BGYS POLİTİKASI

Politika Numarası	PLTK-22
Politika Tanımı	Ekipman Konumlandırma ve Koruma Politikası
Amaç ve İlkeler	Şirketimiz, ekipmanların güvenli bir şekilde konumlandırılması ve korunmasını sağlamak için bu politikayı oluşturmuştur. Çevresel ve fiziksel tehditlere karşı direncimizi artırmak amaçlanmaktadır.
Sorumluluklar	**Bilgi İşlem Personeli:** Politika dışı davranılmasının engellenmesi amacıyla sistem kurulması ve kurulan sistemin denetlenmesinden sorumludur. **Tüm çalışanlar:** Belirlenen politika ve prosedürlere uymakla yükümlüdür.
Sapma ve Özel Durumlar	Politika dışı durumlar veya özel durumlarla karşılaşılırsa, çalışanlar durumu hemen ilgili departmana bildirir. İhlaller incelenir, gerekli önlemler alınır ve uygun cezai yaptırımlar uygulanır.

UYGULAMA

"Ekipman," genel olarak kullanıldığında, bir işi yapma veya bir görevi yerine getirme amaçlı olarak kullanılan araçları, makineleri, cihazları ve diğer fiziksel varlıkları ifade etmektedir. Bu bağlamda, iş süreçlerini yürütmek veya belirli bir görevi tamamlamak için kullanılan her türlü malzeme, araç veya makine ekipman olarak adlandırılabilir. Örnek olarak, bilgisayarlar, yazıcılar, üretim makineleri, araçlar, mobilya ve diğer benzeri nesneler ekipman kategorisine dahil edilebilir.

Çalışma alanlarında ekipmanlar, gereksiz erişimi en aza indirmek ve yetkisiz erişimi önlemek amacıyla belirlenmiş güvenli bölgelere yerleştirilmelidir. Özellikle hassas veya kritik ekipmanlar, sadece yetkilendirilmiş personel tarafından erişilebilecek güvenli bölgelere yerleştirilmelidir.

Hassas verileri işleyen bilgi işleme tesislerinin dikkatli bir şekilde konumlandırılması, şirketimizin güvenlik politikaları doğrultusunda alınan önlemler arasında yer almaktadır. Bu konudaki uygulamalar aşağıdaki gibidir:

- **Fiziksel Güvenlik Kontrolleri:** Hassas verilerin işlendiği bilgi işleme tesisleri, fiziksel güvenlik kontrollere tabi tutulmalıdır. Bu, sınırlı erişim, izinsiz girişi önleme ve yetkisiz kişilerin bu alanlara girmesini engelleme amacını taşımaktadır.
- **Erişim Kontrolleri**: Bilgi işleme tesislerine erişim, sadece ilgili personel için yetkilendirilmeli, gereksiz kişilerin bu alanlara girmesi önlenmelidir. Yetkisiz erişimi engellemek ve gözetim sağlamak adına güvenlik kameraları ve giriş kontrol sistemleri kullanılmalıdır.
- **Konum Seçimi:** Hassas verilerin işlendiği tesisler, olası tehditlere karşı dikkatli bir şekilde konumlandırılmalıdır. Özellikle dışarıdan görünmeyen veya erişimi zor bölgeler tercih edilmelidir.
- **Güvenlik Politikaları ve Eğitim**: Çalışanlar, hassas verilerin işlendiği alanlarda görev yaptıklarında güvenlik politikalarına uymakla yükümlüdürler. Ayrıca, düzenli güvenlik eğitimleri ile bilgi işleme tesislerindeki güvenlik önemleri vurgulanmalıdır.
- **Teknolojik Çözümler:** Bilgi işleme tesislerinde kullanılan teknolojik çözümlerle, yetkisiz erişimi ve bilgi güvenliği risklerini minimize etmeye yönelik ek önlemler alınmalıdır.

Potansiyel fiziksel ve çevresel tehdit riskini en aza indirmek için şu kontroller gerçekleştirilmelidir;

- **Hırsızlık Kontrolleri:** Tesislerde güvenlik personeli, güvenlik kameraları ve alarm sistemleri gibi önlemlerle hırsızlık riskini en aza indirilmelidir. Kontrollü erişim ve izleme, hırsızlık durumunda hızlı müdahaleyi sağlamak adına kullanılır.

YAYIMLANMA TARİHİ	REVİZYON NO/TARİHİ	HAZIRLAYAN	ONAYLAYAN
02.02.2024	-	Mehmet YALÇIN BGYS Temsilcisi	Yusuf KAYA Genel Müdür Yardımcısı

- **Yangın Kontrolleri:** Yangın riskini azaltmak için yangın söndürme sistemleri, yangın dedektörleri ve yangın eğitimleri gibi kontroller uygulanmalıdır. Tesislerde yangın çıkması durumunda hızlı müdahale ve güvenli tahliye sağlanmalıdır.
- **Su ve Su Kaynağı Arızası Kontrolleri**: Su kaynaklı risklere karşı, tesislerimizde su baskını dedektörleri kullanılmalıdır.
- **Elektrik Kaynağı Paraziti Kontrolleri:** Güç düzenleme sistemleri ve dalgalanma korumalı ekipmanlar kullanılmalıdır.
- **İletişim Girişimi Kontrolleri**: Elektromanyetik radyasyon ve iletişim girişimine karşı koruma önlemleri alınmalıdır. Özellikle hassas elektronik sistemlerin bulunduğu alanlarda, bu tür etkileri minimize etmeye yönelik teknik kontroller uygulanmalıdır.
- **Vandalizm Kontrolleri**: Tesislerde güvenlik kameraları ve aydınlatma sistemleri gibi önlemlerle vandalizm riski azaltılmalıdır. Alanların düzenli olarak kontrol edilmesi ve güvenlik personeli tarafından izlenmesi, potansiyel vandalizm olaylarına karşı etkili bir koruma sağlar.

Bilgi işleme tesislerinin olumsuz etkilenebileceği çevresel koşulları izlemek ve kontrol etmek amacıyla gerçekleştirilecek çalışmalar;

- **Çevresel İzleme Sistemleri:** Bilgi işleme tesislerinde, sıcaklık, nem ve benzeri çevresel koşullara ilişkin anlık verileri toplayan ve anormal durumları sürekli olarak izleyen özel sensör sistemleri bulunmalıdır.
- **Uzaktan İzleme ve Kontrol**
- Planlı Bakım
- **Güç Yedekleme Sistemleri:** Elektrik kesintisi durumunda, güç yedekleme sistemleri devreye girer. Bu, sıcaklık kontrol sistemlerinin ve izleme ekipmanlarının sürekli çalışmasını sağlar.

Tesislerin güvenliğini sağlamak ve yıldırımdan kaynaklanabilecek olası zararları en aza indirmek amacıyla; paratoner kurulması, güç ve iletişim hatlarına filtreler uygulanması ve bu çalışmaların periyodik bakım ve testlerinin gerçekleştirilmesi gibi çeşitli yıldırımdan korunma önlemleri alınmalıdır.

Endüstriyel ortamlardaki ekipmanlarda özel koruma yöntemleri olarak klavye membranları yerine standart klavyeler kullanılmalıdır. Bu tercih, hem maliyet avantajlarından faydalanmayı sağlar hem de bakım ve değişim süreçlerini daha pratik hale getirir. Standart klavyeler, membranlı klavyelere göre daha ekonomik bir seçenek sunmaktadır. Ayrıca, kullanım sırasında olası bir arıza durumunda, hızlı ve uygun maliyetli bir şekilde yeni bir klavye temini ve değişimi yapılmaktadır. Bu yaklaşım, üretim süreçlerinin sürekli ve verimli bir şekilde devam etmesini desteklemektedir.

Firma bünyesinde, elektromanyetik yayılım nedeniyle bilgi sızıntısı riskini en aza indirmek amacıyla gizli bilgileri işleyen ekipmanın güvenliğini sağlamak için alınan önlemler şu şekildedir;

- **Server Odası Güvenliği**: Gizli bilgileri içeren sunucular, özel bir server odasında tutulmalıdır. Bu oda, kalın duvarlara sahip ve sinyal geçişleri zor olacak şekilde tasarlanmış olmalıdır.
- **Sınırlı Erişim:** Server odasına sadece bilgi işlem personeli tarafından erişim izni verilmelidir. Bu, odanın içinde gizli bilgilerin işlendiği ekipmanlara yetkisiz kişilerin girmesini önleyecektir.
- **Fiziksel Güvenlik Kontrolleri:** Server odası, fiziksel güvenlik kontrolleri ile donatılmalıdır. Bu kontroller arasında elektronik kilit sistemleri, güvenlik kameraları ve erişim izinleri bulunmalıdır.
- **Güçlü Altyapı:** Sunucular, güç kaynakları ve enerji kesintilerine karşı dayanıklı bir altyapı üzerine kurulmalıdır. Bu, elektromanyetik dalgalardan kaynaklanan güç sorunlarını en aza indirmektedir.

Bilgi işleme tesisleri; üretim izleme ve kontrol sistemleri, veri toplama noktaları, endüstriyel bilgisayarlar, baskı ve etiketleme sistemleri, lojistik depo yönetim sistemleri ve ERP gibi çeşitli sistemleri içermektedir. Bu tesisler, işletmenin genel üretim süreçlerini izleme, kontrol etme, veri toplama, raporlama, envanter yönetimi ve diğer kritik görevleri

gerçekleştirme amacıyla kullanılmaktadır. Fiziksel güvenlik önlemleri, bu tesislerin işletme içinde özel olarak yönetilmesini ve dışarıdan gelen müdahalelere karşı korunmasını sağlamak için titizlikle uygulanmalıdır. Bu tesisler, diğer işletme alanlarından fiziksel olarak ayrılmış ve sınırlı erişimle korunmuş olmalıdır. Bu sayede, hassas bilgilerin korunması, veri bütünlüğünün sağlanması ve iş süreçlerinin güvenli bir şekilde yürütülmesi hedeflenmektedir.