Information Security Policy

ISO 27001 : 2022

IDS is committed to protecting all information assets by implementing and maintaining the highest standards of security measures to ensure their confidentiality, integrity, and availability, thereby supporting business operations, regulatory compliance, and ethical responsibility.

This Information Security Policy outlines the principles and measures we follow to protect data, ensure business continuity, and promote a culture of trust, transparency, and continuous improvement.

- **Establishment and Continuous Enhancement of ISMS: We are dedicated to protecting our assets through the establishment, implementation, ongoing maintenance, and continual enhancement of an Information Security Management System (ISMS) aligned with the ISO 27001 : 2022 standard.**
- **Ethical Leadership and Accountability in Security: Ethical leadership is central to our information security strategy. Leaders at every level are expected to model integrity, uphold accountability, and embed information security into all decision-making processes as a reflection of our organizational values.**
- **Ongoing Threat and Vulnerability Monitoring: We proactively monitor and evaluate emerging threats and vulnerabilities that may impact our operations, ensuring timely responses to mitigate risks to business continuity.**
- **Risk Management: We identify, analyze, evaluate, and address information security risks using a structured risk management procedure that supports decision-making.**
- **Asset Identification and Control Measures: All company assets are systematically identified, classified, and labeled, with appropriate controls implemented to regulate their use and prevent misuse.**
- **Supportive Infrastructure and Training Programs: We maintain a secure and supportive work environment by providing the necessary infrastructure, regular training, skills development, and awareness to strengthen our security culture.**
- **Assurance of Data Availability: We ensure that all critical information remains accessible to authorized personnel whenever needed, supporting operational continuity and reliability.**
- **Protection Against Unauthorized Alterations and Breaches: We implement robust controls to protect data from unauthorized access, alteration, or disclosure, preserving its integrity at all times.**
- **Controlled Access to Networks and Assets: Access to networks, systems, and data is granted based on clearly defined roles and responsibilities, and is regularly reviewed to prevent unauthorized use.**
- **Security of Data in Transmission: We apply secure transmission protocols and encryption standards to ensure that data remains protected throughout its lifecycle, particularly during transfers.**
- **Secure Software Development Practices: Our software development lifecycle integrates strict access controls and rigorous testing to prevent vulnerabilities and protect source code and data from exposure.**
- **Maintenance of Information Processing Facilities: We ensure that all information processing facilities are consistently maintained, updated, and secured to support reliable and safe operations.**
- **Timely Incident Reporting and Response: All information security incidents are promptly reported, thoroughly investigated, and resolved in accordance with established procedures to minimize impact and prevent recurrence.**
- **Security in External Providers Relationships: We enforce clear information security requirements and guidelines when engaging with external providers, ensuring our supply chain meets the same high standards of protection.**
- **Clear Communication of Security Policies and Objectives: Our information security policies, objectives, and procedures are clearly documented and communicated to all relevant stakeholders.**
- **Commitment to Continuous Improvement: We adopt a culture of ongoing improvement by regularly reviewing and refining our security goals, practices, and policies in response to internal assessments, technological advancements, and changing risk landscapes.**

CEO

2025

Pioneers of Quality Systems & Certifications

CERTIFICATE

IDS

This is to Certify that the Management System of

Integrated Digital Systems

Bir Hasan, United Nations St., AlZahraa Bldg., Beirut, Lebanon

Has been assessed and found to be in accordance with the management System Requirements { Information Security Management System (ISMS)}

ISO 27001:2022

This certificate is valid for the following scope of operation:

Turnkey Solutions in Information Technology, with a primary focus on Software Engineering.

Certificate No.: **PQS/C05/LBN190525**

Initial Date of Certification:	19-05-2025	1st Surveillance Audits Due on:	19-04-2026
Date of Certificate:	19-05-2025	2nd Surveillance Audits Due on:	19-04-2027
Date of Expiry:	18-05-2028		

This Certificate Remains Valid Subject to Satisfactory Surveillance Audit.

MANAGING DIRECTOR

CERTIFICATION MANAGER

EGAC Accredited

ISMS Certification
CAB # 012103

For Verification & Updated information concerning the present certificate visit to

PQS website:
www.pqscert-eg.com

IAF website:

https://www.iafcertsearch.org

Address: Pioneers of Quality Systems & Certifications Co. LTD
{Egyprt - 17 Ibrahim Al-Sannan St. - Building No.17}
Website:- www.pqscert-eg.com – Email:- info@pqscert-eg.com