**FİZİKSEL ORTAM GÜVENLİĞİ PROSEDÜRÜ**

**GALLİNA EURASİA POLİKARBONAT SİSTEMLERİ SAN. VE TİC. LTD. ŞTİ.**

**1. Amaç**

Bu prosedürün amacı, Gallina Eurasia Polikarbonat Sistemleri San. ve Tic. Ltd. Şti. bünyesinde Bilgi Güvenliği Yönetim Sistemi uygulanması esnasında uyulması gereken fiziksel ortam güvenliği gereksinimlerini tanımlar.

**2. Kapsam**

Şirket faaliyetlerinin yürütüldüğü tüm alanlar ve ilgili tüm personeller bu politika kapsamındadır.

**3. Sorumlular**

Bu prosedürün uygulanmasından tüm şirket personeli sorumludur.

Ayrıca ek olarak aşağıdaki özel sorumluluklar bulunmaktadır.

**4. Kurallar**

**4.1 Fiziksel Güvenlik Temel Prensipler**

* Bilgi varlıklarına erişim yetkileri “Açıkça izin verilmedikçe her şey yasaklanır” ve “Kullanması gerekli” prensiplerine göre verilir.
* Bilgi varlıklarına erişimde kimlik doğrulama (Authentication), yetkilendirme (Authorization) ve aktivitelerin izlenmesi (Auditing) işlevleri uygulanır.
* Hassas ya da kritik bilgi varlıklarını içeren alanlara erişim, “Kullanması gerekli” prensibine göre uygun şekilde, yalnızca yetkili kişilere sağlanır.
* Çalışanlar ve 3. Taraflar, güvenli alanlarda yürütülen faaliyetleri “Bilmesi gerektiği kadar” bilmelidir.

**4.2 Fiziksel Güvenlik Sınırı ve Giriş Kontrolleri**

* Şirket binası ve çevresi, izinsiz fiziksel erişimi engellemek amacıyla 7/24 süreyle kameralar aracılığıyla gözlenir. Kamera kayıtları, herhangi bir uygunsuzluğun araştırılabilmesi amacıyla yeterli süreyle saklanır.
* Bina ve alanların fiziksel erişim kontrolü, güvenlik birimi ve danışma noktası aracılığıyla sağlanır.
* Ziyaretçilerin güvenli alanlarda yalnız başlarına dolaşmalarına hiçbir koşulda izin verilmez.
* Ziyaretçi ve tedarikçilerin bilmesi gereken kadar prensibine göre hareket etmesi sağlanmalıdır.
* Ziyaretçi ve tedarikçilere refakat etmek, personelin ziyaret sebebi ile ilgili olan personelin sorumluluğundadır.
* Bina ve alanlarda çalışanların ve 3. Tarafların güvenliği ve sağlığına ilişkin 6331 Sayılı İş Sağlığı ve Güvenliği Kanunu hükümlerine uygun kontroller uygulanır.
* Güvenli alanlarda sesli ve görüntülü kayıt yapılmasına izin verilmez.

**4.3 Binalar, Ofisler ve Odalar**

* Hassas ya da kritik bilgi varlıklarını içeren ofisler ve odalar, erişimi zorlaştırıcı şekilde konumlandırılır, bu ortamlarda yürütülen faaliyetleri tanımlayarak zafiyet oluşturacak şekilde tabela, gösterge ve işaretler kullanılmaz.
* Sözlü, sesli ya da görüntülü hassas ya da kritik bilgi varlıklarını içeren ofis ve odalar, varlıkların dışarıdan duyulması ve görülmesini engelleyecek şekilde korunur.
* Binadaki giriş/çıkış noktaları ile ortak alanlar, güvenlik tarafından 7/24 süreyle izlenir ve kayıt altına alınır.
* Veri merkezi, sistem odası ve arşiv odası gibi kritik odalar, su tesisatındaki sorunlardan etkilenmeyecek şekilde konumlandırılır.
* Veri merkezi, sistem odası ve arşiv odası gibi kritik odalarda, ortam koşullarının sınırları dışına çıkmasını engelleyecek önlemler alınır.

**4.4 Teslimat ve Yükleme Alanları**

* Kişisel veri barındıran alanlar (arşiv, sistem odası vb.) yetkisiz kişilerin tesise giriş yapabildiği teslimat ve yükleme alanlarından ayrı konumlandırılır.
* Teslimat ve yükleme alanlarına binanın dışından erişim, yalnızca yetkili personel ile sınırlandırılır.
* Teslimat ve yükleme alanları, güvenlik tarafından 7/24 süreyle izlenir ve kayıt altına alınır.
* Teslimat ve yükleme alanlarına gelen malzemelerin bina içerisine alınmadan önce risk oluşturabilecek maddeleri içerip içermediği kontrol edilir.

**4.5 Sistem Odası ve Dağıtım Odaları**

* Sistem Odası’na girişler, kartlı giriş/çıkış sistemine sahiptir.
* Sistem Odası’na giriş yetkisine sahip kişiler, Şirket yönetimi tarafından belirlenir.
* Şirket çalışanı dışında herhangi bir kişiye sistem odası giriş/çıkış yetkisi verilemez.
* Bakım/Destek/Denetim vb. amaçlarla sistem odasına girmesi gereken kişiler, yetkili kişi refakatinde ve Sistem Odası Ziyaretçi Kayıt Listesi’ne kayıt edilerek içeri alınırlar.
* Sistem odasından dışarıya ya da dışarıdan sistem odasının içine Şirket bilişim birimi/ sorumlusu onayı dışında herhangi bir malzeme taşınamaz.
* Sistem odasında bulunan tüm malzemelerin envanter kaydı yapılır.
* Sistem odası, depolama amaçlarıyla kullanılamaz.
* Sistem odası,7/24 süreyle kameralar aracılığıyla gözlenir. Kamera kayıtları, herhangi bir uygunsuzluğun araştırılabilmesi amacıyla yeteri kadar süreyle saklanır.
* Sistem odası birbirini tam olarak yedekleyen klimalar ile iklimlendirilir.
* Sistem odasında, yangından korunmak amacıyla, otomatik yangın algılama ve gazlı söndürme sistemi ile kuruludur
* Sistem odasının sıcaklık, nem ve enerji değerleri, algılayıcılarla izlenmelidir.
* Sistem odasında karton, kâğıt vb. diğer kolay yanabilen türde malzemeler bulundurulmaz.
* Sistem odasına yiyecek, içecek, vb. maddeler ile girilemez.
* Sistem odası erişim yetkileri, en çok 6 ayda bir, Şirket bilişim birimi/ sorumlusu tarafından kontrol edilir.

**5. Yaptırım**

Bu prosedürün ihlal edilmesi durumunda yönetim tarafından gerekli personel desteği de alınarak ihlal nedeni incelenir. İhlal kasıtsız olup personelin eğitim vb. bir eksikliğinden kaynaklanıyorsa problemin kaynağını oluşturan eksikliği kapatmak için çalışma yapılır. Personel yönetim tarafından yazılı olarak uyarılır.

Eğer ihlal işleminin kasıtlı olduğu anlaşılırsa veya kasıtsız olan ihlaller 3’ten fazla tekrar ederse ilgili disiplin yaptırımları gereğince personel hakkında işlem yapılır.

Tüm çalışanlar, güvenlik ihlali olaylarını ve bu prosedürün ihlallerini, en kısa sürede yönetime bildirme sorumluluğundadır.