KAS	***TALİMAT***
	ERİŞİM KONTROLÜ

TALİMAT NO	:	***T.785.02***
İLGİLİ PROSEDÜR	:	
İLGİLİ SÜREÇ	:	

İLGİLİ BÖLÜM	:	***TÜM BÖLÜMLER***
ISO 27001	:	***EK – A.9***
HAZIRLANMA TARİHİ	:	***03.04.2018***
SAYFA SAYISI	:	***5***

***1. AMAÇ**: KAYALAR (Vana, Batarya, Flex, Plastik) bünyesinde bilgiye erişimi kontrol etmek için yöntemlerin oluşturulmasıdır.*

2. UYGULAMA

*KAYALAR, iş ve bilgi güvenliği şartları temelinde **PLTK – 04 Erişim Kontrol Politikası** benimsemiş, uygulamakta ve yıllık periyotlarda gözden geçirmektedir;*

2.1. Ağlar

*Firmamız bünyesinde; 1 adet **mevcut personellerin (kullanıcıların)** kullanmış olduğu ağ ve 1 adet de **ziyaretçilerin** kullanmış olduğu ağ olmak üzere toplam 2 adet ağ bulunmaktadır.*

*Mevcut personellerin (kullanıcıların) dahil olduğu ağda **dosya paylaşım sunucusu** bulunmakta olup bu sunucu üzerinde de **her bölüm/kişi için** oluşturulan **klasörler** bulunmaktadır. Kullanıcılar, ağda yer alan ve Bilgi İşlem Bölümü tarafından **FR.386 Erişim ve Kullanım Yetki Tablosu** ile erişim izni tanımlanan kendi klasörlerine kullanıcı adı ve parola ile erişim yapabilmektedirler. Kullanıcıların, yetki sahibi olmadıkları klasörlere erişim imkanları bulunmamaktadır.*

*Ayrıca kullanıcıların ERP sunucu üzerinde ki erişim hakları varsayılan olarak **FR.386 Erişim ve Kullanım Yetki Tablosu** içinde bulunan yetkilere göre verilmektedir. O yetkiler dışında talep edilecek ekstra yetkiler için madde "**2.2.4 Harmony ERP Programı Kullanıcı Oluşturma, Silme, Yetkilendirme**" de bulunan işlemler geçerli olacaktır.*

***FR.386 Erişim ve Kullanım Yetki Tablosu** ilgili bölümlerin ihtiyaçları doğrultusunda bilgi işlem sorumlusu ve bölüm yöneticileri ile analiz edilerek ihtiyaçlar belirlenerek çıkarılmakta ve forma işlenmektedir.*

ERP modülleri üzerine yapılan geliştirme ve iyileştirmeler sonucunda ortaya yetkiler çıkmaktadır. Bu yetkiler ana modüle sonradan dahil edildiği için ekstra yetkiler durumunda olduğundan madde 2.2.4 te bulunan kurallar çerçevesinde yetkilendirme yapılmaktadır.

Bilgi işlem sorumlusu üst yönetimin yazılı talimatı ile kullanıcıların mevcut yetkilerini kapatabilir.

Misafir ağına katılmak isteyen ziyaretçiler Bilgi İşlem personelinden erişim için kullanıcı adı ve şifre talebinde bulunmalılar. Ziyaretçiler bu ağ üzerinde sadece internet erişimi ile ilgili işlem yapabiliyor olup, mevcut kullanıcı ağı içerisinde yer alan klasörlere erişim yapamazlar. Ayrıca misafirlerin internete çıkışları "5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" doğrultusunda kayıt altına alınmaktadır.

2.2. Kullanıcı Erişim Yönetimi

2.2.1. Kullanıcı Ekleme ve Kullanıcı Silme

İşe başlayan yeni personel için bölüm amiri tarafından bilgi işlem personeline yeni bir kullanıcı açılması yönünde e-posta gönderilir. Bilgi işlem personeli ilgili personelin ad, soyadı, bölüm ve görev bilgilerini ilgili bölüm amirinden talep eder. Gelen bilgiler doğrultusunda kullanıcı için bilgisayar, ERP, e-mail hesaplarını kullanabilmesi için kullanıcı oluşturulur.

2.2.2. Kullanıcı Silme

2.2.2.1. *Hesabın kapatılması, firmamız inisiyatifinde olup, hesapların Bilgi İşlem Bölümü tarafından denetlenme ve kapatılma yetkisini elinde tutar.*

2.2.2.2. *Bilgisayarın hacklenmesi, şifrelerin sızması vb. şüpheli durumların saptanması durumunda Bilgi İşlem Bölümü tarafından kullanıcı bloke edilir. Bu durumlarda kullanıcı uygunsuzluğun giderilmesi ve yeni şifre başvurusunda bulunmalıdır.*

2.2.2.3. *İdari personelin emeklik, işten ayrılma vb. istihdamın sona ermesi durumlarında kurumdan ayrıldığı andan itibaren bütün hesapları (e-mail, harmony, ağ parolaları, erişim yaptığı diğer yerler) kapatılır. Ayrıca personele ilişkin* ***FR.386 Erişim ve Kullanım Yetki Tablosu'*** *nda tüm yetkiler de kaldırılır.*

2.2.2.4. *İnsan Kaynakları Bölümü'nün önceden bildirmesi durumunda erken kapatma süresinin uygulanması da Bilgi işlem Bölümü'nün inisiyatifine bağlı olarak erken uygulanabilir.*

2.2.2.5. *Özel bir durum neticesinde ayrılan personelin hesabının kapatılması uzatılacaksa Genel Müdür ya da Genel Müdür Yardımcısı'nın onayı ile kapatma işlemine ilişkin süre uzatılabilir.*

2.2.3 Harmony ERP Programı Kullanıcı Oluşturma, Silme, Yetkilendirme

2.2.3.1. *Elektronik ortamda tutulan verilere erişimler kullanıcı adı ve şifre ile yapılmaktadır. Gelen talep doğrultusunda kullanıcı erişim hesapları oluşturulur. Harmony ERP programında, Tedarik Zinciri (ithalat, ihracat, dış ticaret, depo, stok hareketleri, kalite kayıtları, sevkiyat, satış, üretim vb.) Muhasebe Finans ve İnsan Kaynakları modüllerinden herhangi birine erişim sağlamak isteyen personelin giriş bilgileri bilgi işlem personeli tarafından açılır.*

2.2.3.2. *Bilgi işlem personeline kullanıcı açma talepleri, bölüm amirleri tarafından mail yolu ile yapılır.*

2.2.3.3 *Bilgi işlem personeli ERP programına erişim sağlayacak personelin ad, soyadı, telefon numarası, çalıştığı departman, görev bilgilerini ve ERP programında erişim sağlayacak modüllerin bilgisini ilgili birimin yöneticisinden ister.*

2.2.3.4. *Gelecek bilgileri doğrultusunda Harmony ERP programında kullanıcı oluşturulur ve şifresi kullanıcıya SMS olarak gönderilir. Şifre işlemleri* ***2.8. Bölümüne*** *uygun olarak yapılır.*

2.2.3.5. *Kullanıcı SMS ile gelen şifreyi kullanabildiği gibi kendisi sisteme erişim sağlayarak şifresini değiştirebilir.*

2.2.3.6. *Kullanıcı sadece kendisine yetki verilen modüllerde "****giriş, ekleme, düzenleme, değiştirme, silme"*** *işlemleri yapabilir. Başka bir modüle giriş yapması ve işlem yapması mümkün değildir.*

2.2.3.7. *Kullanıcıların ERP sunucu üzerinde ki erişim hakları varsayılan olarak* ***FR.386 Erişim ve Kullanım Yetki Tablosu*** *içinde bulunan yetkilere göre verilmektedir.*

2.2.3.8. *Kullanıcı bölüm amirinin bilgisi dışında Harmony ERP modülünde yetki talebinde bulunamaz.*

2.2.3.9. *Kullanıcı şifresini kimse ile paylaşmamalıdır. Bunun tespiti durumunda Bilgi işlem personeli kullanıcının şifresini değiştirip ilgili kişi hakkında uyarıda bulunur ve bölüm amirine rapor eder. Bu olayın tekerrür etmesi durumunda kullanıcı hesabı kapatılır ve üst yönetim bilgilendirilir.*

2.2.3.10. *Personel görev değişikliği yaptığı zaman İK ya da bölüm amirinden bilgi işlem bölümüne personel görev değişikliği ile ilgili bilgi gelir. Görev değişikliği yapan personelin kullanıcı yetkileri sıfırlanır ve yeni görev yeri için gelen talep doğrultusunda yeniden yetkilendirme yapılır.*

2.2.3.11. *Kullanıcının işten ayrılması durumunda İK departmanından gelecek olan bilgi doğrultusunda kullanıcının hesabı kapatılır.*

2.2.3.12. *Kullanıcının Harmony ERP modülü üzerinde yaptığı her giriş, çıkışlar, erişimler ve eşya hareketleri ile ilgili işlemler kayıt altına alınmaktadır. Kullanıcıların hangi tarihte, ne işlem yaptığı (kayda erişme, silme, kayıt ekleme, kayıt değiştirme vb.), kayıtların değişiklikten önceki halleri vb. izlenmektedir.*

2.2.3.13. *Elektronik ortamda tutulan kayıtlara erişimlerin kronolojik kayıtları (log), Harmony ERP programı veritabanı üzerinde en az 2 yıl süre ile tutulmakta olup bu kayıtlara sadece bilgi işlem personeli erişebilmektedir.*

2.3. Ayrıcalıklı Erişim Haklarının Yönetimi

2.3.1. *Ayrıcalıklı erişim hakları (Örn; dosya paylaşım sunucusu, yedekleme ünitesi, kameralar vb. özellikli alanlar) sunucu üzerinde ve veri tabanı üzerindeki verilere ulaşım hakkını kapsamaktadır. Bu erişim hakları* ***FR.386 Erişim ve Kullanım Yetki Tablosu'*** *nda belirtilir.*

2.3.2. *Sunucu üzerinde yönetici (administrator) olarak yalnızca BGYS temsilcisi ayrıcalıklı erişim hakkına sahip olup diğer personelin ayrıcalıklı erişim hakları bulunmamaktadır.*

2.3.3. *Dışarıdan destek alınması gereken durumlarda sunuculara erişim BGYS Temsilcisi gözetiminde sınırlı bir şekilde gerçekleştirilebilir.*

2.4. Kullanıcılara Ait Gizli Kimlik Doğrulama Bilgilerinin Yönetimi

2.4.1. *Kurumumuzda gizli kimlik bilgisi olarak parolalar kullanılmaktadır. Bilgisayar oturum açma parolası, yerel ağ parolaları kullanıcılarının kendi talepleri doğrultusunda oluşturulur. Kullanıcılar, kendilerine tanımlanmış olan kullanıcı adı ve parolalarını unutmaları durumunda Bilgi İşlem Bölümünden talepte bulunur. Bilgi İşlem Bölümü parola sıfırlaması yaparak yeni parola oluşturulmasını sağlar.*

2.4.2. *Personellere e-mail hesabı oluşturma işlemi Bilgi İşlem personeli tarafından yapılmaktadır. Burada geçici parola tanımlaması yapılarak kullanıcının webmail ayarlar bölümünden şifresini güncellemesi istenir.*

2.4.3. *Personellere ERP'ye yalnızca kullanıcı adı ve şifreleri girebilir. Kullanıcı adı ve şifreleri Bilgi İşlem personeli tarafından verilmektedir. Bilgi işlem personeli kullanıcıya sadece bir kereye mahsus girebileceği bir şifre gönderir, kullanıcı bu şifreyi girdiği zaman program yeni bir parola oluşturmasını ister. Kullanıcı bu sayede kimsenin bilmediği yeni şifresini oluşturmuş olur. Kullanıcı verilen parolanın değiştirilmesi ile ilgili olarak Bilgi İşlem Bölümünden talepte bulunabilir veya bu işlem kendi de yapabilir. Bilgi işlem personeli ERP'de kullanıcıya çalışma alanları ve işlem alanları tanımlar. Bunun dışındaki alanlara girme ve işlem yapma yetkisi alınamaz. Yalnızca kullanıcıya tanımlı alanlarda, tanımlı işlemleri (veri girme, erişim, silme, değiştirme) Bilgi İşlem personelinin sistem yetkisi vermesi ile yapabilir. Her sistem kullanıcısı*

*için ayrı tanımlamalar yapılır. Kullanıcı kendisine tahsis edilen parolayı yetkisiz kişilerin erişimine karşı korumak amacıyla kimseyle paylaşmaması ile ilgili olarak **FR.99 KAYALAR GRUP BİLGİSAYAR VE AĞ KULLANIM SÖZLEŞMESİ'**ne uygun davranması hususunda bilgilendirilir.*

2.5. Kullanıcı Erişim Haklarının Gözden Geçirilmesi

*Varlık sahipleri kullanıcıların **FR.386 Erişim ve Kullanım Yetki Tablosu'**nda belirtilen erişim hakları BGYS Temsilcisi tarafından yıllık periyotlarda gözden geçirilmektedir.*

2.6. Kullanıcı Erişim Haklarının Kaldırılması veya Düzenlenmesi

*Tüm çalışanların ve dış taraf kullanıcılarının bilgi ve bilgi işleme olanaklarına erişim yetkileri, istihdamları, sözleşmeleri veya anlaşmaları sona erdirildiğinde kaldırılarak BGYS Temsilcisi tarafından **FR.386 Erişim ve Kullanım Yetki Tablosu** güncellenmektedir.*

2.7. Gizli Kimlik Doğrulama Bilgisinin Kullanımı - Kullanıcı Sorumlulukları

*Kullanıcılara teslim edilen parolaların ifşa edilmeyeceğine dair taahhüt **FR.99 KAYALAR GRUP BİLGİSAYAR VE AĞ KULLANIM SÖZLEŞMESİ** ile alınmaktadır. Bu taahhüde aksi şekilde davrananlar hakkında yasal merciler nezdinde işlem başlatılır.*

2.8. Bilgiye Erişimin Kısıtlanması ve Parola Yönetimi - Sistem ve Uygulama Erişim Kontrolü

Bilgi ve uygulama sistem fonksiyonlarına erişim, Bilgi İşlem personeli tarafından gizli kimlik doğrulama bilgisi (parolalar) kullanılarak sağlanmaktadır. Parolalara ilişkin uyulması gereken kurallar şunlardır;

- ⇒ *Sistem hesaplarına ait parolalar (örnek; root, administrator, enable, vs.) ve kullanıcı hesaplarına ait parolalar (örnek, e-posta, web, masaüstü bilgisayar vs.) kullanıcı talebi doğrultusunda değiştirilir.*
- ⇒ *Sistem yöneticisi sistem ve kullanıcı hesapları için farklı parolalar kullanmalıdır.*
- ⇒ *Parolalar e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.*
- ⇒ *Kullanıcı, parolasını başkası ile paylaşmamalı, kâğıtlara ya da elektronik ortamlara yazması durumunda güvenliğini sağlamalıdır.*
- ⇒ *Kullanıcı güçlü bir parola oluşturmak için aşağıdaki parola özelliklerini uygulamalıdır.*
  - *En az 8 haneli olmalıdır.*
  - *İçerisinde en az 1 tane harf bulunmalıdır. (a, b, C...)*
  - *İçerisinde en az 1 tane rakam bulunmalıdır. (1, 2, 3...)*
  - *İçerisinde en az 1 tane özel karakter bulunmalıdır. (@, !,?,^,+,$,#,&,/,{,*,-,],=,...)*
  - *Aynı karakterler peş peşe kullanılmamalıdır. (aaa, 111, XXX, ababab...)*
  - *Sıralı karakterler kullanılmamalıdır. (abcd, qwert, asdf,1234,zxcvb...)*
  - *Kullanıcıya ait anlam ifade eden kelimeler içermemelidir. (Aileden birisinin, arkadaşının, bir sanatçının, sahip olduğu bir hayvanın ismi, arabanın modeli vb.)*

Şifre koruma standartları ile ilgili kurallar aşağıda belirtilmiştir.

- ⇒ *Bütün parolalar kuruma ait gizli bilgiler olarak düşünülmeli ve kullanıcı, parolalarını hiç kimseyle paylaşmamalıdır.*
- ⇒ *Web tarayıcısı ve diğer parola hatırlatma özelliği olan uygulamalardaki "parola hatırlama" seçeneği kullanılmamalıdır.*

⇒ *Parola kırma ve tahmin etme operasyonları belli aralıklar ile bilgi güvenliği yetkililerince yapılabilir. Güvenlik taraması sonucunda parolalar tahmin edilirse veya kırılırsa kullanıcıdan parolasını değiştirmesi talep edilebilir.*

2.9. Güvenli Oturum Açma

Erişim kontrol politikası, güvenlik duvarı, dosya paylaşım sunucusu, mail sunucu vb. yerlerde ortamda bulunan kötü niyetli sızmaları engellemek için güvenli oturum açmaya ihtiyaç duyulabilir. Bunun için sunuculara BGYS Temsilcisi tarafından SSL, TLS, HTTPS, protokolleri ile bağlantı kurulur.

2.10. Ayrıcalıklı Destek Programlarının Kullanımı

*Firmamızda sistem ve uygulamaların kontrollerini geçersiz kılabilecek destek programlarının kullanılmaması konusunda taahhüt **FR.99 KAYALAR GRUP BİLGİSAYAR VE AĞ KULLANIM SÖZLEŞMESİ** ile kayıt altına alınmaktadır. Kullanıcılar herhangi bir programı indirse bile bilgisayara kurulum yapılması BGYS Temsilcisi iznine tabidir. Bu taahhüde aksi şekilde davrananlar hakkında yasal merciler nezdinde işlem başlatılır.*

2.11. Program Kaynak Koduna Erişim Kontrolü

ERP programı kaynak kodu sadece Üst Yönetimde bulunmakta olup yetkisiz erişim, kötü kullanım ve bozulmalara karşı kilitli dolaplarda tutulmaktadır. Programın güncel kaynak kodu tedarikçi firmada bulunmaktadır.

*Web tabanlı uygulamaların kaynak kodları firma bünyemizdeki sunucuda bulunmakta olup buranın güvenliği ile ilgili hususlar **T.785 Erişim Kontrolü Talimatı** ve **T.786 Fiziksel Alanlar ve Çevresel Güvenlik Talimatı** doğrultusunda gerçekleştirilmektedir.*

3. SORUMLULUKLAR:

***BGYS Temsilcisi:** Ağlara kullanıcı ekleme/silme, mevcut kullanıcı ve misafir ağlarının yönetimi, erişim izinlerinin verilmesi, izin kullanımların tespiti ve müdahale edilmesi, ayrıcalıklı erişim haklarının yönetimi, kullanıcılara ilişkin gizli kimlik doğrulama bilgileri ve parolaların yönetimi, güvenli oturum çalışmalarının yürütülmesi ve koordinasyonundan sorumludur.*

***Kullanıcılar:** İnternet ve mevcut ağlarda yapacakları işlerde uyması gereken kurallar doğrultusunda hareket etmek, kendilerine tahsis edilen parolalar, gizli kimlik doğrulama vb. bilgileri erişim izni olmayan kişilerden korumak ve izin verilenler dışında ayrıcalıklı destek programlarını kullanmamakla sorumludur.*