INFORMATION SECURITY POLICY

The main theme of ISO 27001 Information Security Management System; Siberson Bilişim Güvenliği A.Ş to demonstrate that information security management is provided within human, infrastructure, software, hardware, user information, organizational information, third party information and financial resources, to ensure risk management, to measure information security management process performance and to ensure information security. To ensure the regulation of relations with third parties on relevant matters.

In this regard, the purpose of our **ISMS Policy** is;

- To protect the information assets of Siberson Bilişim Güvenliği A.Ş against all kinds of threats that may occur from inside or outside, knowingly or unknowingly, to ensure accessibility of information as required through business processes, to meet legal legislation requirements, to work for continuous improvement,
- To prevent unauthorized or unauthorized access, use, modification, disclosure, elimination, change of hands and damage to information assets made available for use, based on confidentiality, integrity and accessibility as the basic elements of information security,
- Information security assets include not only data held electronically; to deal with the security of all data in written, printed, oral and similar media,
- To undertake the necessary work to ensure the privacy and confidentiality of all persons' data within the framework of the law,
- To raise awareness by providing Information Security Management and KVKK /GDPR training to all personnel,
- To ensure that the personnel of the institution have a conscious approach to information security and fulfill their duties within their areas of responsibility, and pay utmost attention to the published policies, procedures, instructions and announcements,
- Evaluating all existing or suspicious vulnerabilities targeting Information Security within the scope of information security incident management and, as a result of the evaluations, ensuring that the activities of updating existing controls or commissioning new controls are carried out as soon as possible,
- To prepare, maintain and test business continuity plans,
- To identify current risks by making periodic evaluations on Information Security; As a result of evaluations, to review and follow up action plans,
- To ensure that the studies that support the objectives in our Information Security Policy are included in the Information Security Targets established every year and that the progress of these studies is monitored and reported throughout the year,
- To ensure continuous improvement of the Information Security Management System and to ensure that efforts for continuous improvement are reviewed by the management.

Gökhan MANAV – CEO

01.03.2022