INFORMATION SECURITY AND PERSONAL DATA MANAGEMENT POLICY

Remed Uluslararası Destek ve Danışmanlık Hiz. Tic. A.Ş. (hereinafter **SpeakHub**) recognizes the critical role of information confidentiality, integrity and availability in the sustainable success of its business processes and appropriate governance practices and understands that failure to ensure adequate information security increases the risk of reputational damage as well as financial losses.

This information security policy sets out the guiding principles and responsibilities which is necessary for safeguarding of information systems, moreover it summarizes **SpeakHub**'s approach to information security management.

SpeakHub management undertakes the establishment, operation, monitoring, maintenance and continuous improvement of the Information Security and Personal Data Management System in accordance with TS ISO/IEC 27001 and ISO/IEC 27701 Standard in order to ensure the confidentiality of the information that it is obliged to protect the integrity and accessibility of the information.

In our company which is providing assistance and business services commits the followings to our shareholders:

- ✓ To follow up current cyber threats related to our activities by using "zero day" approach, to comply contractual conditions and legal requirements which occurred with agreements.

- ✓ To ensure that activities are carried out efficiently, accurately, quickly and safely, To operate activities in accordance with quality standards required by the sector.

- ✓ To carry out our activities in awareness, access privacy, accessibility and by considering integrity risks upon all kinds of information that belongs to our company, customers, employees, suppliers and business partners.

- ✓ To ensure the information security management system and information security awareness are as corporate culture.

- ✓ To ensure necessary plans are prepared, implemented and tested in order to provide business and service continuity.

- ✓ To provide assessment of risks which are against our information assets and processes in accordance with the generally accepted risk management methodologies.

- ✓ To communicate with special interest groups with the purpose of making benefit from developing technologies and knowledge in information based sector that we are servicing.