BİLGİ SİSTEMLERİ ve GÜVENLİĞİ POLİTİKASI

SANMAR olarak,

Faaliyetlerimizin sağlıklı bir şekilde yürütmek, müşterilerimizin ve çalışanlarımızın bilgi güvenliğini sağlamak ve bilgi sistemlerinin verimli kullanımını temin etmek amacıyla bilgi güvenliği ve bilgi sistemleri yönetimine büyük önem veririz.
Bu doğrultuda, aşağıdaki ilkeleri taahhüt ederiz:

Bilgi Sistemleri Yönetimine Stratejik Destek

Bilgi sistemlerinin organizasyonel stratejilere ve hedeflere katkı sağladığından emin olmak için bilgi sistemleri yönetimini kurumsal hedeflerle uyumlu hale getirmeyi, bilgi sistemlerinin etkin yönetimi ve optimizasyonu için gerekli teknolojik yatırımları ve kaynakları sağlamayı, çalışanlarımızın iş akışlarını daha verimli hale getirmek amacıyla, bilgi sistemleriyle etkileşimlerini artıracak teknolojik ortamı sürekli olarak geliştirmeyi.

Sürekli İyileştirme, Denetim, Eğitim ve Farkındalık

Bilgi güvenliği ve bilgi sistemleri yönetiminin sürekli olarak izlenmesi, denetlenmesi ve iyileştirilmesi amacıyla iç ve dış denetimler gerçekleştirmeyi, iyileştirme fırsatlarını değerlendirecek ve süreçlerimizi sürekli olarak geliştirerek güvenliği artırmayı, tüm çalışanlarımızın, bilgi güvenliği ve bilgi sistemleri yönetimi konularında farkındalık kazanması ve yetkinliklerini artırması için düzenli eğitimler ve farkındalık programları düzenlemeyi.

Bilgi Güvenliği Yönetim Sistemi (BGYS) Uygulama ve İyileştirme

Bilgi güvenliği politikalarımızı, ISO 27001 Bilgi Güvenliği Yönetim Sistemi gibi uluslararası standartlara uygun olarak oluşturmayı, uygulamayı ve sürekli iyileştirmeyi. Bu doğrultuda, risk yönetimi süreçlerini uygulayarak bilgi varlıklarımızı koruyacak tedbirleri almayı.

Yasal Uyumlulukların Sağlanması

Bilgi sistemlerimizin ve tüm bilgi işleme faaliyetlerinin yürürlükteki yerel ve uluslararası yasalara (örneğin, Kişisel Verilerin Korunması Kanunu - KVKK) tam uyum içinde olmasını sağlayacak önlemleri almayı, yasal gerekliliklere uyum için gerekli olan süreçleri ve eğitimleri sağlamayı.

Risk Yönetimi ve Güvenlik Önlemleri

Bilgi sistemlerimizdeki tüm varlıkların ve süreçlerin risk değerlendirmesi yapılarak, uygun teknik ve idari güvenlik önlemlerinin alınmasını sağlamayı. Riskleri minimize etmek için stratejik ve operasyonel düzeyde proaktif önlemler alarak, olası tehditleri önlemeye yönelik çalışmalar yapmayı.

Yukarıda belirtilen odaklar doğrultusunda bilgi güvenliği ve bilgi sistemleri politikalarımıza uygun şekilde hareket etmeyi, tüm bilgi varlıklarımızı ve paydaşlarımızın bilgilerinin güvenliğini korumayı, bilgi sistemlerimizin verimliliğini arttırmak ve gelişen teknolojililere ayak uydurmak için sürekli iyileştirmeler yapmayı taahhüt ederiz.

INFORMATION SYSTEMS AND SECURITY POLICY

As SANMAR,

We assign great emphasis on information security and information systems management to ensure that our activities are conducted in a healthy manner, to safeguard the information security of our customers and employees, and to ensure the effective use of information systems. In this regard, we make the following commitments:

Strategic Support for Information Systems Management

Aligning information systems management with corporate objectives to ensure that information systems contribute to organizational strategies and goals, providing the necessary technological investments and resources for the effective management and optimization of information systems, and continuously enhancing the technological environment to increase our employees' interactions with information systems, making their workflows more efficient.

Continuous Improvement, Auditing, Training, and Awareness

Conducting internal and external audits to continuously monitor, audit, and improve information security and information systems management, evaluating improvement opportunities to enhance security by continually developing our processes, and organizing regular training and awareness programs to ensure that all our employees gain awareness and competence in information security and information systems management.

Information Security Management System (ISMS) Implementation and Improvement

Establishing, implementing, and continuously improving our information security policies in accordance with international standards such as ISO 27001 Information Security Management System. In this context, we promise to take measures to protect our information assets by implementing risk management practices.

Ensuring Legal Compliance

Taking necessary measures to ensure that our information systems and all information processing activities are fully compliant with applicable local and international laws (such as the Personal Data Protection Law - KVKK) and to providing the processes and training required for compliance with legal requirements.

Risk Management and Security Measures

Conducting risk assessments for all assets and processes within our information systems to ensure that appropriate technical and administrative security measures are in place. We pledge to proactively take strategic and operational measures to minimize risks and work on preventing potential threats.

We undertake to act in accordance with the commitments mentioned above, to protect the security of all our information assets and our stakeholders' information, and to continuously improve our information systems to enhance efficiency and keep pace with emerging technologies.

January / Ocak 2012 (Rev: 300318)

Ali GÜRÜN | Cem SEVEN