Meet Compliance Requirements to Protect Personal Information in South Africa.

The mandate of South Africa’s Protection of Personal Information (PoPI) Act is to regulate the processing of personal information. With this Act, data breaches need to be reported by law. Organisations need to develop a clear data protection plan to build trust with customers, drive business growth, and avoid costly penalties. The Act comes into force on 24th May 2017 with a grace period that ends on 24th May 2018.

The foundation of any data security strategy is to identify sensitive and regulated data so that both users and security technologies can make informed, deliberate decisions on how that information should be protected. Titus Classification Suite helps organisations comply with PoPI by discovering, identifying, and classifying files and emails to ensure compliant policy enforcement.

Make staff aware of the value of personal data

A central pillar of PoPI is increased accountability to protect personal data. Data protection must be built into every aspect of the data handling workflow. Titus visual markings and pop-up reminders build a culture of security by forcing employees to consider the value of the personal data with which they are working.

Protect personal data

The Act states that organisations must identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control. When people and systems know the sensitivity of an email or file they can accurately enforce the proper data protections. Titus Classification helps to ensure data is shared according to policy across departments, locations, and organisations. In addition, Titus Classification enhances the effectiveness of the entire data security ecosystem. For example, classification metadata can automatically trigger encryption technologies and provides explicit instructions for DLP and CASB systems.

Proactively delete old data after a reasonable time

Personal information collected by organisations is also subject to deletion. It can be difficult to guarantee all personal data is deleted if it has been exported to files outside the central database. The metadata associated with
Protection of Personal Information (PoPI) Act

Titus Classification helps enable staff to locate files that should be deleted for compliance purposes, no matter where they are stored.

Supporting the Information Officer

One of the mandates for compliance with PoPI is to have a named Information Officer appointed within your organisation. The Information Officer must ensure that the organisation complies with PoPI. He or she needs the means to monitor how personal information is being shared, discover violations, and enhance data protection policies. As users work with email, documents, and files, Titus logs meaningful activities and policy alerts, permitting detailed reporting and analytics. Classification adds a level of detail to reporting that is not normally available, enabling the Information Officer to identify exactly where sensitive data is being mishandled, or where a user presents a threat to data security.

About Titus

Titus is a leader in providing solutions that enable businesses to accelerate their adoption of data protection. Millions of users in over 120 countries trust Titus to keep their data compliant and secure, including some of the largest financial institutions and manufacturing companies in the world, government and military organizations across the G-7 and Australia, and Fortune 2000 companies. To learn more about how Titus can help with CUI and CNSI marking and metadata programs visit www.titus.com.