**TAŞINABİLİR CİHAZ 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 çalışan personelin kullandıkları depolama aygıtlarında yer alan bilgilere yetkisiz kişilerce erişimini engellemek için minimum gereklerin tanımlanmasıdır.

**2. Kapsam**

Şirket bünyesinde kullanılan tüm taşınabilir depolama aygıtlarının kullanım esaslarını kapsar. Yalnızca depolama özelliği olan; CD/DVD, flash disk, taşınabilir hard disk gibi aygıtlar ve bilgi işleme kapasitesi bulunan taşınabilir bilgisayar gibi aygıtlar bu kapsamdadır.

**3. Sorumlular**

Prosedürün uygulanmasından tüm personel sorumludur.

**4. Kurallar**

* “Gizli” gizlilik seviyesinde kurum bilgilerini içeren taşınabilir depolama üst yönetimin onayı olmadıkça, kurum dışına çıkarılamaz.
* “Hizmete özel” gizlilik seviyesindeki kurum bilgilerini içeren taşınabilir depolama, sadece laptop gibi parola koruması olan ortamlarla kurum dışına çıkarılabilir.
* Kurum dışına çıkarma durumlarında aygıtların korunmasından dışarıya çıkarma işlemini gerçekleştiren personel sorumludur.
* Kurum içinde “Hizmete özel” veya daha üst seviye gizlilik seviyesinde gizli bulunan depolama aygıtları parola korumasız ortamlarda başıboş bırakılamaz.
* Kurum içindeki taşınabilir ortamda bilginin sorumluluğu da bilgiyi son teslim alan (yedekleyen vs.) personeldedir.
* Taşınabilir aygıtlar bilgisayar ve sistemlerde açılmadan önce mutlaka güncel bir anti-virüs taramasından geçirilmelidir.
* “Gizlilik”, “bütünlük” veya “erişilebilirlik” seviyesi “yüksek” veya daha üst olan bilgisayar ve sistemlere, güvenliği sistemli ve sürekli olarak kontrol edilen aygıtlar dışında taşınabilir depolama aygıtı takılmamalıdır.
* Depolama aygıtlarındaki bilgilere ihtiyaç duyulma süreci tamamlandığı andan itibaren, aygıt sorumlularınca silinmelidir.
* CD/DVD gibi silinemeyen aygıtlar eğer “gizli” seviyesinde bilgi içeriyorsa kırpma makinesi ile imha edilmelidir. Daha düşük seviyeli kurum bilgilerini içeren ortamlar fiziksel olarak kırılma, parçalanma gibi yöntemlerle imha edilmelidir.

**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.