BİLGİ GÜVENLİĞİ POLİTİKASI

FICOSA International Otomotiv Sanayi ve Ticaret A.Ş. olarak, tüm çalışanları ve ilgili hizmet sağlayıcıları ile birlikte kurum bilgi varlıklarına yönelik risklerin etkin bir şekilde yönetilebilmesi amacıyla bu politika dokümanı hazırlanmıştır. Bilgi Güvenliği'nin ve bu politikanın amacı, Ficosa' ya ait bilgi varlıklarının yetkili kişilerde kalmasının ve "**Bilgi Varlıklarının Gizlilik, Bütünlük Ve Erişilebilirlik"** mevcudiyetinin sağlanmasıdır. Bu amaçla aşağıdaki unsurların sürekli ve en iyi seviyede uygulanmasını amaçlamaktayız. FICOSA International Üst Yönetimi, bu politikanın kurum genelinde uygulanmasının takipçisi olacağını taahhüt etmektedir.

- Şirketimiz güvenirliğini ve temsil ettiği grubun imajının korunmasını sağlamak.
- Temel ve destekleyici iş faaliyetlerinin en az kesinti ile devam etmesini sağlanmak.
- Bilgi güvenliği ile ilgili tüm yasal mevzuat ve sözleşmelere uyulmasını sağlamak.
- Bilgi varlıklarına ve işletme süreçlerine yönelik risklerin sistematik olarak yönetilmesini sağlamak.
- Şirketimiz iç ve dış bağlamını oluşturan taraflar için bilgi güvenliği bilincini oluşturmak ve ilgili yükümlülüklerini aktarmak.
- Bilgi güvenliği farkındalığını artırmak amacıyla teknik ve davranışsal yetkinlikleri geliştirecek eğitimlerin gerçekleştirilmesini sağlamak.
- Kişisel verilerin korunmasını sağlanmak.
- Programları, verileri, iletişim ağını ve ekipmanları (donanım) kayıplara, yetkisiz kullanıma ve suiistimallere karşı koruma altına almak.
- Tüm kullanıcıların bilgi güvenliği politikası ve ilgili destekleyici prosedürlere, talimatlara bütünüyle uymalarını ve farkında olmalarını sağlamak.
- Kurumun bilgi güvenliğine olan bakışını vurgulamak ve detaylandırmak, Üst Yönetim'in kurumda bilgi güvenliği oluşumuna verdiği önemi ve desteği ifade etmek.
- Kurum Bilgi Varlığı politikasının sürekli iyileştirilmesini sağlamak
- Tedarik edilen tüm ürünlerin siber güvenliğini sağlamak. Tasarım, üretim ve teslimat sonrası aşamalar dahil olmak üzere ürün yaşam döngüsü boyunca ürünleri, sistemleri ve müşterileri potansiyel siber tehditlerden, yetkisiz erişimden ve veri ihlallerinden korumak.

  Politika, küresel güvenlik standartları ve düzenlemeleriyle (ör. UN ECE R155 ve ISO21434:2021 Karayolu Taşıtları – Siber Güvenlik Mühendisliği) uyumludur.

Levent Cansu
Ülke Genel Direktörü

12.12.2024_Ed02

INFORMATION SECURITY POLICY

This policy document has been prepared by Ficosa International Otomotiv A.Ş. to manage risks associated with corporate information assets effectively with all employees and related service providers. The objective of Information Security and this policy is to ensure that the information assets of Ficosa remain in the authorized persons and **"Confidentiality, Integrity and Availability of Information Assets"** are provided. For this purpose, we aim to apply the following facts in a continuous and optimal way. Ficosa Top management is committed to ensure that this policy is followed throughout the company.

- To ensure the reliability of our company and the image of the group it represents.
- To ensure that basic and supportive business activities continue with minimum interruption.
- Ensure compliance with all legal regulations and contracts related to information security.
- To manage the risks related to information assets and business processes systematically.
- To establish information security awareness and inform related parties about information security obligations according to the internal and external context of our company.
- To provide trainings aimed to increase the awareness of information security in order to improve technical and behavioral competencies.
- To provide the protection of the personal data.
- To protect the programs, data, communication network and equipments (hardware) against the loss, unauthorized use and abuse.
- To provide that all users are fully aware of and comply with the information security policy and relevant supportive procedures and instructions.
- To demonstrate the support of Top Management to information security and its importance to the company in all aspects.
- To ensure continuous improvement of the corporate information asset policy.
- To ensure the cyber security of all supplied products. Protecting products, systems and customers from potential cyber threats, unauthorized access and data breaches throughout the product lifecycle, including design, manufacturing and post-delivery phases.

  The policy is aligned with global safety standards and regulations (i.e., UN ECE R155 and ISO21434:2021 Road Vehicles – Cybersecurity Engineering).

Levent Cansu
Country General Director

12.12.2024_Ed02