



Eastern Drilling Services

Information Security Policy

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

EDS employees are not to disclose confidential information to any unauthorized person, either intentionally or by accident. Unintentional disclosure of confidential information can just as harmful as intentional disclosure, and employees should alert to the possibility of inadvertent disclosure, 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 HSEQ function will continue to participate in information security risk identification and mitigation processes at operational sites. Personnel remain responsible for properly initiating new and termination 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 addressed 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
15th April 2008