# Confidentiality and Information Security Policy

Information is the foundation of our business. Protection of confidential information, whether belonging to SLB 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 SLB. Common examples include tool designs, application source code, smart card personalization data, marketing plans, clients' reservoir information, information kept in the Corporate Directory, operating results, financial information, ongoing research planning, inventions, and techniques. While the technology applications we use and the other confidential information we develop usually belong exclusively to SLB, at times, we may also be entrusted with highly confidential information of others, including our customers.

It is vital to the business success of SLB that we maintain confidentiality to all such information. All business, financial and technical conversations, notes, manuals, and papers and other forms of confidential information, whether physical or electronic, must be protected and SLB 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. SLB employees must be careful to avoid accidental disclosure—whether through careless conversations or the improper handling of documents, data, and software. Employees are to be adequately trained and are 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 Quality and HSE function will continue to participate in information security risk identification and mitigation processes at operational sites. Personnel remains 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 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.

Any violation of this Policy may subject the employee to disciplinary action.

Olivier Le Peuch

Chief Executive Officer, Schlumberger Limited

For further information regarding this policy:
CONTACT: Sebastien Lehnherr, Chief Information Officer
LOCATION: Schlumberger Limited, Houston
EMAIL: Sebastien Lehnherr

SLB-QHSE-L005
Released on 5 June 1997
Last Update on 9 August 2019