Dar recognizes that information security is a critical factor that shall integrate into all aspects of its business and digital capabilities, and is the cornerstone of Dar's stability, survival, and success.

Dar is committed to securing all information assets, especially those entrusted to us through our business relations or those collected through personal data processing activities. In our day to day business operations, security has been fostered by integrating the appropriate safeguards for protecting the confidentiality, privacy, integrity, and availability of physical and information assets for our clients, business partners, employees, and stakeholders.

This commitment to information security is achieved through:

1. Establishing an information security and privacy strategy in alignment with organizational goals and objectives to navigate Dar's information security program;
2. Identifying and prioritizing at-risk corporate information assets and activities, understanding their relevant threats and vulnerabilities and taking the necessary measures to improve their security to definable and acceptable levels;
3. Establishing a secure collaborative workspace to facilitate information sharing while maintaining the efficiency and innovation called for by Dar business requirements;
4. Managing the security of all computing systems and supporting infrastructure through the implementation of appropriate security controls;
5. Securing the adoption of new digital technologies, applications, and processes through the incorporation of "secure by design" principles to drive the digital transformation journey;
6. Educating all Dar members and raising their information security awareness to properly handle information assets and to enable the aspired security-aware culture at Dar;
7. Maintaining the level of competency of our information security and cybersecurity professionals to build the required skill sets to fulfill their security duties and responsibilities;
8. Advancing third-party risk management practices to manage risks related to suppliers, contractors, and consultants and monitor their adherence to information security requirements;
9. Enhancing threat hunting and cybersecurity testing programs to continuously respond to newly dynamic and emerging threats;
10. Implementing corrective and preventive mechanisms to ensure that information security incidents are reported, investigated and responded in a timely manner;
11. Complying with law, regulations, and contractual client requirements related to information security and data protection;
12. Implementing and testing controls to maintain business continuity during crises and disasters; and
13. Assessing the status of the security management system on a regular basis and continuously improving performance by establishing key goal indicators and critical success factors.

Dar security objectives are subject to annual review during our annually held management review meetings, after which the new or revised objectives are communicated throughout the company and, in the case of significant change, incorporated into the scope of business risk management practices.

Our goal is to continually improve our information security management system at Dar in full compliance with the requirements of the international standard ISO/IEC 27001, thus safeguarding all information assets in our trust.

Talal Shair, Chairman

July 2023

"Our vision is to be a secure, resilient, and a risk-managed operating environment capable of executing its missions and delivering its "secure by design" services to its clients within a digital, collaborative, and secure workspace anytime, anywhere, and on par with leading world-class security practices."