arena	**Bilgi Güvenliği Politikası**	
	Doküman No:	**POL.BS.01**
	Doküman Sahibi	**Bilgi Sistemleri Yönetimi**

Revizyon No	*Revizyon Tarihi*	*Revizyon Tanımı*	*Revizyonu Yapan*	*Onaylayan*
0	*19.10.2018*	*İlk Yayın*	*Bilgi Güvenliği Yöneticisi*	*Yönetim Kurulu*
1	*17.09.2021*	*ISO/IEC 27001:2017 standardı eklendi.*	*Bilgi Güvenliği Yöneticisi*	*Yönetim Kurulu*
2	*22.11.2021*	*Bilgi güvenliği hedeflerine tedarikçi bilgi güvenliği ifadesi eklendi.*	*Bilgi Güvenliği Yöneticisi*	*Yönetim Kurulu*
2	*10.08.2022*	*Güncelliği gözden geçirildi.*	*Bilgi Güvenliği Yöneticisi*	*Yönetim Kurulu*
3	*15.03.2023*	*Güncelliği gözden geçirildi ve imla hataları düzeltildi.*	*Bilgi Güvenliği Yöneticisi*	*Yönetim Kurulu*
4	*29.11.2023*	*3.Tanımlar, Roller, Sorumluluklar ve Yetkiler başlığı, 3. Tanımlar, 4 Roller Sorumluluklar ve Yetkiler olarak ayrıldı. Roller, Sorumluluklar ve Yetkiler başlığı detaylandırıldı. 5 Politika başlığı ve altındaki alt başlıklar güncellendi. 6 Politikanın Gelişimi altındaki ibareler düzenlendi.*	*Bilgi Güvenliği Yöneticisi*	*Yönetim Kurulu*

Hazırlayan	Kontrol Eden	Onaylayan
Bilgi Güvenliği Yöneticisi	Üst Yönetim	Yönetim Kurulu

1. Amaç

Bu politikanın amacı, hukuka, yasal düzenleyici ya da sözleşmeye tabi yükümlülüklere ve her türlü güvenlik gereksinimlerine ilişkin ihlalleri önlemek için, Üst Yönetim'in bilgi güvenliği yaklaşımını tanımlamak, tüm çalışanlara ve ilgili taraflara bildirmektir.

Bilgi Güvenliği Politikası kurumsal bilgi güvenliği ilkelerimizi ana hatlarıyla belirler. Bilgi Güvenliği Politikası, kurumda bilginin ve işlenme yöntemlerinin güvenli olarak gerçekleştirilmesi amacıyla düzenlemeler yapar.

2. Kapsam

Bu politika Bilgi Güvenliği Yönetim Sistemi (BGYS) kapsamında bulunan tüm çalışanları, ve diğer tüm paydaşlara ilişkin süreçleri kapsamaktadır.

3. Tanımlar

Bilgi Güvenliği Yönetim Sistemi (BGYS): Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçasıdır.

Bilgi Varlığı: Şirket'in sahip olduğu, işlerini aksatmadan yürütebilmesi için gerekli olan dolayısıyla korumakla yükümlü olduğu bilgi sistemleri varlıklarıdır.

4. Roller Sorumluluklar ve Yetkiler

Bu politakanın hazırlanması, gerekli analizlerin yapılması gözden geçirilmesi, güncellenmesi ve yürürlükten kalkanların toplanarak imha edilmesinden Bilgi Güvenliği Yöneticisi, kontrol edilmesinden Üst Yönetim, onaylanmasından Yönetim Kurulu sorumludur.

Bu politika periyodik olarak senede bir defa veya gerekli görülen hallerde Bilgi Güvenliği Yöneticisi tarafından gözden geçirilir. Arena Bilgisayar Üst Yönetimi Bilgi Güvenliği Politikası'nın tüm çalışanlara ve ilgili diğer tüm paydaşlara duyurulmasını sağlar.

Gözden geçirmeler sonrasında gerçekleştirilen değişiklikler için Yönetim Kurulu onayı alınır.

5. Uygulama

5.1. Yönetim Kurulu Bağlılığı

Şirket Yönetim Kurulu bilgi güvenliğinin gerçekleştirilmesi, işletimi, izlenmesi, gözden geçirilmesi, bakımı ve iyileştirilmesi için gerekenin yapılacağını taahhüt eder.

5.2. Bilgi Güvenliği Politikası

- Bilgi Güvenliği Yönetim Sistemini, uluslararası olarak kabul edilmiş olan ISO/IEC 27001:2017 Bilgi Güvenliği Yönetim Sistemi standardı şartları doğrultusunda planlamak, gerçekleştirmek ve geliştirmek.
- Bilgi güvenliğini etkin biçimde yönetmek ve yaşanabilecek olan zararları en aza indirmek ve sürekli iyileştirmesini sağlamak.

- Bilgi güvenliği ihlallerinin önüne geçmek ve oluşabilecek bilgi güvenliği ihlallerine koordineli bir şekilde yanıtlamak ve çözüm bulmak.
- İş sürekliliği kapsamında yaşanabilecek kesintiler için önlem almak ve önüne geçmek.
- Kritik iş süreçlerinin hedef kurtarma süreleri içerisinde, tekrar çalışır hale getirmek.
- Bilgi sistemleri kapsamındaki yasal yükümlülüklere uyumlu hale gelmek.
- Bilgi Güvenliği Yönetim Sistemi kapsamında müşterilerimizin ve tedarikçilerimizin bilgi varlıklarının gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak.

5.3. Bilgi Güvenliği Yönetim Sistemleri Genel Süreçleri

Şirket bilgi güvenliğini sağlamak amacıyla kendi kurumsal işleyişini düzenleyici prensipleri oluşturur. Bilgi Güvenliği Politikasının belirlenmesi, güvenlik rollerinin tanımlanması ve ilgili tüm güncellemelerin yapılması Üst Yönetim'in desteği ve tüm birimlerin koordinasyonuyla gerçekleştirilir. Arena Bilgisayar gerekli durumlarda iç ve dış uzmanların görüşüne başvurabilir.

Bu çerçevede şirket aşağıdaki uygulamalar ile Bilgi Güvenliği Politikasını benimser ve sistemin işleyişini sürekli hale getirir;

Varlıklar: Şirket sahip olduğu bilgi varlıklarını sınıflandırır. Bu sınıflandırmanın nasıl yapıldığı ve varlıkların nasıl değer ataması yapıldığı Varlık Yönetimi Prosedüründe detaylı olarak aktarılmaktadır.

Risk Değerlendirme ve Risk Analizi: Bilgi varlıklarıyla ilgili oluşabilecek risklerin belirlenmesi ve risklerin ölçümlenmesi ve değerlemesinin yapıldığı devamlı bir süreçtir.

Talimatlar: Bilgi sistemin uygun şekilde işletilebilmesi, işletmenin genel kurallara bağlı, denetlenebilir, tekrar edilebilir ve iyileştirilebilir olması amacıyla gerekli talimatlar hazırlanır.

Fikri Mülkiyet Hakları: Şirket, fikri mülkiyet hakkı taşıyan ürün, yazılım, hizmet veya sistemler sahibinden izin alınmadan veya kullanım lisansı olmadan kullanılamaz.

Eğitim: Tüm personele ve gereken durumlarda üçüncü taraf personellere, bilgi güvenliği ile ilgili politika, talimat ve prosedürler hakkında gerekli eğitimler verilir. Eğitim kapsamına giren kurallar bütününde muhtemel değişiklik ve güncellemeler gerçekleştikten sonra güvenlik eğitimleri tekrarlanır.

Yasal Uyumluluk: Şirket, bilgi güvenliği ile ilgili yayınlanmış kanun, yönetmelik ve tebliğlere uygun olarak hizmet vermek için gerekli tüm çalışmaları yapar.

İş Sürekliliği: Üst Yönetim, bilgi güvenliği iş süreklilik ilkelerini belirler ve iş süreklilik ilkelerinin hayata geçirilmesi için bir İş Süreklilik Planı oluşturulmasını ve değişen koşullara göre güncel tutulmasını sağlar. Güncel İş Sürekliliği Planı ile ilgili roller ve sorumluluklar İş

Sürekliliği Planı'nda belirtilir. İş sürekliliğine ilişkin genel prensipler İş Sürekliliği Politikasında yer almaktadır.

Temiz Masa Temiz Ekran: Çalışma saatleri süresince ve dışında, çalışanların açık olan bilgisayarlarının veya çalışma masalarının başından geçici veya sürekli olarak ayrılmaları gerektiğinde bilgiye yetkisiz erişim, bilgi kaybı ve hasarı risklerini azaltmak amacıyla kâğıtlar, kaldırılabilir depolama ortamları ve kişisel bilgisayarlar için gerekli şartlara uyulması gerektiğini tanımlamaktadır.

Sürekli İyileştirme: Şirket, bilgi güvenliği politikasını, denetim sonuçlarını, izlenen bilgi güvenliği olaylarının analizini, düzeltici ve önleyici faaliyetleri ve yönetim gözden geçirmelerini kullanarak Bilgi Güvenliği Yönetim Sistemini sürekli olarak iyileştirir.

Bilgi Güvenliği Organizasyonu:

Bilgi Güvenliği Yönetim Sistemi kapsamında organizasyon belirlenmesi ve uygulanması Üst Yönetim sorumluluğundadır. Bu sorumlukların neler olduğu, kişi isimleri ve sorumlulukları BGYS Roller ve Sorumluluklar Prosedürü dokümanında detaylı olarak aktarılmaktadır. Bu dokümanda belirtilen hususlara uyulması ve uygun çalışılması tüm personeli kapsamaktadır.

- Varlıkların güvenliğini sağlanmasından ve gözetilmesinden tüm personel sorumludur.
- Varlıklara ve bilgilere erişirken Bilgi güvenliği kapsamında belirlenmiş olan erişim yetki esaslarına uyum konusunda tüm çalışanlar yükümlüdür.
- Bilgi güvenliği kontrol önlemlerinin uygulamaya alınması ve kontrolü BGYS Kurulu tarafından gerçekleştirilir.
- Bilgi bulunan her türlü ortamın (elektronik ortam, basılı doküman, usb…vb) saklanması, oluşturulması, imha edilmesi ve erişilmesi konularında belirtilen kurallara uyulması tüm personelin yükümlülüğüdür.
- Bilgi güvenliği ile ilgili kritik kararların alınması, onaylanması ve gözden geçirilmesi Bilgi Güvenliği Yöneticisi tarafından yerine getirilir.
- Varlıkların korunması ve politikanın gerçekleştirilmesiyle ilgili güvenlik rollerinin şirket personeline atanması gerçekleştirilir. Hassas sistemlere erişim yetkisi olan yeni ve deneyimsiz kullanıcılar için gerekli gözetimlere dikkat edilir. Çalışanların sorumluluklarından haberdar olmaları sağlanır.
- Kapsam dahilindeki personel sahip olduğu varlıkların değerlendirmesini belirlemekten sorumludur.
- Varlıklarda gerçekleşmesi muhtemel ekleme ve çıkarma işlemleri sonrası gerekli durumlarda risk değerlemesi ve risk raporunun güncellenmesi yapılmalıdır.
- Güvenlik sorunları ve bozulmaları BGYS kuruluna raporlanır. Raporlanmış bir güvenlik sorunu öncelikli olarak çözümlenir. Yazılım problemlerinden kaynaklanan sorunlar da aynı şekilde ele alınır.

- **Üçüncü Taraf Erişimi**: Üçüncü şahıs ve kurumların bilgi sistemlerine erişimlerinin güvenli olarak gerçekleştirilmesi amacıyla gerekli düzenlemeler yapılır. Bu çerçevede, riskler analiz edilir, erişim gereksinimleri belirlenir ve sınıflandırılır. Anlaşmalı kurumların personeli ve diğer üçüncü taraflar için ilkeler belirlenir ve uygulanır. Üçüncü taraf erişimleri için uygun risk analizi yapılır. Güvenlik sorumluluklarını da içeren Gizlilik Sözleşmeleri hazırlanır.

- **Fiziksel ve Çevresel Güvenlik**: Fiziksel ve çevresel güvenliğin bilgi güvenliği kapsamında eksiksiz olarak sağlanması amacıyla düzenlemeler ve denetimler yapılır. Hassas varlıkların bulunduğu yerler güvenlikli olmak zorundadır. Güvenli bölgeler bu amaçla hazırlanır ve bu bölgelerin güvenliği sağlanır. İhtiyaca göre farklı güvenlik seviyeleri tanımlanarak her bir seviye için farklı güvenlik mekanizmaları devreye sokulabilir. Donanım güvenliği düşünülerek bu cihazların yetkisiz fiziksel erişim, yangın, su baskını gibi tehdit ve tehlikelere karşı korunması sağlanır. Donanımların yerleştirilmesi, güç kaynaklarının kurulumu, kablolamanın gerçekleştirilmesi güvenlik düşünülerek yapılır. Donanımların düzenli bakımı gerçekleştirilir. Donanımların yapılandırılması esnasında güvenlik ilkelerine dikkat edilir.
- **Denetimler:** Şirket içerisinde Bilgi Güvenliği Yönetim Sistemi kapsamında yılda en az 1 defa iç denetim gerçekleştirilir. Üst Yönetimin gerek görmesi halinde, üçüncü taraf bağımsız denetim uzmanlarından da bağımsız denetim hizmeti veya iç denetimlere danışmanlık hizmeti alınabilir.
- **Disiplin Süreci ve Yasal Yükümlülükler:** Tüm çalışanlar, bu politikaya uymakla yükümlüdür. Tüm çalışanlar, çalışma saatleri dışında veya çalışma alanı dışında da bilgi güvenliği ile ilgili yükümlülüklere sahiptir. Bilgi Güvenliği Politikası, diğer ilgili politikalar ve BGYS'ni etkileyen süreçlere uyulmaması durumunda ilgili disiplin süreci uygulanır.

6. Politikanın Gelişimi

6.1. Kalite Kayıtları

Kayıt Ad/Tanımı	Saklandığı Ortam	Sorumlu	Saklama Süresi
Ağ Güvenliği Politikası	Ortak Alan	Bilgi Güvenliği Yöneticisi	10 yıl
Erişim Kontrol Politikası	Ortak Alan	Bilgi Güvenliği Yöneticisi	10 yıl
Şifre Yönetim Politikası	Ortak Alan	Bilgi Güvenliği Yöneticisi	10 yıl
Kabul Edilebilinir Kullanım Politikası	Ortak Alan	Bilgi Güvenliği Yöneticisi	10 yıl
İş Sürekliliği Politikası	Ortak Alan	Bilgi Güvenliği Yöneticisi	10 yıl
Teçhizat ve Medya Güvenliği Politikası	Ortak Alan	Bilgi Güvenliği Yöneticisi	10 yıl

6.2. Referanslar

- SPK Bilgi Sistemleri Yönetim Tebliği, ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı, Madde 5.1 Liderlik ve bağlılık, Madde 5.2 Politika, A.5 Bilgi güvenliği politikaları

6.3. Arayüzler

- myHR