OMSA	**KENDİ CİHAZINIZLA ÇALIŞMA POLİTİKASI**	DOKÜMAN NUM.: KVK / PL.001 YAYINLANMA TARİHİ: 10.03.2020 REVİZYON NUM.: 000 REVİZYON TARİHİ: --/--/----

DAĞITIM BİRİMLERİ:
PAY KLASÖRÜ-YAYIN BİRİMİ / KVK BELGELERİ
WEB SİTE-YAYIN BİRİMİ: ISLAK İMZALI DOKÜMAN

1. AMAÇ
Bu politika, tesisin veri ve teknoloji altyapısının güvenliğini ve bütünlüğünü korumayı amaçlamaktadır.

2. KAPSAM
Tesisin, çalışanları, taşeronları ve aracı hizmet sağlayıcıları "Kullanıcılar" olarak anılacaktır.
E-postalarına ve diğer bilgi teknoloji sistemlerine bağlanma izni verebilir. İşbu prosedür, tesisin veri ve teknoloji alt yapısının güvenliğinin sağlanması amacıyla kullanıcıların uyacakları esasları belirleyecektir.

3. TANIMLAR
ERP: Yazılım programı

4. SORUMLULAR
YÖNETİM
KULLANICILAR

5. UYGULAMALAR

5.1. Faaliyetlerin Gerçekleştirilmesi

- **Uygun Kullanım**

Kabul edilebilir ticari kullanım, tesisin veya onunla ilişkili şirketlerin veya işletmelerin işlerini doğrudan veya dolaylı olarak destekleyen faaliyetlerden oluşur. Tesis için kabul edilebilir kişisel kullanım, ilgili kişisel nedenler kapsamında makul ve sınırlı kişisel iletişimden oluşur. Tesis için, uygun kişisel kullanımı, Tesis markası ve itibarı ile uyumlu makul ve sınırlı kişisel iletişim, tarama gibi diğer faaliyetler oluşturur.
Kullanıcılar mobil cihazlarını tesise ait şu kaynaklara erişmek için kullanabilir;
-Belgeler, sunucular, e-posta ortamı, network, ürün / yazılım dizinleri, firewall, temel ticari set, ERP, Exchange Server, Wi-Fi erişimi vb.

- **Kısıtlamalar**

Kullanıcıların, tesis ağlarına bağlı olduklarında çalışma saatleri süresince belirli web sitelere erişimleri engellenebilir. Bu web siteleri sınırlı olmamakla birlikte belirli kategorilerde erişimler için engelleme içerir.
Cihazların kamerası ve / veya videosu tesisin önceden açık rızası olmaksızın kullanılmamalıdır.
Cihazlar bazı zamanlarda kullanılamayabilir;
-Yasa dışı materyalleri saklama ve iletmede,
-Başka bir şirkete ait tescilli bilgileri saklama ve iletmede,
-Başkalarını rahatsız / taciz etme,
-Dış ticaret faaliyetlerinde bulunmada,
-Microsoft, iTunes, GooglePlay vb. tanınmış ana sağlayıcılardan indirilemeyen uygulamalar veya yazılımlara izin verilmez.

Tesis, sürüş sırasında mesajlaşma veya e-posta gönderme konusunda sıfır tolerans politikasına sahiptir. Sadece güvenli olduğunda kullanılabilir. Yalnızca hands-free sistemlerle konuşma izni verilir.

- **Güvenlik**

Yetkisiz erişimi önlemek için, cihazların parola ile korunması ve tesis ağına erişmek için güçlü bir parola gerekir. Bunun mümkün olmadığı durumlarda tesise bildirimde bulunulmalıdır.
Tesisin koruma politikası;

-Şifreler en az sekiz karakter olmalı,
-Büyük ve küçük harfler, sayılar ve sembollerin bir kombinasyonu olmalı,
-Süreli parola geçerliliği sağlanmalıdır. (Maksimum 6 Ay)

Tesis verilerine erişen kullanıcılar zaman zaman tesis tarafından belirlenecektir.
Cihazlardan uzaklaşıldığında, bir parola, PIN veya biyometrik tanıma ile kilitlenmelidir.
Kilitleme süresi, en düşük uygun zamana ayarlanmalıdır.
Rooted (Android) veya jailbroken (iOS) cihazlar veya benzerlerinin Tesis ağına erişmesi kesinlikle yasaktır.
Tesis, Kullanıcı cihazında uzaktan silme teknolojisini kurma ve kullanma hakkını saklı tutar.

a) Cihazın kaybolması durumunda
b) Kullanıcının Tesis ile ilişkisinin kesilmesi durumunda,
c) Bir veri veya politika ihlali, virüs veya benzeri bir güvenlik tehdidi algıladığında, cihaz uzaktan silinebilir.

Kaybolan veya çalınan cihazlar 24 saat içinde tesise bildirilmelidir.
Kullanıcılar, bir cihaz kaybettikten hemen sonra mobil operatörlerini bilgilendirmekten sorumludur.
Kullanıcının kendi cihazlarını her zaman etik bir şekilde kullanması ve yukarıda özetlenen tesisin uygun kullanım politikasına uyması beklenir.
Kullanıcı kendi cihazıyla ilişkili tüm masraflardan kişisel olarak sorumludur.

- **Cihazlar ve Destek**

IPhone, Android, Blackberry ve Windows telefonlarını içeren akıllı telefonlar ve tabletler kullanılabilir.
Bağlantı sorunları tesis tarafından desteklenebilir; Kullanıcılar, tüm işletim sistemi veya donanımla ilgili sorunlar için aygıt üreticisine veya operatörlere başvurmalıdır.
Cihazlar, tesis ağlarına erişmeden önce, tarayıcılar, ofis yazılımları ve güvenlik araçları gibi standart uygulamaların uygun şekilde yapılandırılmış haliyle tesise sunulmalıdır.

- **Giderler veya Geri Ödeme**

Tesis, kullanıcı cihazındaki tesis sistemlerinin kullanımı ile ilgili kullanıcılara tekrar ödeme yapmaz.

- **Riskler / Yükümlülükler / Feragatler**

Tesis, kullanıcının kendisine ait kişisel verilerinin kaybolmasını önlemek için her türlü tedbiri almak için gerekiyorsa cihazı uzaktan silebilir. Fakat kişisel e-postaların yedeklenmesi, kişi bilgileri, fotoğraflar, belgeler vb. gibi kendi kişisel verilerine ait ek önlemler almak kullanıcının sorumluluğundadır.
Tesis, bildirimde bulunmadan cihazların ağlarına erişimini kesme/engelleme veya hizmetleri devre dışı bırakma hakkını saklı tutar.
Kullanıcı, bir işletim sistemi çökmesi, aygıtı kullanılamaz hale getiren hatalar, virüsler, kötü amaçlı yazılımlar ve / veya başka bir yazılım veya donanım nedeniyle tesisin ya da kendisine ait kişisel verilerin kısmen veya tamamen kaybını içeren ancak bunlarla sınırlı olmayan riskler için tam sorumluluk üstlenir.
Kullanıcı, bilgi sistemleri yöneticilerinin, izni / onayı, bilgisi dışında herhangi bir uygulama yüklememelidir. Ancak onay karşılığında uygulama yükleme işlemi gerçekleştirilebilir. İzinsiz / Onaysız yüklenen uygulamalardan doğacak zarardan kullanıcılar sorumludur.
Doğacak zararların tesise yüklenmesi halinde, tesis kullanıcılara rücu hakkını saklı tutar.
Tesis, bu politikaya uyulmadığı durumlarda; cezalar, yaptırımlar veya sözleşmenin sona ermesi (ve çalışanlar için iş akdinin feshi de dahil olmak üzere disiplin prosedürlerinin uygulanması) gibi kullanıcılara karşı uygun eylemde bulunma haklarını saklı tutar.

5.2. Dokümanların Yenileme ve Kayıt İşlemleri

- Revizyon gerektikçe yapılır ve revizyon işlemleri dok. Rev. Talep ve onay formları ile gerçekleştirildikten sonra güncel dokümanlar kvk belgeleri klasörüne yerleştirilir.