DOF ROBOTİK SANAYİ A.Ş.
BİLGİ GÜVENLİĞİ POLİTİKASI

Amaç:

DOF ROBOTİK SANAYİ A.Ş. ("Şirket") olarak bilgi sistemlerinin ve varlıkların gizliliği, bütünlüğü ve erişilebilirliğini sağlamak amacıyla, tabi olunan tüm mevzuat, sözleşme ve standartlara uygun şekilde bilgi güvenliği faaliyetlerinin tanımlanmasıdır.

1. **Bilgi Güvenliğinin Sağlanması**

- Tüm bilgilerin doğru ve tam olmasını sağlamak, bilgi hatalarını ve eksikliklerini aza indirgemek için sürekli kontroller yapmayı,
- Bilgilerin gizliliğini sağlamak için yetkisiz erişimlere karşı önlemler almayı,
- Verilerin bütünlüğünü ve sürdürülebilirliğini yedekleme ve güvenli depolama ile korumayı,
- Bilgilere sadece yetkili kişilerin erişebilmesini sağlamaktır.

2. **Bilgi Güvenliği Risk Yönetimi**

- Bilgi güvenliği risklerinin sistematik biçimde belirlenmesi, değerlendirilmesi ve yönetilmesi,
- Kabul edilebilir risk seviyeleri için sürekli iyileştirme süreçlerinin yürütülmesi,
- Tehdit ve zafiyetlere karşı uygun tedbirlerin önceden alınmasıdır.

3. **Kaynakların Tahsisi ve Yetki Dağılımı**

- Yeterli insan kaynağı, teknoloji ve finansman ayırarak bilgi güvenliğinin desteklenmesi,
- Bilgi güvenliğiyle ilgili yetki ve sorumlulukların açıkça belirtilmesidir.

4. **İş Sürekliliği ve İhlal Yönetimi**

- Olası kesintilere karşı iş sürekliliği planlarının hazırlanması ve test edilmesi,
- Bilgi güvenliği ihlallerini yönetmek için etkin sistemler kurularak, düzeltici/önleyici tedbirler alınmasıdır.

5. **Servis Yönetimi**

- Hizmet kalitesini ve güvenliğinin izlenip iyileştirilmesi,
- Servis kesintilerinin minimize edilip, kurtarma planları geliştirilmesi,
- Müşteri geri bildirimlerinin dikkate alınarak süreçlerin iyileştirilmesidir.

6. **Mevzuat ve Sözleşmelere Uyum**

- Tüm yasal ve sözleşmesel yükümlülüklere uyulması,
- Müşteri ve tedarikçi sözleşmelerindeki bilgi güvenliği maddelerine tam uyumun sağlanmasıdır.

7. **Güncel İş Plan ve Prosedürler**

- Plan ve prosedürlerin düzenli gözden geçirilip güncellenmesidir.

8. **Güvenli İş Ortamı**

- Fiziksel ve dijital ortamda güvenliğin sağlanıp, farkındalığın artırılmasıdır.

9. **Bilgi Güvenliği Eğitimi**

- Tüm çalışanlara ve paydaşlara düzenli bilgi güvenliği eğitiminin verilmesidir.

10. **Denetimler ve Uyum**

- İç ve dış denetimler ile politika uygunluğunun sürekli kontrol edilmesi,
- Uygunsuzluklara yönelik düzeltici faaliyetlerin planlanmasıdır.

11. **Sürekli İyileştirme**

Yeni tehditlere karşı sürekli iyileştirmelerin yapılarak, Entegre Yönetim Sistemi'nin geliştirilmesi ve güncel tutulmasıdır.