Information Security Policy

ISO 27001:2013

IDS is committed to protect the confidentiality, integrity, and availability of its assets by protecting them from unauthorized access, breaches, or disclosure.

To achieve this, the company is committed to:

- Secure its assets by establishing, implementing, maintaining, and continually improving an Information Security Management System according to ISO 27001:2013 requirements.

- Continually identify and monitor threats and vulnerabilities that can affect business continuity.

- Continually identify risks, understand them, analyze them, assess them, and treat them.

- Identify, classify, and label the company's assets and control their use.

- Provide and protect the infrastructure needed to achieve objectives already set by providing an appropriate work environment, training employees, improving their knowledge and skills, and raising their awareness about all security issues.

- Ensure that its data stays available to authorized users at all times.

- Ensure that its data is protected from alterations and breaches.

- Control and monitor access to its networks and assets.

- Ensure that data is protected during data transmission.

- Secure software production by restricting access to data and source code, and by performing extensive software testing.

- Ensure correct and secure operations of all information processing facilities by continuously updating and maintaining them.

- Ensure that information security accidents are reported, investigated, and handled properly.

- Secure its purchasing process by establishing information security rules and policies for the relationship with the external providers.

- Ensure that information security rules, policies, objectives, processes and procedures are communicated to all interested parties.

- Adopt the continual improvement approach in its policy, objectives, and processes.

المدير العام