1. AMAÇ

VERİON Bilgi Güvenliği Politikası, tüm çalışanlara, tedarikçilere, iş ortaklarına ve paydaşlara Şirket'in bilgi güvenliği ihtiyacını, kapsamını, amaçlarını, hedeflerini, ilkelerini ve esaslarını ve bilgi güvenliği ile ilgili rol ve sorumlulukları bildirmek amacıyla hazırlanmıştır.

2. KAPSAM

Bu politika, Şirket bünyesindeki veri ve bilgilerin; bilgi güvenliğinin kapsamını, hedeflerini, ilkelerini, yönetim desteğini, risk yönetimi çerçevesini, sürekliliğini, görev ve sorumlulukları, uyum gereksinimlerini ve bu politikanın ihlali durumunda uygulanacak yaptırımları kapsamaktadır.

3. ROLLER VE SORUMLULUKLAR

Bilgi Güvenliği Politikasının güncelliğinin ve sürekliliğinin sağlanmasından Bilgi Güvenliği Komitesi sorumludur. Bilgi Güvenliği politikasında yapılacak güncellemeler Bilgi Güvenliği Komite toplantılarında belirlenir ve Bilgi Güvenliği Yöneticisi tarafından dokümana yansıtılır. Politikada yapılan her revizyon Yönetim Kurulu onayına sunulur.

İlgili tarafların bu kapsamdaki görev ve sorumlulukları Bilgi Güvenliği Rol ve Sorumluluklar Prosedürü'nde açıklanmıştır.
Tüm birim yöneticileri kendi sorumluluk alanlarına giren sistemlerin sürekli gözden geçirilmesi ve iyileştirmesinden, tüm çalışanlar güncel olan dokümanları kullanmak ve uygulamaktan sorumludur.
Bu politika ile çerçevesi belirlenen bilgi güvenliği gereksinimleri ve kurallarına ilişkin ayrıntılar, bilgi güvenliği prosedürleri ile düzenlenir. Şirket çalışanları ve üçüncü taraflar bu prosedürleri bilmek ve çalışmalarını bu kurallara uygun şekilde yürütmekle yükümlüdür.

4. TANIMLAR VE KISALTMALAR

BGYS	: Bilgi Güvenliği Yönetim Sistemi
KEYS	: Kurumsal Entegre Yönetim Sistemi
KVKK	: Kişisel Verilerin Korunması Kanunu
Şirket	: Verion Teknoloji Sanayi ve Ticaret Anonim Şirketi

5. İLGİLİ DOKÜMANLAR / REFERANSLAR

- Siber Güvenlik Başkanlığı Bilgi ve İletişim Güvenliği Rehberi
- TS EN ISO 27001 Bilgi Güvenliği Yönetim Sistemi Standardı
- TS EN ISO 9001 Kalite Yönetim Sistemi Standardı
- ISO/IEC 27701 Kişisel Bilgi Yönetim Sistemi Standardı
- ISO 22301 İş Sürekliliği Yönetim Standardı
- TS EN ISO 15504-2 (CMMI) Süreç Olgunluk Modeli
- LST.01-Doküman Kayıt ve Takip Listesi
- PRO.02-Çalışma Düzeni ve Disiplin Prosedürü
- PRO.05-Bilgi Güvenliği Rol ve Sorumluluklar Prosedürü

6. BİLGİ GÜVENLİĞİ POLİTİKASI

Şirket, tabi olduğu ulusal, uluslararası veya sektörel düzenlemelerden, ilgili mevzuat ve standart gereklerini yerine getirmek, sözleşmelerden doğan yükümlülüklerine uygun süreçler işletmek, iç ve dış paydaşlara yönelik kurumsal sorumluluklardan kaynaklanan bilgi güvenliği gereksinimlerini sağlamak amacı ile:

- Bilginin gizliliğini sağlayarak, bütünlüğünü koruyacak ve sürekli erişilebilirliğini (kullanılabilirliğini) sağlayacak altyapıyı ve kontrolleri hayata geçirir.
- Bilgi güvenliği bilincini kurum kültürünün bir parçası haline getirerek, çalışanların bilgi güvenliği farkındalığını üst seviyede tutmayı sağlar.
- Kişisel bilginin 6698 sayılı Kişisel Verilerin Korunması Kanunu ve ilgili ikincil mevzuat uyarınca mahremiyetinin korunmasını sağlamak amacıyla idari ve teknik tedbirleri alır.
- Analiz, tasarım, geliştirme, test ve uygulama süreçlerinde görevler ayrılığı prensibine uygun yetkilendirmeyi sağlar ve kritik işlemlerde çoklu onay (dört göz) mekanizması tesis eder.
- Bilgiye erişimi, "en az erişim hakkı" prensibi ile sadece "bilmesi gereken" verir ve yetkisiz erişim engellenmesini sağlar.
- Dış ağlardan gelebilecek tehditlere karşı ağ güvenliğini tesis eder.
- Geliştirme, test ve üretim ortamlarının fiziksel ve düşünsel olarak ayrılmasını sağlar.
- Kullanıcıların yetkilendirilmesinde gerekli olan minimum yetkilendirme prensibinin sağlanması ve yetkilerin düzenli olarak kontrol edilmesini sağlar.
- Katmanlı güvenlik mimarisini tesis eder ve sürekli gözetimini sağlar.
- Mobil uygulama ve internet sayfası aracılığıyla sunduğu hizmetlerde, ilgili servislerin Şirket tarafından sağlandığını doğrulayacak teknikler kullanır.
- Kullanılan şifreleme anahtarlarının güvenilirliğini sağlar.
- Mobil cihazlar üzerinde çalışan uygulamalar tarafından kullanılan hassas ödeme verilerinin güvenliğinin sağlanmasını tesis eder.
- Bilgi güvenliği konusunda periyodik olarak değerlendirmeler yaparak mevcut riskleri tespit eder; değerlendirmeler sonucunda, aksiyon planlarını gözden geçirir ve takibini sağlar.
- Mobil cihazlar üzerinde çalışan uygulamaların güvenliğini sağlamaya yönelik önlemleri alır, gerekli güncellemeleri sağlar.
- Bilgi güvenliği faaliyetlerinin yönetilmesini ve koordinasyonunu sağlamak amacıyla bir bilgi güvenliği organizasyonu oluşturarak, tüm bileşenlerini bütünleşik olarak yönetir.
- Bilgi ve bilgi işleme olanakları ile ilgili varlık envanterini oluşturarak, sahiplikleri belirler ve bilgi varlıkları üzerindeki riskleri yönetir.
- Bilgi güvenliği olaylarının tespit edilmesi, raporlanması ve tekrarının önlenmesi adımlarını içeren bilgi güvenliği olay yönetimi faaliyetleri gerçekleştirir.
- Bilginin işlendiği alanlarda bilginin güvenliğinin sağlanabilmesi amacıyla gerekli fiziksel ve çevresel güvenlik önlemlerini alır.
- Bilgi sistemleri edinim, geliştirme ve bakımında güvenlik gerekliliklerinin neler olduğunu belirler ve hayata geçirir.
- İş faaliyetlerindeki kesintileri önlemek ve bilgiye sürekli erişimi sağlamak için iş sürekliliği faaliyetleri gerçekleştirir.
- Bilgiye erişimi kontrol etmek ve yetkisiz erişimleri önlemek için ilgili tüm alanlarda gerekli güvenlik kontrollerini hayata geçirir.
- Bilgi güvenliği konusundaki güncel teknolojileri ve yenilikleri takip ederek, çözümler geliştirerek, sürekli iyileştirmeyi sağlar.
- Bilgi güvenliği yönetim sisteminin verimliliğini, iç ve dış denetimlerle kontrol ederek, izleyerek, gözden geçirerek, sistemi sürekli uyumlu kılar.

7. BİLGİ GÜVENLİĞİ HEDEFLERİ VE AMAÇLARI

Bilgi Güvenliği Politikası, Şirket çalışanlarına, tedarikçilerine, temsilcilerine, iş ortaklarına ve paydaşlarına Şirket'in güvenlik gereksinimlerine uygun şekilde hareket etmesi konusunda yol göstermek, bilinç ve farkındalık seviyelerini artırmak ve bu şekilde Şirket'te oluşabilecek riskleri minimuma indirmek, Şirket'in güvenilirliğini ve imajını korumak, üçüncü taraflarla yapılan sözleşmelerde belirlenmiş uygunluğu sağlamak, teknik güvenlik kontrollerini uygulamak, Şirket'in temel ve destekleyici iş faaliyetlerinin minimum kesinti ile devam etmesini sağlamak amacıyla Şirket'in tüm işleyişini etkileyen fiziksel ve elektronik bilgi varlıklarını iç ve dış kasıtlı veya kasıtsız tehditlere karşı korumayı hedefler.

8. BİLGİ GÜVENLİĞİ ORGANİZASYONU

Şirket yönetimi bilgi güvenliği organizasyonunu Şirket bünyesinde oluşturur. Bu kapsamda Şirkette güvenlik politikalarının bütünsel bir yaklaşım oluşturulması, sürdürülmesi ve yönetilmesine ilişkin çalışmalar Bilgi Güvenliği Yönetim Süreci kapsamında yürütülür. Şirketin güvenlik kontrol süreçlerini koordine edecek, yönetecek rol ve sorumluluklar Bilgi Güvenliği Rol ve Sorumluluklar Prosedürü kapsamında belirlenir.

9. RİSK YÖNETİM ÇERÇEVESİ

Şirket'in bilgi güvenliğine ilişkin risk değerlendirme yaklaşımı Bilgi Güvenliği Yönetim Temsilcisi tarafından belirlenir ve Bilgi Güvenliği Yönetim Süreci kapsamında tanımlanır. Bilgi güvenliği risk değerlendirme yaklaşımı ile şirketin bilgi güvenliği risklerinin hangi yöntemler ile belirleneceği, risk seviyelerinin nasıl hesaplanacağı ve risklerin nasıl değerlendirileceği belirlenir. Bilgi varlıklarıyla ilgili oluşabilecek risklerin tanımlanması, derecelendirilmesi, işlenmesi ve gözden geçirilmesi çalışmaları belirlenen risk değerlendirme yaklaşımına uygun olarak gerçekleştirilir

Risk değerlendirme çalışması sonucunda, riskleri azaltmaya yönelik aksiyonları da içeren "Bilgi Sistemleri Risk Değerlendirme Raporu" oluşturulur.

10. POLİTİKANIN İHLALİ VE YAPTIRIMLAR

Bu politikanın ihlali halinde, Çalışma Düzeni ve Disiplin Prosedürü gereğince; uyarma, kınama, maaş kesintisi, yasal otoritelere bildirim ve sözleşme feshi yaptırımlarından biri ya da birden fazla uygulanabilir.

11. GÖZDEN GEÇİRME, YAYINLAMA VE DENETİM, RAPORLAMA

Yönetmeliklerde veya bilgi güvenliği uygulama süreçlerindeki değişiklikler politikanın gözden geçirilmesini gerektirir. Gözden geçirilen ve güncellenen politika Yönetim Kurulu tarafından onaylanır. Onaylanan politika kurumun tüm çalışanlarının eriştiği ortak dosya sunucusu üzerinde yer alan "Kurumsal Entegre Yönetim Sistemi" klasöründe yayınlanır.

Bu politika, güvenlik anlayışı ile hizmet sunulması faaliyetleri kapsamında Kalite Yönetim Temsilcisi sorumluluğunda yılda en az (1) bir defa denetlenir.

Doküman Revizyon Bilgileri		
Yapılan Değişiklik	**Tarih**	**Gözden Geçirme No:**
Bilgi Güvenliği Politikası Oluşturulması	01.07.2024	01.0
Yıllık Gözden Geçirme	25.06.2025	01.1
POL-01 olarak politikanın ayrıştırılarak, güncellenmesi ve Yıllık Gözden Geçirme	03.02.2026	01.2