7 Information Security Policy

Information is the foundation of our business. Protection of confidential information, whether belonging to GTDS 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 any part of the businesses of GTDS. Common examples include tool designs, application source code, marketing plans, clients' reservoir information and operating results.

GTDS employees are not to disclose confidential information to any unauthorized person, either intentionally or by accident. Unintentional disclosure of confidential information can be just 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. Employees are to be adequately trained and then expected to protect confidential information by adhering to the Information Security standards and procedures related to their use, administration, or support of information technology resources.

Information Security will publish and update standards and procedures that apply to all employees and operations. The HSE function will continue to participate in information security risk identification and mitigation process at operational sites. Personnel remain responsible for properly initiating new and terminating exiting user accounts, as well as the deployment of employee education, supported by the Information security function.

The ultimate responsibility for information security lies with the line management of each Product Line. They are to ensure it is addresses as a critical business issue by providing the leadership and resources required in their respective organizations. Management should ensure the organization's compliance to the Information Security Standards through regular measurement of security results and audit of risk mitigation activities.

Violations of this policy can result in disciplinary action, including possible termination.

Kashif Rehman
CEO - GeoTarget Drilling Services.

23 June 2011