1. AMAÇ

Bu kalite politikasının (“Politika”) amacı, Verion Teknoloji Sanayi ve Ticaret Anonim Şirketi (“Şirket”)’nin Kurumsal Entegre Yönetim Sistemi (“KEYS”) çerçevesinde; sunulan hizmetlerin veya yeni hizmet fırsatları yaratmak ve/veya bunları karşılamak için işlemleri ve kabiliyetinin ayrılmaz bir parçası olan teknolojinin ulusal ve uluslararası düzenlemeler, standartlar ve rehberler kapsamında etkili teknoloji yönetimi ve iş stratejileri ile uyumlu teknolojik çözümlerin kullanılmasını amaçlamaktadır.

2. KAPSAM

Bu politika, Şirket bünyesinde kurulan ve işletilen kurumsal entegre yönetim sistemlerine ait tüm süreçleri, faaliyetleri ve geliştirilen tüm teknolojileri kapsar.

3. ROLLER VE SORUMLULUKLAR

Bilgi Teknolojileri Politikasının güncelliğinin ve sürekliliğinin sağlanmasından Bilgi Teknolojilerinden Sorumlu Genel Müdür Yardımcısı sorumludur. Bilgi Teknolojileri politikasında yapılacak güncellemeler toplantılar ile belirlenir. Bilgi Teknolojilerinden Sorumlu Genel Müdür Yardımcısı ve Yönetim Temsilcisi ile koordineli olarak dokümana yansıtılır. Politikada yapılan her revizyon Yönetim Kurulu onayına sunulur.

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 sürekli kalite artırımına yönelik gereksinimleri ve kurallarına ilişkin ayrıntılar, Kurumsal Entegre Yönetim Sistemi 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
BTK	: Bilgi Teknolojileri ve İletişim Kurumu
BT	: Bilgi Teknolojileri
KEYS	: Kurumsal Entegre Yönetim Sistemi
Yeşil Bilişim	: Enerji verimliliği, kaynak tasarrufu ve çevre dostu bilişim uygulamalarını ifade eder.
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
- POL.01-Bilgi Güvenliği Politikası
- PRO.02-Çalışma Düzeni ve Disiplin Prosedürü

6. BİLGİ TEKNOLOJİLERİ POLİTİKASI

6.1. MİMARİ SÜREÇ

Mimari süreç, şirketin teknolojiyi yaygınlaştırmak ve geliştirmek için kullandığı ve ilgili plan, politika, prosedürlerinde belirtilmiş olan misyon, vizyon, ilkeler ve standartlardan oluşmaktadır. Şirket teknolojisinin ve faaliyetlerinin hızla değişen yapısı göz önüne alındığında, tutarlı teknik karar verme için mimari süreç temel bir gereksinimdir.

Şirketin bilgi teknolojileri ve iş birimlerinin koordinasyonu, verinin varlık olarak ele alınması, kesintisiz iş

sürekliliğinin sağlanması, mevzuat, standart ve politikalara sürekli uyum şirketin mimari prensipleridir.

6.2. DEĞİŞİM YÖNETİMİ

Değişim Yönetimi, değişiklikleri planlama, programlamak, uygulamak, dağıtmak ve takip etmek için kullanılan süreçtir. Etkili değişim yönetimi süreci, iş ihtiyaçları tarafından gerekli görülen değişiklik adımını sürdürürken ortamın bütünlüğünü ve güvenilirliğini sağlar.

Şirketin bilgi teknolojileri ve iş birimlerinin koordinasyonu, Gereksinim tabanlı değişiklik, mimari onay, bilgi güvenliği onayı, mevzuat, standart ve politikalara sürekli uyum şirketin değişim yönetimi prensipleridir.

6.3. İŞ SÜREKLİLİĞİ

Şirketin kalite, müşteri memnuniyeti ve minimum kesinti odaklı hizmet anlayışı prensibi bulunmaktadır. Bu iş modeli kapsamında planlanan İş Sürekliliği aşağıdaki hedefleri kapsamaktadır.

- Planlanan iş sürekliliği aktivitelerinin amacı, iş sürekliliği planının sürekli iyileştirilmesine dair farkındalık yaratılması ve sadece teknolojiyi değil iş süreçlerini muhafaza etmektir.
- Etkili iş sürekliliği planlaması, sadece yıllık uygulama olarak değil iş operasyonlarının ayrılmaz bir parçası olduğuna dair anlayış olarak benimsenmesi için faaliyetler gerçekleştirilir.
- İş sürekliliği planlarının, bütün iş faaliyetlerini kapsamasını ve herhangi bir iş kesintisi halinde detaylı ve koordineli olarak müdahale edilmesi sağlanır.
- Rol ve sorumlulukları tanımlanmış olan İş Sürekliliği Komitesi oluşturulur ve faaliyetlerinin iç denetim ekibi tarafından denetimi sağlanır.
- Acil durum veya öngörülemeyen durum halinde kriz durumunun ilan edilmesi ve stratejik kararların alınması sağlanır.

6.4. BİLGİ GÜVENLİĞİ

Şirket tarafından oluşturulan, işlenen ve kullanılan veri ile bilgi, şirketin en değerli varlıklarındandır. Tüm birimler, bu varlıkları korumak için gerekli tüm idari ve teknik tedbirleri alır.

Tüm çalışanlar, bu veri ve bilgileri, iş ile ilişkili amaç doğrultusunda yayınlanmış politikalar ve prosedürlere uygun olarak işler ve korur.

6.5. YEDEK VE YEDEKTEN DÖNÜŞ

Şirketin, bağlı olduğu tüm elektronik ve ile bilgi kaynaklarının, bilgi teknolojileri altyapısının, veri kaybına ve bozulmalara karşı korunmasını sağlamak için tutarlı politikalar ve prosedürleri uygulaması kritik öneme sahiptir. Bu doğrultuda:

- Şirketin hedeflerine ulaşmak için bilgi teknolojileri sistemlerinin ve verilerin yedeklenmesi için gereken minimum kontroller tanımlanmaktadır.
- Donanım veya yazılım hatası, fiziksel felaket veya insan hatası nedeniyle oluşabilecek veri kaybına karşı koruma sağlanmaktadır.
- Afet ve acil durumlarda şirket içinde iş sürekliliği sağlanmaktadır.

Şirket, tüm kurumsal verileri aşağıdaki temel prensiplere göre yedeklemektedir.

1. Hangi verilerin ve sistemlerin yedeklendiğine dair tamamlanma logları tutulur.
2. Tüm yedekleme zamanlanmış işlerinin logları kayıt edilir ve bakımı yapılır.
3. Tüm yedek medyalar (sunucu, kartuş vb.) açıkça etiketlenir.
4. Yedekler, canlı sistemler ile aynı binada saklanmaz. Şirket, birincil sistemleri/verileri ile yedeklerini coğrafi olarak farklı lokasyonlarda tutar.
5. Veri ve sistem kurtarma süreçleri sık sık test edilir. Testler arasındaki maksimum süre bir yılı geçmez. Acil durum veya felaket durumunda yedeklerin kullanılabilmesi için kurtarma prosedürleri test edilir.
6. Yedekten geri dönüş prosedürleri güncel tutulur.

6.6. BİLGİ TEKNOLOJİLERİ RİSK YÖNETİMİ

Bilgi Teknolojileri (BT) risk yönetimi, Şirket'in genel operasyonel risklerinin bir parçasıdır. BT riskleri, bilgi ve siber gibi birçok farklı disiplinden türetilmiş, arıza ve çözüm, düzenleme, teknolojik değişiklikler, iş değişiklikleri, insan kaynakları ve daha fazlası ile ilgili geniş tabanlı risklerdir. Risk yönetimi, Şirket faaliyet ortamındaki değişikliklerle ilgili sürekli ve dinamik bir süreçtir. Bu değişiklikler teknolojik boyutta, iş boyutunda, düzenleyici boyutta, insan boyutunda ve tehdit boyutunda meydana gelebilir.

Bilgi Güvenliği Yöneticisi koordinasyonunda Bilgi Güvenliği Yönetim Komitesi tarafından bilgi ve iletişim güvenliği rehberi ve bilgi güvenliği yönetim sistemi (BGYS) çerçevesinde periyodik risk değerlendirmesi gerçekleştirmektedir. Bu değerlendirme, BT süreçlerine atıfta bulunmayı, Şirket'e ait varlıkları, üçüncü tarafa ait varlıkları ve bunları çeşitli risk düzeylerine göre sınıflandırmayı içerir. Risk değerlendirmesine dayanarak, Şirket;bilgi teknolojisi sistemine zarar verme olasılığını en aza indirmek için gerekli önlemleri alır. Değerlendirme ayrıca Bilgi Güvenliği Birimi tarafından Şirket'in bilgi sistemlerini güvence altına almak için sağlanacak ek adımlar hakkında kararlar almak için kullanılır.

7. 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.

8. 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 Teknolojileri Politikası Oluşturulması	17.02.2026	01.0