BİLGİ GÜVENLİĞİ POLİTİKASI

1. AMAÇ

USB Certification'ın tüm hizmetlerinde insan, alt yapı, yazılım, donanım, müşteri bilgileri, kuruluş bilgileri, üçüncü şahıslara ait bilgiler ve finansal kaynaklar içerisinde bilgi güvenliği yönetiminin sağlandığını göstermek, risk yönetimini güvence altına almak, bilgi güvenliği yönetimi süreç performansını ölçmek ve bilgi güvenliği ile ilgili konularda üçüncü taraflarla olan ilişkilerin düzenlenmesini sağlamaktır.

2. KAPSAM

USB Certification bünyesinde yürütülen tüm hizmetlerde bilgi güvenliği gerekliliklerinin işbu politika çerçevesinde eksiksiz yürütülmesine ilişkin usul ve esasları kapsar.

3. SORUMLULAR

3.1. Genel Müdür

İşbu Politikanın onaylanmasından sorumludur.

3.2. Bilgi Güvenliği Yöneticisi

İşbu Politikanın ön onayından ve ihtiyaç halinde güncellenmesinden ve politikada belirtilen tüm esasların eksiksiz yürütülmesinden sorumludur.

3.3. Bilgi Teknolojileri ve Altyapı Uzmanı / Uzman Yardımcısı

İşbu Politikada belirtilen tüm esasların uygulanmasından, eksiksiz yürütülmesinden ve Bilgi Güvenliği Yönetici'ne destek olmaktan sorumludur.

3.4. Tüm Çalışanlar

Bu politikanın işleyişinden tüm USB Certification çalışanları ve dış denetçileri sorumludur.

4. UYGULAMA

BGYS Politikamızın amacı;

- İçeriden veya dışarıdan, bilerek ya da bilmeyerek meydana gelebilecek her türlü tehdide karşı USB Certification' nin bilgi varlıklarını korumak, bilgiye erişilebilirliği iş prosesleriyle gerektiği şekilde sağlamak, yasal mevzuat gereksinimlerini karşılamak,
- Yürütülen tüm faaliyetlerde Bilgi Güvenliği Yönetim Sisteminin üç temel öğesinin sürekliliğini sağlamak.

Gizlilik : Önem taşıyan bilgilere yetkisiz erişimlerin önlenmesi,
Bütünlük : Bilginin doğruluk ve bütünlüğünün sağlandığının gösterilmesi,
Erişebilirlik : Yetkisi olanların gerektiği hallerde bilgiye ulaşılabilirliğinin gösterilmesi,

- Sadece elektronik ortamda tutulan verilerin değil; yazılı, basılı, sözlü ve benzeri ortamda bulunan tüm verilerin bilgi güvenliği ile ilgilenmek.
- Bilgi Güvenliği Yönetimi eğitimlerini tüm personele her yıl, yeni giren personele iş başı itibariyle vererek bilinçlendirmeyi sağlamak.
- Bilgi Güvenliğindeki gerçekte var olan veya şüphe uyandıran tüm açıkların, Bilgi Güvenliği Yöneticisine eposta kanalı aracılığı ile rapor etmek Bilgi Güvenliği Yöneticisi tarafından soruşturulmasını sağlamak.
- İş süreklilik planları hazırlamak, Genel Müdür onayına sunmak ve onaylı iş planlarını yıllık olarak gözden geçirmek ve iş planlarını bu doğrultuda sürdürmek ve test etmek.
- Bilgi Güvenliği konusunda her yıl mevcut riskler için risk analizi yapmak ve Genel Müdür onayına sunmak, periyodik olarak değerlendirmeler ile mevcut riskleri tespit etmek. Değerlendirmeler sonucunda, aksiyon planlarını gözden geçirmek ve takibini yapmak ve Genel Müdür'e raporlamak.