Cyber Security Committee Charter

v1.0

Document Control Information

Document Version Control Information				
Version	Date	Author	Reviewer	Approver
1.0	**03 Oct 2024**	Abdulrahman AlJamani	Ahmed Al-Kelani	Misfer Al-Ajmi

Document Change History Information			
Author	Date	Version	Change Description

Contents

1 Purpose 4
2 Membership 4
3 Meetings 4
4 Authority 4
5 Responsibilities and Duties 4

1 Purpose

The Cybersecurity Committee (the “Committee”) is a committee of the Jadarah Legal (the “Company”) Board of Directors (the “Board”). Its purpose is to assist the Board in fulfilling its responsibilities to provide oversight of the Company’s systems (i.e., processes, policies, controls and procedures) to

1. Identify, assess and manage risks related to cybersecurity,
2. Respond to and manage cybersecurity threats, including cybersecurity incidents, and
3. Comply with legal and regulatory requirements governing data security.

2 Membership

The Committee shall consist of at least three (3) members. Members of the Committee shall be appointed, and may be removed, by the Board. The Board shall designate a Committee Chair.

3 Meetings

4. The Committee shall meet at least two times a year, and additionally as appropriate.
5. Members representing 50% or more of the members of the Committee shall constitute a quorum.
6. The Company Secretary or a designate shall be the Secretary of the Committee.
7. Minutes of each meeting and resolutions of Committee meetings shall be taken and kept by the Secretary.
8. The Committee may invite any other individuals to attend meetings of the Committee, as it considers appropriate.
9. The Committee shall have access to professional advice from employees of the Company, and from any external advisers, as the Committee considers appropriate.

4 Authority

The Committee has the authority to retain, set the terms of engagement, and terminate outside advisors, including outside counsel and outside forensic or technical experts, as it deems appropriate, and the Committee has the sole authority to approve related fees and retention terms. The Committee has the authority to form, and to delegate authority to, subcommittees, to the extent it deems appropriate.

5 Responsibilities and Duties

The following shall be the responsibilities and activities of the Committee in carrying out its purpose, including but not limited to:

1. Reviewing with management the status of information technology systems and the Company’s risks relating to information technology, including reviewing the state of the Company’s cybersecurity, emerging cybersecurity developments and threats, and the Company’s strategy to manage cybersecurity risks.
2. Reviewing with management the Company’s cybersecurity incident response plan and program, including escalation protocols with respect to prompt reporting of cybersecurity incidents to management, the Committee and the Board as appropriate.
3. Overseeing the selection, appointment and retention (by the Committee or otherwise) of outside advisors to review the Company’s cybersecurity program and to otherwise support the work of the Committee, as the Committee deems appropriate.

4. Reviewing the plans and methodology for the periodic review and assessment of the Company's cybersecurity program by outside advisors, if applicable.
5. Reviewing with management and outside advisors the findings from reviews, assessments, and audits of the Company's cybersecurity program by outside advisors as well as corresponding remediation plans to address any areas for improvement identified.
6. Reviewing with management the Company's assessment of how its cybersecurity program aligns with industry frameworks and standards.
7. Reviewing with management and reporting to the Board with respect to any significant cybersecurity incident, reports to or from regulators with respect thereto, and root cause and remediation/enhancement efforts with respect thereto.
8. Reviewing and discussing with management the laws and regulations, as well as significant legislative and regulatory developments, that could materially impact the Company's cybersecurity risk exposure, and evaluating the integrity of the Company's information technology systems, processes, policies and controls to maintain compliance.
9. Reviewing and discussing with management the current cybersecurity best practices utilized by the Kingdom of Saudi Arabia (KSA) government and organizations in the Company's industry to assess whether the Company's information technology systems, processes, policies and controls meet benchmark standards.
10. Reviewing the appropriateness and adequacy of the Company's cyber insurance coverage.
11. Reviewing and reporting to the Board with respect to the budget and resources allocated to cybersecurity.
12. Meeting periodically in separate executive session with the Company's Chief Information Security Officer (CISO), and have such other direct and independent interaction with such persons from time to time as the members of the Committee deem appropriate.
13. Reviewing the Committee Charter at least annually and revising it as appropriate.
14. Conducting an annual cyber security program performance and self-evaluation.