



TALİMAT

FİZİKSEL ALANLAR VE ÇEVRESEL GÜVENLİK

TALİMAT NO	:	T.786.02
İLGİLİ PROSEDÜR	:	
İLGİLİ SÜREÇ	:	

İLGİLİ BÖLÜM	:	TÜM BÖLÜMLER
ISO 27001	:	EK – A.11
HAZIRLANMA TARİHİ	:	06.04.2018
SAYFA SAYISI	:	6

1. AMAÇ: KAYALAR (Vana, Batarya, Flex, Plastik) bünyesindeki bölümler ve bilgilere yetki dışı fiziksel erişim, hasar ve müdahaleyi engellemek için yöntemlerin oluşturulmasıdır.

2. UYGULAMA

Güvenli Alanlar ve Fiziksel Güvenlik Sınırı

Server odası, arşiv odası, insan kaynakları, üst yönetim, depo, fabrika giriş vb. yerler hassas veya kritik bilgi ve bilgi işleme olanakları barındıran alanlardır. Kötü niyetli girişimlerin ve kontrolsüz çalışmaların engellenmesi, güvenliğin sağlanması için buralarda gerekli güvenlik önlemleri alınmaktadır.

2.1. Fiziksel Giriş Kontrolleri

Aşağıdaki güvenli alanlarda bilgi güvenliğini tehlikeye atacak olası durumları engellemek için çeşitli fiziksel kontrol uygulamaları gerçekleştirilmektedir. Bu kontroller şu şekildedir;

- ⇒ Tüm personelin (mavi ve beyaz yaka) işe girişinde unvan ve isim bilgisi ile birlikte çalıştığı alan kaydı bir liste halinde tutulur. Hangi personelin hangi alanlara girme yetkisi olduğu bu listelerden güncellenir ve takip edilir. Giriş yetkileri (anahtar, kart, parmak izi vb) bu listelere göre verilir. Listeler ilgili çalışma alanlarının girişlerinde asılı tutulur ve çalışma alanındaki/birimindeki amirlerce takibi sağlanır.
- ⇒ Yasaklı alanlara (Server, Bilgi İşlem, arşiv, İK vb.) girişler kartlı, şifreli, parmak okuma sistem ile sağlanmaktadır. İlgili alanlara giriş yapacak kişilere ilişkin yetkiler bölüm amirleri tarafından belirlenerek parmak okuma sistemine kayıt yapabilmek adına Bilgi İşlem departmanına bildirilir. Bilgi İşlem departmanı giriş yetkilerine ilişkin bilgileri **FR.386.00-Erişim ve Kullanım Yetki Tablosu**'na işler. Yasaklı alanlara yetkisiz personel ve ziyaretçilerin girişleri engellenecektir.
- ⇒ **Server odası**, sürekli olarak kilitli halde tutulmakta ve kamera ile 24 saat boyunca kayıt altına alınmaktadır. Serverların yanı sıra tüm tesiste yer alan kamera cihazlarının kayıt kutusu da bu odada bulunmaktadır. Odaya giriş – çıkış sadece Bilgi İşlem personeli nezaretinde gerçekleştirilmektedir. Tüm giriş – çıkışlar kartlı okuma, şifre veya parmak okutma sistemi ile sağlanmaktadır.
- ⇒ **Arşiv odası**, sürekli olarak kilitli halde tutulmakta ve kamera ile 24 saat boyunca kayıt altına alınmaktadır. Odaya giriş – çıkış sadece Arşiv Sorumlusu nezaretinde gerçekleştirilmektedir. Tüm giriş – çıkışlar kartlı okuma, şifre veya parmak okutma sistemi ile sağlanmaktadır.
- ⇒ **İnsan kaynakları odası**, sürekli olarak kapalı/kilitli halde tutulmaktadır. Personel özlük dosyaları metal dolaplarda kilitli bir şekilde tutulmaktadır. Tüm giriş – çıkışlar kartlı okuma, şifre veya parmak okutma sistemi ile sağlanmaktadır.

Bu dokümanın aslı sanal ortamdır. Bu doküman gizlilik taşıyan bilgiler içerir. Sadece KAYALAR (Vana, Batarya, Flex, Plastik) dâhilinde kalmalı, güvenli bir yerde saklanmalı ve fotokopiyle çoğaltılmamalıdır.

REVİZYON NO	REVİZYON TARİHİ	YAYIMLAMA TARİHİ	HAZIRLAYAN	KONTROL	ONAY
02	26.03.2019	09.04.2018	Kalite Sistem	BGYS Temsilcisi	Genel Müdür Yrd.

FİZİKSEL ALANLAR VE ÇEVRESEL GÜVENLİK

- ⇒ **Depo alanına giriş – çıkışlar** kamera ile 24 saat boyunca izlenmekte ve kayıt altına alınmaktadır. Burada çalışan personel listeleri asılı bulunmakta ve depo sorumlusunca takip edilmektedir. Ayrıca bu alanda çalışan personel lacivert kıyafet ve yeşil yelek giyerek ayrıştırılır.
- ⇒ **Üretim alanları ve eşyanın bulunduğu diğer yerlerin güvenliğinin sağlanması için;** Tesis girişinden itibaren personel ve ziyaretçilerin, tesise ve ilgili alanlara zararlı, tehlikeli maddeleri sokmasını engellemek üzere el dedektörü ile arama yapılması sağlanmaktadır. Gerekmesi halinde elle de arama yapılır.
- Personel girişleri kart veya parmak okuma sistemi ile yapılarak yasadışı girişler engellenmektedir.
 - Ziyaretçiler refakat ile gezdirildiğinden belirtilen alanlara girişleri kısıtlanmıştır.
 - Eşyaların bulunduğu üretim alanları, depolar, sevkiyat alanlarında kamera sistemi bulunmakta ve 24 saat izlenmesi sağlanmaktadır.
 - Bu alanlarda çalışan personelin ayrımının yapılabilmesi için farklı renk ve biçimde kıyafetler kullanılmaktadır. Üretimde çalışan işçiler lacivert, kalite personeli yeşil, depo ve sevkiyat personeli lacivert-yeşil renkli kıyafetler giymektedir.
 - Ziyaretçiler ziyaretçi kartı ve kıyafetleri nedeniyle bu alanlarda fark edilebilmektedir.
 - İlgili alanlarda çalışan personellerin listesi birim sorumlularında bulunmakta olup, takibi sağlanmaktadır.
- ⇒ **Fabrika girişinde özel güvenlik** bulunmaktadır. Ziyaretçiler fabrikaya girişi – çıkışlarında Güvenlik personeli tarafından Harmony programına kayıt edilerek izlenmektedir. Bu kayıta gelen kişinin adı, soyadı, araç varsa plakası, geldiği tarih ve saat, çıkış yaptığı saat vb. bilgiler işlenir. Tüm giriş – çıkışlar kamera ile 24 saat boyunca izlenmekte ve kayıt altına alınmaktadır.
- ⇒ **İdari kata** gelen ziyaretçiler Güvenlik tarafından ziyaret edilecek kişi onayı alınarak Ziyaretçi Bekleme Alanına veya Sekreterya Bekleme Alanına yönlendirilir. Ziyaretçilerin fabrika alanı ya da idari katlarda refakatçi olmadan dolaşmalarına izin verilmez.

2.2. Ofisler, Odalar ve Tesislerin Güvenliğinin Sağlanması

Ofisler, odalar ve tesisler boşken odanın kapı ve pencereleri kapalı ve kilitli halde tutulur. İdari katlardaki odaların bulunduğu koridorlar kamera ile 24 saat boyunca kayıt altına alınmaktadır. Ayrıca mesai saatleri dışında ve gündüz mesai bitiminde idari katlara yetkisiz kişilerin girmesini engellemek amacıyla alarm sistemi devreye alınmaktadır.

2.3. Dış ve Çevresel Tehditlere Karşı Koruma

Yangın riskine karşı ofisler/koridorlarda erişilebilecek bir noktada yangın söndürme tüpü yerleştirilmiştir.

Fabrika çevresi olası sızmaları engellemek için otopark tarafında demir korkuluk ile diğer alanlarda da sac paneller ve jiletli teller aracılığıyla güvenli hale getirilmiştir.

Yıldırım çarpması ve buna bağlı yangın oluşma riskine karşı çatıya 2 adet paratoner konulmuştur.

Elektrik panolarına yangın riskini engellemek üzere yangın söndürücü cihazlar takılmıştır.

Fabrikanın çeşitli alanları güvenlik tarafından kamera ile izlenmektedir.

Bu dokümanın aslı sanal ortamdır. Bu doküman gizlilik taşıyan bilgiler2 içermektedir. Sadece KAYALAR (Vana, Batarya, Flex, Plastik) dâhilinde kalmalı, güvenli bir yerde saklanmalı ve fotokopiyle çoğaltılmamalıdır.

REVİZYON NO	REVİZYON TARİHİ	YAYIMLAMA TARİHİ	HAZIRLAYAN	KONTROL	ONAY
02	26.03.2019	09.04.2018	Kalite Sistem	BGYS Temsilcisi	Genel Müdür Yrd.

2.4. Güvenli Alanlarda Çalışmalar

Sistem odalarında yapılacak çalışmalarda aşağıdaki kurallara dikkat edilmelidir;

- ⇒ Sistem odaları yetkisiz personelin bilerek veya kaza ile erişiminin engellenmesi amacıyla her zaman kilitli tutulmaktadır.
- ⇒ Sistem odasına girmeye yetkili olmayan ama bakım/onarım, danışmanlık vb. gibi amaçlarla sistem odasında çalışma ihtiyacı olan kişilerin; uygun şartlar altında, gerekli önlemler alındıktan sonra ve ancak firma çalışanı bir kişinin gözetiminde çalışması sağlanır.
- ⇒ Sistem odasında bulunan sunuculara ve bilgi içeren her türlü ekipmanlara fiziksel erişim, kullanıcı başında bulunmadığı zaman zarfında kontrol altında tutulmaktadır.
- ⇒ Sistem odalarının bulunduğu binaların girişlerinde 24 saat güvenlik görevlisi bulundurulmaktadır.
- ⇒ Sistem odalarının bulunduğu binalara girişte ziyaretçilerin kaydı (kimi ziyaret ettikleri, giriş ve çıkış saatleri) alınıp Harmony programına işlenmektedir.

Sistem odalarında fiziksel güvenlik amacıyla aşağıdaki önlemler alınmıştır;

- ⇒ Yangın söndürme cihazı odaya konulmuştur.
- ⇒ Su baskınına karşı yerden yükseltilmiş taban kullanılmıştır.
- ⇒ Sistem odaları elektrik kesinti ve arızalarına karşı kesintisiz güç kaynağı (UPS) ve jeneratör ile desteklenmiştir.
- ⇒ Sistem odalarında ısı ve nem farklılıklarının önüne geçebilmek amacıyla iklimlendirme sistemleri kullanılmaktadır.

Arşiv odasında yapılacak çalışmalarda **T.794 Arşiv Talimatı** doğrultusunda hareket edilmelidir.

2.5. Teslimat ve Yükleme Alanları

2.5.1. Depo alanına giriş – çıkışlar kamera ile 24 saat boyunca izlenmekte ve kayıt altına alınmaktadır.

2.5.2. Sevkiyat alanı indirme ve yükleme olarak iki kısma ayrılmıştır.

2.5.3. Bu alanlarda işlem yapıldığı zaman çevresi sınırlandırılarak giriş – çıkış bağımsız hale getirilir.

2.5.4. Depo personellerine, diğer bölüm çalışanlarından farklı renklerde giysiler giydirilerek alana izinsiz kişilerin giriş yapmaları durumunda hızlı bir şekilde tespit yapabilme imkanı sağlanmıştır.

2.6. Teçhizat Yerleştirme ve Koruma

Sunucu, DVR (kameraların bağlı olduğu kayıt cihazı) vb. teçhizatlar çevresel tehditlerden ve tehlikelerden, yetkisiz erişim fırsatlarından kaynaklanan riskleri azaltacak şekilde yerleştirilmiş ve korunmaktadır. Teçhizatlar, yerleştirildiği odalarda, hırsızlık, yangın, patlayıcı, duman, su baskını, su kesilmesi, toz, titreşim, kimyasallar ve elektrik sorunları gibi tehditlerden korunmak ve zararı minimuma indirmek için gerekli şekilde konumlandırılmıştır. Teçhizatlar (Sunucu, DVR cihazı vb.) erişimin minimum düzeyde gerekeceği ve prosesle ilgili kişilerin kullanabileceği ayrı odalarda konumlandırılmıştır. Sunucuların korunmasına ilişkin aşağıdaki uygulama ve kurallara dikkat edilmelidir;

- ⇒ Sunucu kurulumları, konfigürasyonları, yedeklemeleri, yamaları, güncellemeleri sadece sorumlu personel(ler) tarafından yapılmalıdır.

Bu dokümanın aslı sanal ortamdır. Bu doküman gizlilik taşıyan bilgiler3 içermektedir. Sadece KAYALAR (Vana, Batarya, Flex, Plastik) dâhilinde kalmalı, güvenli bir yerde saklanmalı ve fotokopiyle çoğaltılmamalıdır.

REVİZYON NO	REVİZYON TARİHİ	YAYIMLAMA TARİHİ	HAZIRLAYAN	KONTROL	ONAY
02	26.03.2019	09.04.2018	Kalite Sistem	BGYS Temsilcisi	Genel Müdür Yrd.

FİZİKSEL ALANLAR VE ÇEVRESEL GÜVENLİK

- ⇒ Sunuculara ait bilgilerin yer aldığı tablo oluşturulmalıdır. Bu tabloda, sunucuların isimleri, ip adresleri ve yeri, ana görevi ve üzerinde çalışan uygulamalar, işletim sistemi sürümleri, donanım, kurulum, yedek, yama yönetimi işlemlerinden sorumlu personel(ler)in isimleri ve telefon numaraları bilgileri yer almalıdır.
- ⇒ Tüm bilgiler, sistem yöneticisinin belirlediği kişi(ler) tarafından güncel tutulmalıdır.
- ⇒ Kullanılmayan servisler ve uygulamalar kapatılmalıdır.
- ⇒ Sunucular üzerinde yapılacak değişiklikler yönetim kuralları çerçevesinde bir onay ve test mekanizmasından geçirildikten sonra uygulanmalıdır.
- ⇒ Sistem yöneticileri gerekli olmadığı durumlar dışında "Administrator" ve "root" gibi genel kullanıcı hesapları kullanmamalı, gerekli yetkilerin verildiği kendi kullanıcı hesaplarını kullanmalıdır. Genel yönetici hesapları yeniden adlandırılmalıdırlar. Gerekli olduğunda, önce kendi hesapları ile log-on olup, daha sonra genel yönetici hesaplarına geçiş yapmalıdırlar.
- ⇒ Ayrıcalıklı bağlantılar teknik olarak güvenli kanal (SSH veya SSL IPSec VPN gibi şifrelenmiş ağ) üzerinden yapılmalıdır.
- ⇒ Sunucular elektrik, ağ altyapısı, kliması olan yerde bulundurulmalıdır.
- ⇒ Sistem odalarına giriş ve çıkışlar erişim kontrollü olmalıdır.
- ⇒ Sunucu olarak çalıştırılacak bilgisayarlar üzerinde kesinlikle kişisel işlemler yapılmamalı.
- ⇒ Sunucular kasti veya bir ele geçirme (hack) sonucu başka bir sisteme erişme ve zarar verme benzeri girişimler için kullanılmamalıdır. Bu duruma uymayan sunuculara erişim anında kapatılacaktır.
- ⇒ Sunucular üzerinde kesinlikle lisansız yazılım kurulmamalıdır.
- ⇒ Sunucular üzerinde daha önce belirtilen servisler haricinde (dosya paylaşımı vb.) başka bir servis çalıştırılmamalıdır.
- ⇒ Yetkisiz kişilerin ayrıcalıklı hesaplara erişip erişemeyeceğinin kontrolü periyodik yapılmalıdır.
- ⇒ Sunucuda meydana gelen mevcut uygulama ile alakalı olmayan anormal olaylar düzenli takip edilmelidir.

2.7. Destekleyici Altyapı Hizmetleri

Veri ve işgücü kaybına yol açabilecek teçhizat kesintisiz güç kaynağı ile desteklenmektedir. Sunucu gibi veri kaybının ve kesintinin önemli sorun yaratacağı yerlerin güç kaynağı daha uzun süreli çalışabilen Jeneratör ile desteklenmiştir. Bunların dışında AR-GE bölümü teknik verilerin tutulduğu alanda bilgisayarlara UPS cihazı konularak olası veri kayıplarının önüne geçilmesi amaçlanmıştır.

2.8. Kablo Güvenliği

Ofis dışında veri taşıyan internet kabloları dışardan kesilmelere karşı yedek hatlar ile korumaya alınmıştır. Hatların kesilmesi durumunda 4g modem ve fiber hat ile iletişim sağlanacaktır.

2.9. Teçhizat Bakımı

Veri güvenliğini sağlamak, sürekli erişilebilirliğini ve bütünlüğünü temin etmek için sunucular ve server odasında bulunan teçhizat bakımlarına ilişkin olarak Bilgi İşlem Sorumlusu tarafından **FR.25 Makine Koruyucu Bakım Fişi** oluşturularak gerekli bakımlarının gerçekleştirilmesi sağlanmaktadır. Ayrıca sunucuların kurulum ve bakım işlemleri Bilgi İşlem Bölümü sorumluluğunda olup aşağıdaki maddeler dikkate alınarak gerçekleştirilmektedir.

Bu dokümanın aslı sanal ortamdır. Bu doküman gizlilik taşıyan bilgiler içermetedir. Sadece KAYALAR (Vana, Batarya, Flex, Plastik) dâhilinde kalmalı, güvenli bir yerde saklanmalı ve fotokopiyle çoğaltılmamalıdır.

REVİZYON NO	REVİZYON TARİHİ	YAYIMLAMA TARİHİ	HAZIRLAYAN	KONTROL	ONAY
02	26.03.2019	09.04.2018	Kalite Sistem	BGYS Temsilcisi	Genel Müdür Yrd.

- ⇒ Kurulması istenen sunucuya ait daha önce konfigürasyon dosyaları ve veriler varsa bunların manyetik bir ortama yedeklerinin alınması sağlanır.
- ⇒ Kurulacak olan işletim sisteminin CD/DVD leri temin edilerek kuruluma başlanır. Bu sırada bulunamayan sürücü varsa bunlar temin edilerek sunucu sisteme yüklenir ve kuruluma tekrar başlanır.
- ⇒ İşletim sistemi kurulumu esnasında sistem sorduğunda gerekiyorsa DNS ve IP adres ayarları ve kurulum tamamlanarak güncelleme işlemi yapılır.
- ⇒ Kurulum sonrasında tanınmayan sürücü olup olmadığı araştırılır, bulunursa daha önceden temin edildiğinden bu sürücülerin kurulumu ve sonrasında gerekiyorsa konfigürasyon ayarları yapılır.
- ⇒ İstenilen sunucunun kurulumu ile ilgili CD/DVD veya diğer manyetik ortamdaki kurulum dosyaları ile söz konusu sunucuya ilave olarak kurulması gereken uygulamalar ve kütüphaneler gerekiyorsa bunlar temin edilir.
- ⇒ İstenen sunucunun kurulumu, ilgili sunucu sistem dokümanı takip edilerek gerçekleştirilir.
- ⇒ Kurulum sonrası gerekli ayarlar yapıp söz konusu sunucunun her açılışta çalışması sağlanır ve sunucu çalıştırılır.
- ⇒ Sunucu gözlemlenerek sağlıklı çalışıp çalışmadığı hata dosyaları (error log) gözlemlenerek izlemeye alınır.
- ⇒ Sistemin periyodik bakımları için sitesinde gerekli ve kritik patchler indirilerek yüklenir.

2.10. Varlıkların Taşınması

Sunucu, DVR (kameraların bağlı olduğu kayıt cihazı) vb. teçhizatlar dış kuruluşlarca yapılacak bakım – onarım gibi çalışmalar için Üst Yönetim (Genel Md. ve Yrd.) onayı alınarak firma dışına çıkarılabilir. Bakım – onarım çalışması dışında teçhizatların firma dışına çıkarılmasına izin verilmez.

FR.383 -Varlık Envanteri Formu’ nda yer alan varlıklar, sadece işyerinin iştigal alanı ile ilgili kullanılmak üzere firma dışına çıkarılabilir. Bunun için Üst Yönetim onayı gereklidir. Ancak, ilgili varlıklar bakım – onarım gibi çalışmalar yapılmak amacıyla Bilgi İşlem Bölümü onayıyla firma dışına gönderilebilir.

Onay işlemleri, bir tutanak ile kayıt altına alınarak Bilgi İşlem Bölümü tarafından arşivlenir.

2.11. Kuruluş Dışındaki Teçhizat ve Varlıkların Güvenliği

Varlıkların kuruluş dışına çıkarılması durumunda firma yerleşkesi dışında çalışmanın farklı riskleri de göz önünde bulundurulur;

- ⇒ Veri kaybını engellemek ve varlığa virüs gibi zararlı yazılımların bulaşmaması için ortam aygıtları kilitli hale getirilmektedir.
- ⇒ Bilgisayarlara kullanıcı adı ve parola ile erişim sağlanabilir. Kullanıcının bilgisayar başında olmadığı durumlarda kilitli ekran moduna geçmesi için gerekli ayarlamalar Bilgi İşlem personeli tarafından yapılmaktadır.

Ayrıca, mobil cihazların firma dışına çıkarılması durumunda **PLTK – 02 Mobil Cihaz Kullanımı Politikası**’na uygun davranılmalıdır.

Bu dokümanın aslı sanal ortamdadır. Bu doküman gizlilik taşıyan bilgiler5 içermektedir. Sadece KAYALAR (Vana, Batarya, Flex, Plastik) dâhilinde kalmalı, güvenli bir yerde saklanmalı ve fotokopiyle çoğaltılmamalıdır.

REVİZYON NO	REVİZYON TARİHİ	YAYIMLAMA TARİHİ	HAZIRLAYAN	KONTROL	ONAY
02	26.03.2019	09.04.2018	Kalite Sistem	BGYS Temsilcisi	Genel Müdür Yrd.



TALİMAT

FİZİKSEL ALANLAR VE ÇEVRESEL GÜVENLİK

2.12. Teçhizatın Güvenli Yok Edilmesi veya Tekrar Kullanımı

Depolama ortamı içeren teçhizatların tüm parçaları **T.784 Taşınabilir Ortam Kullanımı Talimatı** “Taşınabilir Ortamların Yok Edilmesi” maddesine uygun şekilde yok edilir. Tekrar kullanım ile ilgili olarak uygulama yapılmamaktadır. Bu tür teçhizatlar tek bir amaç için kullanılmakta olup tekrar kullanımına izin verilmez.

2.13. Gözetimsiz Kullanıcı Teçhizatı

Kullanıcılar sahip oldukları teçhizatlar ile ilgili **PLTK – 06 Temiz Masa Temiz Ekran Politikası**’na uygun hareket etmektedirler.

Herhangi bir teçhizatla işleri bittikleri vakit oturumlarını sonlandırmaktadırlar.

2.14. Temiz Masa Temiz Ekran

Kâğıtlar ve taşınabilir depolama ortamları için **PLTK – 06 Temiz Masa Temiz Ekran Politikası** oluşturulmuş ve uygulanmaktadır.

3. SORUMLULUKLAR:

BGYS Temsilcisi: Server odası ve teçhizatlarının güvenliğinden, bakımlarının yapılması/yaptırılmasından teçhizatların güvenli yok edilmesi işlemlerinin yürütülmesinden sorumludur.

Arşiv Sorumlusu: Arşiv odası

İnsan Kaynakları Personelleri: Personellere ait özlük dosyalarının korunmasından sorumludur.

Güvenlik: Fabrikaya gelen ziyaretçilerin harmony programına kaydedilmesi ve tesise izinsiz girişleri engellemekten sorumludur.

Kullanıcılar: Bu talimata uygun şekilde davranmaktan sorumludur.

Bu dokümanın aslı sanal ortamdır. Bu doküman gizlilik taşıyan bilgiler6 içermektedir. Sadece KAYALAR (Vana, Batarya, Flex, Plastik) dâhilinde kalmalı, güvenli bir yerde saklanmalı ve fotokopiyle çoğaltılmamalıdır.

REVİZYON NO	REVİZYON TARİHİ	YAYIMLAMA TARİHİ	HAZIRLAYAN	KONTROL	ONAY
02	26.03.2019	09.04.2018	Kalite Sistem	BGYS Temsilcisi	Genel Müdür Yrd.