefore enables faster adoption and greater ease of deployment.