# BİLGİ GİZLİLİĞİ, BİLGİ GÜVENLİĞİ VE DİJİTALLEŞME POLİTİKASI

## 1.AMAÇ

Su Biyomedikal Sistemler ve Sağlık Hizmetleri Sanayi ve Ticaret A.Ş. (SUBMED) Bilgi Gizliliği, Bilgi Güvenliği ve Dijitalleşme Politikası ile şirketimiz, ISO 27001:2022 Bilgi Güvenliği Yönetim Sistemi şartlarını karşılamayı, geliştirme faaliyetlerini sürdürmeyi, yasaları ve mevzuatlara uyumluluğu kontrol etmeyi, riskleri ve fırsatları analiz ederek bilgi güvenliği gereksinimlerini yerine getirmeyi ve dijitalleşme noktasında yeni nesil teknolojileri takip ederek iş süreçlerine entegre etmeyi amaçlamaktadır.

## 2. KAPSAM

Şirketimizin çalışanları, tedarikçileri, grup şirketleri ve iş ortakları Bilgi Gizliliği, Bilgi Güvenliği ve Dijitalleşme Politikamıza tam uyum göstermelidir. Politikamız kapsamında belirtilen tüm ilkelere zıt faaliyetler bilgi güvenliği ihlali olarak kabul edilip, etik değerlendirme ve disiplin süreçlerine tabii tutulur.

Bilgi Güvenliği ve Dijitalleşme Politikası, şirketimize ait;

- Etik, Uyumluluk ve Bilgilendirme Politikası,
- Rüşvet ve Yolsuzlukla Mücadele Politikası,
- Sorumlu Satın Alma ve Tedarik Zinciri Politikası,
- Entegre Yönetim Sistemi Politikası,
- Sürdürülebilirlik Politikası,

ile ayrılmaz bir bütün olarak değerlendirilmektedir.

## 3. BİLGİ GİZLİLİĞİ VE BİLGİ GÜVENLİĞİ

### 3.1 Bilgi Erişimi

Şirketimize ait her türlü teknoloji, ürün, müşteri, tedarikçi veya grup şirketlere ait bilgiler şirketimizin yetkili kişilerine açık olmalıdır. Erişim yetkisi olmayan kişiler yönetim kurulumuzun izni olmadan bu bilgilere erişememelidir. Eğer bir çalışanımız yetki alanı dışındaki bir veriye ulaşmak istiyorsa yönetim kurulu onayı almalıdır.

### 3.2 Bilgi Gizliliğinin ve Bilgi Güvenliğinin İhlali Olarak Görülen Davranışlar

Bilgi gizliliği ve bilgi güvenliğinin ihlali olarak değerlendirilen süreçler şirketimiz tarafından belirlenmiştir:

- Herhangi bir kişisel verinin sızdırılması veya menfaat için kullanılması,
- Şirket içi gizli bilgilerin iş dışı bir amaç için kullanılması veya üçüncü taraflarla paylaşılması,
- Şirkete ait gizli tutulan teknolojik altyapı, tasarım veya yazılımın şirket dışına çıkarılması,
- Hisse ticaretinde kullanılmak, maddi çıkar sağlamak veya manevi menfaat elde etmek için şirketimizin, çalışanlarımızın, tedarikçilerimizin, grup şirketlerimizin veya iş ortaklarımızın bilgilerinin şirket dışına çıkarılması,
- Bilgi sistemimize dair erişim sınırlarının kırılmaya çalışılması veya kırılması,
- Şirketimizin sistemlerinde çalışanlarımız tarafından herhangi bir açık tespit edilmesi halinde şirketimizden gizlenmesi

- Çalışanlarımızın izin alınmadan yetki alanı dışındaki bir alandan bilgi edinilmesi,
- Müşterilerimize ait bilgilerin kişilerin izni olmadan kullanılması,
- Müşterilerimizden iş süreçlerinde kullanılacak verilerin dışında veriler talep edilmesi,
- Şirketimize ait sistemlere kötü niyetli yazılımların bulaştırılması,
- Zayıf şifre kullanımı nedeniyle sızıntıya neden olmak,
- Gizlilik anlaşması yapılmadan danışman firmalara sistemsel şifrelerin verilmesi,
- Fiziksel olarak tutulan belgelerin izinsiz bir şekilde imha edilmesi,
- Sahte e-postalar veya web siteleri aracılığıyla bilgilere erişim girişimleri,

şirketimiz tarafından bilgi gizliliği ve güvenliğinin ihlali olarak kabul edilir.

### 3.3 Bilgi Güvenliği Önlemlerimiz

- Şirketimizin ağ erişimi kişiler bazında kısıtlandırılmıştır. Kullanıcılara atanan adresler aracılığıyla eşleştirmeler gerçekleştirilerek veri erişimleri tanımlanmaktadır.
- Departmanlar ve kişiler bazında, bilgi sistemimiz içerisinde filtreleme uygulamaları ve kurallar bulunur.
- Bilgilerimiz dış erişimlere kapalı olup şirketimizin kullandığı güçlü bir VPN yapısı ile korunmaktadır.
- E-posta güvenliğimiz uluslararası düzeyde kendini kanıtlamış sağlayıcılar tarafından korunmaktadır.
- Şirketimizin her departmanına özel bilgi depolama alanları tahsis edilmiştir. Verilerin erişimleri ilgili departman yetkililerimize tanımlanmış olup diğer departmanlardan veri ihtiyacı oluşması halinde çalışanlarımız, bu veriyi o departmanın yetkilisinden talep etmelidir.
- Ulusal ve uluslararası bilgi güvenliği sistemleri yakından takip edilmekte ve güçlendirme çalışmalarına dahil edilmektedir.
- Bilgi güvenliği ile ilgili riskler bilgi teknolojileri uzmanlarımız tarafından düzenli olarak analiz edilerek önlemler alınmaktadır.

### 3.4 SUBMED Bilgi Sistemlerini Kullanma Kuralları

Şirketimize ait bilgi sistemlerini ve teknolojik alt yapıyı kullananlar;

- Bilgi teknolojileri uzmanlarımızın belirlediği risklere karşı önlemlerini almalıdır.
- Bilgi sistemlerimizi kullanmadan önce “Etik, Uyumluluk ve Bilgilendirme Politikamızı”, “Bilgi Gizliliği, Bilgi Güvenliği ve Dijitalleşme Politikamızı” ve “Rüşvet ve Yolsuzlukla Mücadele Politikamızı” detaylı bir şekilde okumalı ve içselleştirmelidir.
- Şirketimize ait bilgi sistemlerini ve altyapılarını kullanırken yasal yükümlülüklerin, politikalarımızın, iş etiği ve iş ahlakı anlayışının dışına çıkmamalıdır.
- Şirket içi bilgileri kesinlikle herhangi bir çıkar veya menfaat için kullanmamalı veya sızdırmamalıdır.
- Tedarik zincirimiz içerisinde yer alan her bir tüzel kişiliğin, grup şirketlerimizin iş ortaklarımızın bilgilerini gizli tutmalıdır.
- Bilgilerimize ve kurumsal kaynaklarımıza yalnızca iş süreci gereği erişim talebi oluşturmalıdır.

### 3.5 Üçüncü Taraflar

Şirketimizin bilgi sistemlerini kullanmak durumunda olan danışmanların veya üçüncü kişilerin politikalarımıza uyumlu bir iş süreci yürütmeleri zorunludur. İş süreçleri gereği üçüncü taraflar sistemlerimize erişmeleri durumunda bu kişiler;

- Şirketimize ait bilgileri ve varlıkları şirketimizin izni olmadan paylaşmamalıdır.
- Şirketimizin onayı olmadan herhangi bir ses veya video kaydı ve fotoğraf çekimi yapılmamalıdır.
- Şirketimizden onay alınmadan herhangi bir cihazdan veri veya yazılım kopyalanmamalıdır.
- Şirketimize ait lokasyonlarda gerçekleştirilecek hizmetler bilgi teknolojileri ekibinin gözetiminde gerçekleştirilmelidir.

## 4. DİJİTALLEŞME

Şirketimiz dijitalleşme çalışmaları ile sağlam yapılarak oluşturarak, var olan yapıları teknolojik açıdan güçlendirerek zaman, maliyet ve güvenlik ile ilgili riskleri bertaraf etmeyi, iş süreçlerimizde verimliliği arttırmayı ve müşterilerine daha kaliteli hizmet sunmayı hedeflemektedir.

### 4.1 Dijitalleşme ile İlgili Çalışanlarımızdan Beklentiler

- Çalışanlarımız, yeni ve güncel teknolojileri yakından takip etmelidir.
- Çalışanlar, tespit ettikleri teknolojik fırsatları üst yönetime belirtmeli ve iş süreçlerine entegre edilmesi için öneriler sunmalıdır.
- Şirketimiz içerisindeki teknolojik altyapıyı tam, doğru ve verimli bir şekilde kullanacak bilgileri içselleştirmelidir.
- Müşterilerimize hizmetlerini teknolojik altyapımızdan faydalanarak tam, doğru ve hızlı bir şekilde gerçekleştirmelidir.
- Yaşadığı teknik sorunları ivedilikle bilgi teknolojileri departmanına iletmeli ve çözüm talep etmelidir.

### 4.2 Çalışanlarımıza Dijital Koşulların Sağlanması

- Şirketimiz, çalışanlarına en kullanışlı ve en yeni teknolojik altyapıyı sunarak verimli ve rahat çalışma ortamı sağlar.
- Bilgi gizliliği ve güvenliğini sağlanması için çalışanlarına güçlü ve güvenilir bir altyapı kaynağı sunar.
- Elektronik iletişim kanallarımız, şirket çalışanlarımıza, tedarikçilerimize, iş ortaklarımıza ve grup şirketlerimize kesintisiz olarak açıktır
- Şirketimize ait ihlaller, iş birlikleri, talep ve şikayetlerde kullanılmak üzere oluşturulan bildirim hatları 7/24 herkese açık tutulmaktadır. Kişiler istedikleri an ihlal, öneri, şikâyet veya talep bildirimi gerçekleştirebilirler.

**Tarih: 01.01.2024**
**SUBMED Yönetim Kurulu Başkanı: Yusuf Yiğit AKKUŞ**

**İmza:**