INFORMATION SECURITY POLICY

Protection of confidential information, whether it belongs to South Western or to others who have entrusted such information to us, is essential to our reputation and to the survival of our business. This information can be in many forms --physical, electronic and intellectual (such as know-how), and can relate to all parts of our business. Common examples include tool designs, computer source code, marketing plans, clients' reservoir or seismic information, information kept in the corporate directory, and operating results.

Our employees must be careful not to disclose this confidential information to any unauthorized person, either intentionally or by accident. Unintentional disclosure of confidential information can be as harmful as intentional disclosure, and employees should be alert to the possibility of inadvertent disclosures, which could occur in social settings or in the course of normal interactions with customers and other business associates.

South Western operations must take all reasonable steps to establish and maintain the physical and electronic security of confidential information. Information security requirements and practicalities differ among the various parts of our organization. The ultimate responsibility for Information security lies with line management, but each Product Line is responsible for establishing information security policies and procedures which are appropriate for the sites involved. Information Technology will publish and update general guidelines and best practices for this process, and will assist the business

Quality, Health, Safety and Environment (QHSE) will coordinate and administer the process, including the design of appropriate training programs, in close cooperation with Information Technology and Personnel. Violations of these Policies can result in disciplinary action, including

Chris Idisi

Managing Director & CEO

10th September, 2017

South Western Technologies & Oilfield Services Ltd.