INFORMATION SECUTIRY POLICY

As Green Transfo Energy Turkey, we believe that securing information security is an absolute necessity in order to ensure the satisfaction of all our stakeholders, to continuously improve the effectiveness of our business processes and to achieve our strategic goals.

In this direction, in order to ensure the continuous development of our information security management system within our organization, we are committed to;

- **Identify information assets and ensure that these assets,**
  - **Business impact:** by addressing issues such as the cost of replacing the asset, the confidentiality of the information, its impact on image, and the damage it may cause in terms of legal and legal obligations,
  - **Considering the likelihood of a threat:** the multiplicity of weaknesses and the extent to which existing controls can close those weaknesses, attacker motivation, the attractiveness of the information to adversaries, gaps in access controls, and threats to the integrity of the information,
- **Identify and assess risks related to confidentiality, integrity and access to information,**
- **Implement necessary controls for all assets above the acceptable level,**
- **To measure the performance of information security processes,**
- **To generate targets from this data,**
- **To minimize our weaknesses and threats through investments in infrastructure, working environment, hardware, software and training,**
- **To meet the security requirements of our business, our customers and legal requirements,**

Abhilash MISHRA
Plant Director

BİLGİ GÜVENLİĞİ POLİTİKASI

Green Transfo Energy Turkey olarak tüm paydaşlarımızın memnuniyetini sağlamak, iş süreçlerimizin etkinliğini sürekli iyileştirmek ve stratejik hedeflerimize ulaşmak amacıyla bilgi güvenliğinin güvence altına alınmasının mutlak gereklilik olduğunu düşünüyoruz.

Bu doğrultuda, kuruluşumuz bünyesinde bulunan Bilgi güvenliği yönetim sistemimizin sürekli gelişimini sağlamak için:

- **Bilgi varlıklarını tanımlamayı bu varlıkların,**
  - **İşe etkisini:** varlığı yerine koyma maliyeti, bilginin gizliliği, imaja olan etkisi, yasal ve hukuki yükümlülükler bakımından yaratacağı zararı gibi konuları ele alarak,
  - **Tehdit olasılığını:** zayıflıkların çokluğu ve var olan kontrollerin bu zayıflıkları ne kadar kapatabildiği, saldırgan motivasyonu, bilginin rakipler için cazibesi, erişim kontrollerindeki açıklar ve bilginin bütünlüğüne ilişkin tehlikeleri ele alarak,
- **Bilginin gizliliği, bütünlüğü ve erişimine ilişkin riskleri belirlemeyi, değerlendirmeyi,**
- **Kabul edilebilir seviyenin üzerinde bulunan tüm varlıklar için gerekli kontrolleri uygulamayı,**
- **Bilgi güvenliği süreçlerinin performansını ölçmeyi,**
- **Bu verilerden hedefler üretmeyi,**
- **Zayıflıklarımızı ve tehditleri alt yapı, çalışma ortamı, donanım, yazılım ve eğitim yatırımlarıyla en aza indirgemeyi,**
- **İşimizin, müşterilerimizin ve yasal şartların gerektirdiği güvenlik şartlarını karşılamayı,**

Taahhüt ederiz.

Abhilash MISHRA

Fabrika Direktörü