KAS	***TALİMAT***
	BİLGİ GÜVENLİĞİ İHLAL OLAYI

TALİMAT NO	:	***T.791.00***
İLGİLİ PROSEDÜR	:	
İLGİLİ SÜREÇ	:	

İLGİLİ BÖLÜM	:	***TÜM BÖLÜMLER***
ISO 27001	:	***EK – A.16***
HAZIRLANMA TARİHİ	:	***25.04.2018***
SAYFA SAYISI	:	***3***

***1. AMAÇ**: KAYALAR (Vana, Batarya, Flex, Plastik) bünyesindeki bilgi güvenliği olayları ve zayıflıklarının zamanında düzeltici önlemlerin alınabilmesine izin verecek şekilde bildirilmesini sağlayacak bir yöntemin oluşturulmasıdır.*

2. UYGULAMA

2.1. Bilgi Güvenliği İhlal Olaylarının ve İyileştirmelerin Yönetimi

2.1.1. Sorumluluklar ve Prosedürler

Bilgi güvenliği ihlali ile ilgili olarak tüm taraflar aşağıdaki kurallara uymakla yükümlüdür;

- ⇒ *Kullanıcılar tarafından kullanılan bilgisayar ya da bilişim cihazlarının fiziki güvenliği kullanıcının kendisine aittir.*
- ⇒ *Kullanıcının şifre güvenliği; kullanıcı ilk kez sisteme giriş yapana kadar BGYS Temsilcisine, sisteme dahil olup şifresini değiştirdikten sonra kullanıcının kendisine aittir.*
- ⇒ *Sisteme ilk defa giren kullanıcı, şifresini kimse ile paylaşmamalıdır.*
- ⇒ *Harmony ERP programını kullanan personel şifresini paylaşmamalı, şifresinin başkası tarafından bilindiğini düşünmesi durumunda Bilgi İşlem Bölümü ile iletişim kurarak şifre değişikliği talebini iletmelidir.*
- ⇒ *Şifresi geçersiz olan (süresi dolan) ya da şifresini unutan kullanıcı en kısa sürede ilgili Bilgi İşlem Bölümü ile irtibata geçmeli ve durumu iletmelidir.*
- ⇒ *Yanlış şifre üzerinde güvenlik ihlali oluşturacak gereksiz tekrarlamalardan kaçınılmalıdır.*
- ⇒ *Kullanıcı bilgisayara giriş yaptıktan sonra, bilgisayarının başından kısa ya da uzun süreli ayrıldığında güvenlik ihlaline sebep olmamak için pc'yi kilitleme (lock) moduna almalıdır.*
- ⇒ *Standart bir bilgisayar kullanıcısı, ağ ortamında daha önce belirlenen haklar (doküman ya da yazıcı gibi çevresel cihazlara erişim, bölümündeki aynı statüdeki çalışanlara tanınan haklar vb.) doğrultusundaki bilgilere ulaşabilirler. Bu haklar dışında hiçbir işlem yapamazlar. Eğer kullanıcının ilgili dosya ya da dokümana erişim hakkı yok ise erişim istemek için Bilgi İşlem Bölümü'ne başvurmalıdır.*
- ⇒ *Kullanıcı, yetkisi dışındaki klasörlere, dosyalara ya da ağ paylaşımlarına erişebiliyorsa bunu en kısa sürede BGYS Temsilcisine bildirmekle sorumludur. Aksi taktirde güvenliği ihlal etmiş olur. Kullanıcının yetkisi olmayan alanlara erişimin engellenmesinden veya kullanıcıya erişim tanımlaması yapılmasından Bilgi İşlem Bölümü sorumludur.*
- ⇒ *Sistemde her bilgisayarın birbirinden farklı bir fiziksel adresi (mac adres) ve network ip adresi (internet protokol) vardır. Kullanıcılar gerekli olan ağ kaynaklarına düzgün bir şekilde bağlanıp gerekli olan bilgi ve paylaşılan kaynaklara erişebilirler.*
- ⇒ *Kullanıcıların internette yasaklanan sitelere girmeleri ve internette güvenliğinden kesin emin olmadıkları kaynakları kullanmaları, güvenlik ihlaline sebep olduğu için uygun değildir.*

- ⇒ *Uygunsuz ya da yasadışı internet sitelerine giren kullanıcılar network izleme cihazları ile takip edilip tespit edilirler. Tespit edilen kullanıcılar öncelikle uyarılır ve bu personel adına* ***FR.389 BGYS Olay Kayıt/Bildirim Formu*** *ya da ilgili bölüm amirine e-mail ile bilgilendirme yapılır. Bilgi güvenliği ihlal olaylarının iki kereden çok kez tekrarı durumunda şirket içi P.08 İnsan Kaynakları Prosedürü içerisinde yer alan Disiplin Yönetmeliği gereği uygulanır.*
- ⇒ *Kullanıcı erişim hakkına sahip yazıcı, dosya ya da dokümana erişip gerekli işlemleri yaptıktan sonra o kaynakla bağlantısını kesmeli, gereksiz yere ağı (network) meşgul etmemelidir.*
- ⇒ *Sanal ortamda tanımadığı kimse ya da kimselerden bilmediği doküman ya da dosyaları almamalı, şirket içindeki bilgileri de şirketin bilgi gizliliği kapsamında dışarıya çıkartmamalıdır.*
- ⇒ *Yetkisiz personel ya da kullanıcıların program yükleme, güncelleme ve silme gibi genel güvenliğe ve talimata aykırı davranmaları kesinlikle yasaktır.*
- ⇒ *Kullanıcılar, mecbur kalmadıkça şirket içindeki diğer bilgisayarları ve Bilgi İşlem Bölümü bilgisi olmadan veri taşıma disklerini (usb memory) kullanmamalıdır.*
- ⇒ *Sadece BGYS temsilcisinin onayı ile şirket içinde kullanılması gereken usb ya da harici diskler her kullanımda sistemde kullanılan antivirüs programı sayesinde otomatik olarak test edilmelidir.*
- ⇒ *Kullanıcılar bilgisayarların kurumsal olduğunu unutmamalı, bütün müzik ve resim dosyaları kısıtlanmalıdır. Bilgisayarlarda müzik, resim vs. dosyaları bulundurmamalı var ise silinmelidir.*
- ⇒ *Kullanıcılar, istenmeyen postalara uyarak hiçbir şey satın almamalı, hiçbir hayır kurumuna bağış yapmamalıdır.*
- ⇒ *Bilgisayarlara hiçbir şekilde lisanssız program kurulumu gerçekleştirilmemelidir. Lisanssız yapılan kurulumların, kurulumunu yapan kişiye cezai işlem uygulanması için süreç başlatılır.*
- ⇒ *Kullanıcılara, BGYS Temsilcisinin onayı olmadan herhangi bir şekilde kurum dışında kullanılmak üzere bilgisayar veya bilgi işlem ekipmanı verilmeyecektir.*
- ⇒ *Çalışanlar sistem ve bilgi işlem genel güvenliği kapsamında, mesai sonunda usb bellek, cd, dvd, disket, harici hard disk ya da gizli bilgi içeren şirket dokümanları (dosya, klasör, gizlilik içeren yazılı Doküman vb.) gibi taşınabilir ortamları masada ya da açıkta bulundurmamalıdır.*
- ⇒ *Yönetim, şirket içinde kullanılan bilgi işlem cihazların ve bunların güvenliğinden, şirket içi bilgilerin gizliliğinden ve bilgi güvenliği ihlalinde yapılması gereken işlemlerden müştereken sorumludur.*

2.1.2. Bilgi Güvenliği Olaylarının Raporlanması

Bilgi güvenliği ihlal olaylarının tespit ve bildirimi ***FR.389 BGYS Olay Kayıt/Bildirim Formu*** *aracılığıyla gerçekleştirilmektedir. Tüm bildirimler BGYS Temsilcisi tarafından kayıt altına alınmakta ve izlenmektedir. İhlal olaylarına ilişkin kayıtlar yıllık dönemlerde rapor haline getirilerek Yönetim Gözden Geçirme Toplantısında değerlendirilir.*

2.1.3. Bilgi Güvenliği Açıklıklarının Raporlanması

Bilgi Güvenliği açıklıkları, ***FR.389 BGYS Olay Kayıt/Bildirim Formu*** *ile personel, tedarikçi vb. taraflar tarafından doldurulmakta ve herhangi bir açıklık görülmesi durumunda BGYS Temsilcisi tarafından raporlanmaktadır.*

2.1.4. Bilgi Güvenliği Olaylarında Değerlendirme ve Karar Verme

Bilgi Güvenliği olaylarında değerlendirme ve karar verme doğrudan BGYS Temsilcisi tarafından sağlanmakta, herhangi bir teknik destek ihtiyacı durumunda altyapıyı oluşturan sistem yöneticisi tarafından gerekli önlemler alınmaktadır.

2.1.5. Bilgi Güvenliği İhlal Olaylarına Yanıt Verme

*Bilgi Güvenliği ihlal olaylarında sorumluluk BGYS temsilcisindedir ve hangi varlıklar üzerinde etkisi olduğunun kararı verildikten sonra gerçekleştirilen faaliyetler **FR.389 BGYS Olay Kayıt/Bildirim Formu**'na işlenmelidir.*

2.1.6. Bilgi Güvenliği İhlal Olaylarından Ders Çıkarma

Bilgi güvenliği ihlal olaylarına ilişkin kayıtlar yıllık dönemlerde rapor haline getirilerek Yönetim Gözden Geçirme Toplantısında değerlendirilmektedir. Toplantı sonucunda oluşan aksiyon planı doğrultusunda gerekli görülen önleyici faaliyetler gerçekleştirilmektedir.

2.1.7. Kanıt Toplama

*Bilgi güvenliği ihlal olaylarında doldurulan **FR.389 BGYS Olay Kayıt/Bildirim Formu** ile birlikte; tutanak, ekran görüntüsü, fotoğraf, video kayıt vb. gibi görsel ve yazılı bilgiler kanıt olarak kullanılmalıdır. Kanıt toplama sorumluluğu BGYS Temsilcisindedir.*

3. SORUMLULUKLAR:

BGYS Temsilcisi: *Bilgi güvenliği ihlallerine ilişkin kayıtların tutulması, izlenmesi ve bunlara ilişkin yıllık periyotlarda raporlar hazırlamaktan, bilgi güvenliği açıklıklarına ilişkin raporlar hazırlamaktan, bilgi güvenliği olaylarının değerlendirilmesi ve gerekli kararların verilmesinden, bilgi güvenliği ihlal olaylarına ilişkin kanıtların toplanmasından sorumludur.*

İç ve Dış Paydaşlar: *Bilgi güvenliğini tehlikeye atacak hareketlerden kaçınmak ve bu talimata uygun şekilde davranmaktan sorumludur.*