# Cyber Security Committee Charter

Issue Date: 22/04/2026

Version: 2.2

**Approved by**

**Chairman**

**Sabah K. AlGhunaim**

شركة شبكة الخدمات الآلية
Automated Services Network Co.

# Contents

**Purpose** ..... 3

**Meetings and Procedures** ..... 3

**Committee Membership** ..... 4

**Meeting Schedule** ..... 4

**Duties and Responsibilities** ..... 4

**Cybersecurity Governance Framework** ..... 5

**Independent Assurance and Testing** ..... 6

**Review** ..... 6

## Purpose

The purpose of the Cybersecurity Committee (the "Committee") of the Board is to enhance its understanding and oversight of the systems (including, processes, policies, controls, and procedures) that management has put in place to:

- Assess, safeguard, and mitigate the Company's key cybersecurity and information technology ("IT") risks against both internal and external threats.
- Ensure systems are adequate to protect against security breach and effectively safeguard the Company's IT infrastructure, assets, intellectual property, development environment, Company data as well as customer and other third-party confidential information in the Company's possession or custody.
- Ensure integrity of security in the Company's products and services that collect, process and/or handle confidential data.
- Develop and monitor the integrity of the Company's IT systems and controls to ensure legal and regulatory compliance over data security.
- Respond to and manage cybersecurity threats, including data breach incidents.

In addition to the powers and responsibilities expressly delegated to the Committee in this Charter, the Committee may exercise any other powers and carry out any other responsibilities delegated to it by the Board from time to time consistent with the Company's bylaws. The powers and responsibilities delegated by the Board to the Committee in this Charter or otherwise shall be exercised and carried out by the Committee as it deems appropriate without requirement of Board approval, and any decision made by the Committee (including any decision to exercise or refrain from exercising any of the powers delegated to the Committee hereunder) shall be at the Committee's sole discretion. While acting within the scope of the powers and responsibilities delegated to it, the Committee shall have and may exercise all the powers and authority of the Board. To the fullest extent permitted by law, the Committee shall have the power to determine which matters are within the scope of the powers and responsibilities delegated to it.

## Meetings and Procedures

The Committee shall have the authority to establish its own rules and procedures for notice and conduct of its meetings so long as they are not inconsistent with any provisions of the Company's bylaws that are applicable to the Committee.

The Committee shall meet on a regularly scheduled basis at least two (2) times per year or more frequently as the Committee deems necessary or desirable. The Chair, in consultation with the other committee members, shall determine the length of the committee meetings and shall set the agendas for Committee meetings.

All non-management directors who are not members of the Committee may attend and observe meetings of the Committee but shall not participate in any discussion or deliberation unless invited to do so by the Committee, and in any event shall not be entitled to vote. The Committee may, at its discretion, include in its meetings members of the Company's management, or any

other person whose presence the Committee believes to be desirable and appropriate. Notwithstanding the foregoing, the Committee may exclude from its meetings any person it deems appropriate other than the members of the Committee, including, but not limited to, any nonmanagement director who is not a member of the Committee.

The Committee may retain any independent counsel, experts or advisors that the Committee believes to be desirable and appropriate, including expert advisors in the field of technology and information security risks. The Committee may also use the services of the Company's regular legal counsel or other advisors to the Company. The Company shall provide for appropriate funding, as determined by the Committee, for payment of compensation to any such persons employed by the Committee and for ordinary administrative expenses of the Committee that are necessary or appropriate in carrying out its duties.

The Chair shall report to the Board regarding the activities of the Committee at appropriate times and as otherwise requested by the Chairperson of the Board.

## Committee Membership

The Committee shall consist of members of the Board along with current members:

- Sabah Al Ghunaim – Chairman
- Lamiaa Al-Kharafi – Member
- Khaled Al Ghunaim - Member
- Jamal Kubeer – General Manager
- Linto Lawrance – Application Support Manager
- Rama – Cyber Security Manager
- ElSayed Thabet – Risk Department

The Board may remove or replace any member at its discretion.

## Meeting Schedule

- The Committee shall meet quarterly (four times per year), with additional meetings scheduled as needed.
- Special meetings may be held by the Chair or at the request of management when urgent cybersecurity matters arise.

## Duties and Responsibilities

- Review with management, at least annually, the Company's assessment of cybersecurity threats and risk, data security programs (including data management systems and controls over company data and systems to protect customer and other third-party data, including confidential information, in our possession or custody), and the Company's management

and mitigation of cybersecurity and information technology risks and potential breach incidents.

- Review with management, at least annually, any major security incidents that have occurred and steps that have been taken to mitigate against reoccurrence.
- Evaluate the effectiveness of the Company's risk management and data security programs measured against the Company's cybersecurity threat landscape, including the following program components: cybersecurity risk monitoring, effectiveness testing, integrity of information security systems and controls and adequacy of resources, security awareness training and cybersecurity insurance coverage.
- Review and discuss with management the regulations, as well as key legislative and regulatory developments, that could materially impact the Company's cybersecurity risk exposure.
- Evaluate the integrity of the Company's information technology systems, processes, policies, and controls to ensure compliance.
- Assess the effectiveness of the Company's data breach incident response plan, including disclosure, investigation, remediation, and post-breach security measures.
- Review and assess the Company's cybersecurity risk systems against industry benchmarks and best practices and make recommendations on enhancements.
- Review the Company's information security planning and resources to manage changes in the Company's cybersecurity threat landscape. Assess the potential impact of cybersecurity risk on the Company's business, operations, and reputation.
- The Committee shall periodically report to the Board on its findings and actions.
- The Committee shall make such recommendations to the Board and management with respect to any of the above and other matters as the Committee deems necessary or appropriate.
- The Committee shall evaluate the Committee's performance and the performance of its members on an annual basis, including the Committee's compliance with this Charter, and provide the Board with any recommendations for changes in procedures or policies governing the Committee. The Committee shall conduct such evaluation and review in such manner as it deems appropriate.
- The Committee shall review and reassess this Charter, including the Committee's purpose and oversight role, at least annually and submit any recommended changes to the Board for its consideration.

## Cybersecurity Governance Framework

The Committee shall oversee the establishment, implementation, and continuous improvement of the Company's cybersecurity governance framework. The framework shall align with recognized international standards and best practices, including but not limited to:

- International Organization for Standardization ISO/IEC 27001
- National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)

- Center for Internet Security CIS Controls

The Committee shall periodically review management's assessment of alignment with these frameworks and oversee initiatives to address identified gaps.

## Independent Assurance and Testing

The Committee shall oversee independent assurance activities, including:

- Internal and external cybersecurity audits
- Vulnerability assessments
- Penetration testing exercises
- Compliance reviews

The Committee shall monitor management's remediation efforts and ensure timely resolution of identified deficiencies.

## Continuous Improvement

The Committee shall promote continuous improvement of the Company's cybersecurity program through periodic maturity assessments, benchmarking against industry best practices, and monitoring of the evolving threat landscape.

## Review

Reviewing the Committee Charter at least annually and revising it as appropriate; and conducting an annual performance self-evaluation.