

BGYS Politikamız

Bilgi Güvenliği Yönetim Sistemi (BGYS) çerçevesinde, kurumumuzun bilgi varlıklarının gizlilik, bütünlük ve erişilebilirlik prensiplerini korumaya yönelik stratejik ve operasyonel süreçleri ayrıntılı olarak tanımlamaktayız. Bu kapsamda;

- **Kapsam ve Hedefler:** Tüm kurum içi süreçler, altyapı, veri işleme ve iletişim kanallarımızın güvenliğinin sağlanması hedeflenmektedir.
- **Risk Yönetimi:** Tanımlanan risklere karşı düzenli risk değerlendirme süreçleri yürütülmekte, risklerin kabul edilebilir seviyeye indirilmesi için kontroller uygulanmaktadır.
- **Sorumluluklar ve Roller:** Üst yönetimden başlayarak tüm çalışanların bilgi güvenliği konusundaki sorumlulukları detaylandırılmıştır. Bu bağlamda, bilgi güvenliği komitesi, BT yöneticileri ve çalışanlar için görev tanımları belirlenmiştir.
- **Eğitim ve Farkındalık:** Düzenli bilgi güvenliği farkındalık eğitimleri, seminerler ve güncellemelerle tüm personelin bilinçlendirilmesi sağlanmaktadır.
- **İzleme ve Sürekli İyileştirme:** Performans göstergeleri, iç denetimler ve düzenli revizyonlarla sistemin etkinliği sürekli izlenmekte ve iyileştirme faaliyetleri uygulanmaktadır.
- **Yasal ve Düzenleyici Uyumluluk:** Mevcut yasa, yönetmelik ve sektörel standartlarla uyum sağlanarak, kurumumuzun yasal yükümlülüklerini yerine getirmesi hedeflenmektedir.

Çerez Politikamız

Web sitemizde, kullanıcı deneyimini optimize etmek ve hizmetlerimizi geliştirmek amacıyla çeşitli çerez türleri kullanılmaktadır. Detaylar;

- **Çerez Tanımı:** Çerezler, web sitesinin işlevselliğini artıran, kullanıcı tercihlerini hatırlayarak kişiselleştirme sağlayan küçük veri dosyalarıdır.
- **Kullanım Amaçları:** Oturum yönetimi, site analitiği, reklam ve içerik kişiselleştirme gibi alanlarda çerezler aracılığıyla veri toplanmaktadır.
- **Çerez Türleri:**
 - *Oturum Çerezleri:* Kullanıcıların geçici oturum bilgilerini saklar.
 - *Kalıcı Çerezler:* Kullanıcı tercihlerini ve site ayarlarını belirli bir süre saklar.
 - *Üçüncü Parti Çerezleri:* İş ortaklarımız tarafından, reklam ve analiz hizmetleri sağlamak amacıyla kullanılmaktadır.
- **Kullanıcı Hakları:** Kullanıcılar, tarayıcı ayarları üzerinden çerezlerin kabulünü reddedebilir veya var olan çerezleri silebilir. Ancak, bu durumun bazı hizmetlerin kısıtlanmasına neden olabileceği belirtilmektedir.
- **Gizlilik ve Güvenlik:** Toplanan veriler, kişisel verilerin korunması yasaları çerçevesinde işlenmekte ve güvenlik önlemleriyle korunmaktadır.

Temiz Masa Temiz Ekran Politikamız

Bilgi güvenliğinin fiziki unsurlarını desteklemek amacıyla geliştirilmiş olan bu politika, çalışma alanlarında hassas bilgilerin korunmasını hedeflemektedir.

- **Amaç:** Çalışma ortamlarında, hassas belgelerin, notların ve dijital ekranlarda gösterilen bilgilerin yetkisiz kişilerin erişimine kapalı tutulmasını sağlamak.
- **Uygulama Prensipleri:**
 - Çalışma bitiminde masa üzerindeki belgelerin düzenli olarak kilitli dolaplarda saklanması veya imha edilmesi.
 - Bilgisayar ekranlarının, çalışma ortamında veya ortak alanlarda izinsiz bakışlara karşı korunması amacıyla ekran kilitleme (otomatik ekran koruyucu) ayarlarının etkinleştirilmesi.
 - Fiziki ortamın düzenli kontrolü ve güvenlik kameraları gibi ek önlemlerle desteklenmesi.
- **Farkındalık ve Eğitim:** Personelimize düzenli aralıklarla bu politikanın önemi ve uygulanması hakkında eğitimler verilmekte, denetimler ve hatırlatmalarla sürekli kontrol edilmektedir.

Kriptoloji Politikamız

Bilgi varlıklarımızın korunmasında temel rol oynayan kriptografi uygulamaları, veri şifreleme ve dijital imza yöntemleriyle desteklenmektedir.

- **Kullanılan Teknolojiler:**
 - Endüstri standartlarına uygun simetrik (AES gibi) ve asimetrik (RSA, ECC gibi) şifreleme algoritmaları kullanılmaktadır.
 - Dijital imza uygulamalarıyla veri bütünlüğü ve doğruluk sağlanmaktadır.
- **Anahtar Yönetimi:**
 - Şifreleme anahtarlarının oluşturulması, saklanması, dağıtımı ve imhası için belirlenmiş prosedürler uygulanmaktadır.
 - Anahtarların düzenli olarak yenilenmesi ve güvenli saklanması için merkezi bir yönetim sistemi kurulmuştur.
- **Politika Kapsamı:**
 - Verilerin aktarım aşamasında, depolama sırasında ve işlem esnasında şifreleme teknikleri uygulanarak veri güvenliği sağlanmaktadır.
 - Kritik sistemlerde, verilerin yetkisiz erişime karşı korunması için ek önlemler alınmaktadır.
- **Uyum ve Süreklilik:** Kriptoloji uygulamaları, teknolojik gelişmeler ve uluslararası standartlar doğrultusunda periyodik olarak gözden geçirilmekte ve güncellenmektedir.

Uzaktan Çalışma Politikamız

Uzaktan çalışma modelinde, bilgi güvenliğinin en üst düzeyde sağlanabilmesi için kapsamlı önlemler uygulanmaktadır.

- **Erişim Güvenliği:**
 - Çalışanlarımız, şirket ağına güvenli erişim sağlamak amacıyla zorunlu VPN bağlantısı kullanmaktadır.
 - Çok faktörlü kimlik doğrulama (MFA) gibi ek güvenlik katmanları uygulanmaktadır.
- **Cihaz ve Yazılım Güvenliği:**
 - Kişisel bilgisayarlar ve mobil cihazlar, antivirüs yazılımları, güvenlik duvarları ve düzenli güncellemelerle korunmaktadır.
 - Uzaktan erişimde kullanılan cihazların, şirket politikalarına uygun olarak yapılandırılması ve düzenli olarak denetlenmesi sağlanmaktadır.
- **Veri Yönetimi:**
 - Verilerin, bulut veya uzaktan sunucularda şifreli olarak depolanması ve aktarılması sağlanmaktadır.
 - Kritik verilerin yerel cihazlarda tutulmaması, bulut tabanlı ve güvenli depolama çözümlerinin tercih edilmesi teşvik edilmektedir.
- **Fiziki Güvenlik:**
 - Çalışanların ev ofislerinde dahi gizlilik prensiplerine uygun bir çalışma ortamı oluşturmaları beklenmektedir.
 - Uzaktan çalışmada, masa ve ekran güvenliğine ilişkin ek hatırlatmalar ve yönergeler düzenli olarak paylaşılmaktadır.
- **Eğitim ve Destek:**
 - Uzaktan çalışma ile ilgili olarak çalışanlarımıza bilgi güvenliği farkındalığı eğitimi verilmekte, teknik destek ve danışmanlık hizmetleri sağlanmaktadır.

Onay ve Yayın Bilgileri

Bu politikalar, kurumumuzun bilgi güvenliği stratejisini desteklemek amacıyla detaylandırılmış olup, ilgili tarih ve yetkili onaylarla yürürlüğe girmiştir:

Onay: Mehmet Can Demirel

Onay Tarihi: 30.06.2024

Yayın Tarihi: 30.06.2024

Kurum içindeki düzenli denetim ve revizyon süreçleri çerçevesinde, bu politikaların gerektiğinde güncellenmesi ve iyileştirilmesi sağlanmaktadır. Her politika, ilgili mevzuat ve standartlara uygunluğu garanti altına almak için periyodik olarak gözden geçirilmektedir.