



YAPAY ZEKA POLİTİKASI

YAPAY ZEKA POLİTİKASI

1. AMAÇ

Bu politikanın amacı, Kazan Soda'nın yapay zekânın (YZ) sorumlu kullanımına ilişkin duruşunu ortaya koymak ve tüm iş faaliyetlerinde benimsenmesini ve kullanımını yöneten ilkeleri ve zorunlu gereklilikleri tanımlamaktır. Kazan Soda, yapay zekânın uygun şekilde ve onaylanmış sınırlar içinde kullanıldığında verimliliği, analizi, kaliteyi, inovasyonu ve karar desteğini iyileştirebileceğini kabul eder.

Aynı zamanda yapay zekâ; siber güvenlik, veri koruma, mahremiyet, fikri mülkiyet, hukuki ve düzenleyici uyum, operasyonel dayanıklılık ve emniyet açısından önemli riskler doğurur. Bu nedenle bu politika, yapay zekânın yalnızca bir teknoloji yeteneği değil, kurumsal bir yönetim meselesi olduğunu ortaya koyar. Yapay zekâ; insanları, çevreyi, bilgiyi, sistemleri, fikri mülkiyeti ve kritik operasyonları koruyan kontrollü, hesap verebilir, riske dayalı ve şeffaf bir şekilde kullanılmalıdır.

Bu politika, tüm yapay zekâ kullanımına uygulanan, pazarlık konusu olmayan ilkeleri tanımlar. İçeride geliştirilmiş, dışarıdan tedarik edilmiş, tedarikçi tarafından gömülü olarak sağlanmış veya üçüncü taraf hizmetler aracılığıyla erişilmiş olsun; yapay zekâ araçları, yapay zekâ destekli özellikler, yapay zekâ sistemleri, büyük dil modelleri ve yapay zekâ ajanlarının kullanımına ilişkin üst düzey gereklilikleri sağlar.

2. KAPSAM

Bu politika; tüm Kazan Soda çalışanlarına, yüklenicilere, danışmanlara, geçici personele ve Kazan Soda adına hareket eden üçüncü taraflara uygulanır. Kazan Soda'nın faaliyet gösterdiği tüm iş birimlerinde, bağlı ortaklıklarda, tüzel kişiliklerde, coğrafyalarda ve yargı bölgelerinde geçerlidir.

Bu politika; üretken yapay zekâ, büyük dil modelleri, makine öğrenimi, öngörücü veya optimizasyon modelleri, yazılım platformlarına gömülü yapay zekâ özellikleri, yapay zekâ destekli otomasyon, yapay zekâ destekli kodlama araçları, yapay zekâ ajanları, özel asistanlar, iş akışı ajanları ve operasyonel, endüstriyel, mühendislik, laboratuvar, lojistik, ticari, destek veya idari ortamlarda kullanılan yapay zekâ dâhil ancak bunlarla sınırlı olmamak üzere yapay zekânın tüm iş amaçlı kullanımına uygulanır.

Bu politika; pilot uygulamalar, kavram kanıtları, deneyler, test, yapılandırma, geliştirme, devreye alma, operasyon, izleme, değişiklik ve devreden çıkarma dâhil olmak üzere üretim ve üretim dışı bağlamlarda kullanılan yapay zekâya uygulanır.

Bir yapay zekâ aracının veya platformunun onaylanması, her kullanım senaryosunu, her veri kategorisini, her entegrasyonu veya her çıktı türünü otomatik olarak onaylamaz. Yapay zekâ kullanımı, Kazan Soda tarafından tanımlanan geçerli veri sınıflandırması, risk, sahiplik, onay ve kontrol gerekliliklerine tabi olmaya devam eder.

3. HEDEF

Bu politikanın hedefi, yapay zekânın açık hesap verebilirlik ve orantılı yönetim ile güvenli, yasalara uygun, sorumlu ve etkili bir şekilde kullanılmasını sağlamaktır. Politika, meşru iş değeri yaratılmasını mümkün kılarken kontrolsüz, güvenli olmayan, yasa dışı veya uygunsuz yapay zekâ kullanımını önlemeyi amaçlar.

Kazan Soda; bu kullanımın tanımlı yönetim ve kontrol sınırları içinde gerçekleştirilmesi ve emniyeti, gizliliği, bütünlüğü, erişilebilirliği, düzenleyici uyumu veya iş güvenliğini tehlikeye atmaması koşuluyla, verimliliği, inovasyonu, hizmet kalitesini, operasyonel verimliliği ve bilinçli karar desteğini artırmak için yapay zekânın sorumlu kullanımını destekler.

YAPAY ZEKA POLİTİKASI

Bu politika ayrıca; yapay zekânın yaşam döngüsü boyunca nasıl onaylanacağını, uygulanacağını, izleneceğini, gözden geçirileceğini ve kontrol edileceğini tanımlayan destekleyici yapay zekâ yönetim dokümanları, standartları, prosedürleri ve gözetim mekanizmaları için temel oluşturur.

4. TEMEL İLKELER

4.1 Hesap Verebilirlik

Tüm yapay zekâ sistemleri, yapay zekâ destekli özellikler, yapay zekâ kullanım senaryoları ve onaylı yapay zekâ araçlarının açıkça tanımlanmış insan hesap verebilirliğine sahip olması gerekir. Adı belirtilmiş bir İş Sahibi; iş amacından, kullanımından, sonuçlarından ve ilgili risklerden sorumlu olmalı ve uygun olduğunda adı belirtilmiş bir Teknik Sahip teknik uygulamadan ve operasyonel kontrolden sorumlu olmalıdır.

Yapay zekânın kullanımı, sorumluluğu bireylerden veya Kazan Soda'dan teknoloji sağlayıcısına aktarmaz. Çalışanlar, yöneticiler, sahipler ve onaylayanlar; yapay zekâ tarafından oluşturulan, bilgilendirilen veya etkilenen kararlardan, çıktılarından, eylemlerden, kayıtlardan ve iletişimlerden sorumlu olmaya devam eder.

4.2 Emniyet ve Operasyonel Bütünlük

Yapay zekâ; insanların, çevrenin, ürünlerin, tesislerin, lojistik operasyonlarının, madencilik operasyonlarının, limanların, gemilerin, laboratuvarların veya herhangi bir diğer operasyonel ortamın emniyetini tehlikeye atmamalıdır. Yapay zekâ kullanımı; operasyonel bütünlüğü, mühendislik güvencesini, süreç disiplinini ve kritik kontrollerin etkinliğini korumalıdır.

Yapay zekâ; işletme prosedürleri, tehlike kontrolleri, değişiklik yönetimi, olay müdahalesi, acil durum planlaması, süreç emniyeti gereklilikleri, mühendislik incelemesi veya zararı önlemeye ya da istikrarlı ve güvenli operasyonları sürdürmeye yönelik diğer kontrol mekanizmaları dâhil olmak üzere yerleşik emniyet çerçevelerini zayıflatmamalıdır.

4.3 Güvenlik

Yapay zekâ sistemleri, araçları, hizmetleri ve entegrasyonları; Kazan Soda'nın siber güvenlik gerekliliklerine uygun olarak seçilmeli, yapılandırılmalı, uygulanmalı ve işletilmelidir. Bu; kimlik ve erişim yönetimi, kimlik doğrulama, yetkilendirme, en az ayrıcalık, varlık yönetimi, güvenli yapılandırma, günlükleme ve izleme, zafiyet yönetimi, değişiklik yönetimi, olay yönetimi, üçüncü taraf güvenliği, güvenli geliştirme ve kimlik bilgilerinin, jetonların, gizli anahtarların ve arayüzlerin korunmasına ilişkin geçerli politikalara, standartlara ve kontrollere uyumu içerir.

Yapay zekâ; Kazan Soda'nın bilgi sistemlerine, operasyonel teknolojisine, ağlarına, uç noktalarına, uygulamalarına, verilerine, kullanıcılarına veya tedarikçilerine kabul edilemez siber risk getirmemelidir. Yapay zekâ; şirket sistemlerinin veya bilgilerinin gizliliğini, bütünlüğünü ya da erişilebilirliğini zayıflatmayan kontrolsüz bağlantılar, yetkisiz veri akışları, gizli bağımlılıklar, yönetilmeyen kod, izlenmeyen entegrasyonlar veya herhangi bir koşul oluşturmamalıdır.

4.4 Veri Koruma ve Gizlilik

Yapay zekâ kullanımı; Kazan Soda'nın veri sınıflandırması, veri işleme, mahremiyet, gizlilik, saklama ve kayıt yönetimi gerekliliklerine uygun olmalıdır. Yapay zekâ ile kullanılan tüm bilgiler kullanılmadan önce sınıflandırılmalı ve sınıflandırma düzeyine ve geçerli hukuki, düzenleyici, sözleşmesel, ticari, emniyet veya gizlilik yükümlülüklerine göre işlenmelidir.

YAPAY ZEKA POLİTİKASI

Kullanıcılar; veri sahibi veya sorumlu otorite bu kullanıma izin vermedikçe ve yapay zekâ sistemi ilgili veri sınıfı ve amaç için onaylanmadıkça, verileri yapay zekâ sistemlerine girmemeli, yüklememeli, yapıştırmamalı, eklememeli, iletmemeli veya başka şekilde ifşa etmemelidir. Veri sınıflandırması, hassasiyet, sahiplik, kullanımın yasallığı veya izin verilen hedef konusunda şüphe olduğunda, bilgi Gizli olarak değerlendirilmeli ve netleşene kadar yapay zekâ ile kullanılmamalıdır.

4.5 Şeffaflık

Yapay zekâ kullanımı; çıktıları, önerileri, analizleri, kararları, kayıtları, iletişimleri veya eylemleri önemli ölçüde etkilediği durumlarda şeffaf olmalıdır. Güven, inceleme, hesap verebilirlik, yasal uyum veya müşteri beklentisi açısından önemli olduğu durumlarda; kullanıcılar ve paydaşlar içeriğin, önerilerin veya çıktıların yapay zekâ tarafından üretilip üretilmediği, önemli ölçüde desteklenip desteklenmediği veya değiştirilip değiştirilmediği konusunda yanıtlanmalıdır.

Şeffaflık ayrıca, Kazan Soda'nın hangi yapay zekâ sistemlerinin veya araçlarının, hangi amaçla, kim tarafından ve hangi yönetim ve onay koşulları altında kullanıldığını belirleyebilmesini gerektirir. Yasaların, düzenlemelerin, müşteri yükümlülüklerinin veya iç politikaların açıklama ya da izlenebilirlik gerektirdiği durumlarda bu gereklilikler karşılanmalıdır.

4.6 Güvenilirlik ve Kalite

Yapay zekâ çıktısı; potansiyel olarak hataya açık kabul edilmeli ve faaliyetin önemi ve riskiyle orantılı bir şekilde kullanılmadan önce doğrulanmalıdır. Kazan Soda, yapay zekânın; makul görünen ancak yanlış olan içerikler de dâhil olmak üzere hatalı, eksik, güncel olmayan, yanlış, yanıltıcı, uydurma veya zayıf gerekçelendirilmiş çıktılar üretebileceğini kabul eder.

Doğrulama düzeyi bağlamı yansıtmalıdır. Düşük etkili kullanımlar kullanıcı incelemesi gerektirebilirken; emniyeti, mühendisliği, operasyonları, düzenleyici uyumu, yasal yükümlülükleri, dış taahhütleri, finansal konuları veya resmi kayıtları etkileyen kullanımlar daha kapsamlı doğrulama ve uygun olduğunda uzman incelemesi ile resmi onay gerektirir.

4.7 Sorumlu ve Yasalara Uygun Kullanım

Yapay zekâ; yasalara uygun, etik bir şekilde ve Kazan Soda'nın değerleri, iç politikaları, sözleşmesel yükümlülükleri ve düzenleyici gereklilikleriyle tutarlı biçimde kullanılmalıdır. Yapay zekâ; yasa dışı faaliyetleri, aldatmayı, dolandırıcılığı, manipülasyonu, tacizi, ayrımcılığı, kontrollerin atlatılmasını veya Kazan Soda'nın çalışanlarına, müşterilerine, tedarikçilerine, düzenleyicilere, topluluklara ya da kamuya karşı yükümlülükleriyle çelişen herhangi bir davranışı kolaylaştırmak için kullanılmamalıdır.

Sorumlu kullanım; kullanıcıların mesleki muhakeme uygulamasını, yapay zekânın sınırlamalarını anlamasını, belirsizliği üst makamlara iletmesini ve insan uzmanlığının, dikkatinin veya incelemesinin gerekli olduğu durumlarda yapay zekâ çıktılarına aşırı güvenmekten kaçınmasını gerektirir.

4.8 Değer ve Orantılılık

Yapay zekâ; verimlilik artışı, daha iyi analiz, gelişmiş kalite, inovasyon veya operasyonel verimlilik gibi meşru bir iş faydası sağladığı ve beklenen faydanın ilgili riski, çabayı ve kontrol gerekliliklerini haklı çıkardığı durumlarda kullanılmalıdır.

Yapay zekâya uygulanan yönetim, onay, kontrol, izleme ve güvence düzeyi; kullanım senaryosunun niteliğiyle, ilgili verinin hassasiyetiyle, otonomi düzeyiyle, sürecin kritikliğiyle ve hata, kötüye kullanım veya arıza potansiyel etkisiyle orantılı olmalıdır. Daha yüksek riskli kullanımlar daha güçlü kontroller, daha güçlü inceleme ve daha güçlü hesap verebilirlik gerektirir.

YAPAY ZEKA POLİTİKASI

4.9 Karar Desteęi Olarak Yapay Zekâ

Yapay zekâ; özellikle kararların emniyeti, yasal uyumu, düzenlenen operasyonları, çalışanları, müşterileri, tedarikçileri, finansal taahhütleri, mühendislik kararlarını veya diğer önemli iş çıkarlarını etkileyebileceęi durumlarda; hesap verebilir insan muhakemesinin yerine geçen bir araç olarak deęil, bir karar destek yeteneęi olarak kullanılmalıdır.

Kararlara, eylemlere ve sonuçlara ilişkin nihai sorumluluk yetkili insan personelinde kalır. Yapay zekâ önerileri, özetleri, sınıflandırmaları, üretilen içerikleri ve önerilen eylemleri sorgusuz kabul edilmemeli ve konuya uygun yetkinliğe ve yetkiye sahip kişiler tarafından gözden geçirilmelidir.

YAPAY ZEKA POLİTİKASI

5. ZORUNLU GEREKLİLİKLER

5.1 Yapay Zekâ Yönetişim Çerçevesi Kapsamında Yetkili Kullanım

Kazan Soda, yapay zekânın yalnızca kendi yapay zekâ yönetim çerçevesi içinde kullanılmasını gerektirir. Yapay zekâ sistemleri, modelleri, araçları, asistanları, ajanları, gömülü özellikleri, API'leri, eklentileri ve yapay zekâ destekli hizmetleri; yalnızca Kazan Soda tarafından açıkça onaylandıkları veya destekleyici yönetim dokümanları kapsamında tanımlanmış düşük riskli kullanım için önceden yetkilendirildikleri durumlarda iş amaçlı kullanılabilir.

Bu durum; kamuya açık yapay zekâ araçları, tarayıcı tabanlı hizmetler, masaüstü veya mobil uygulamalar, tedarikçi tarafından gömülü yapay zekâ özellikleri, kod asistanları, yapay zekâ eklentileri, yapay zekâ ajanları, yapay zekâ özelliğine sahip otomasyon araçları ve harici yapay zekâ API'leri için de eşit şekilde geçerlidir. Yetkilendirme; riske, veri hassasiyetine ve iş etkisine bağlı olarak araç düzeyinde, kullanım senaryosu düzeyinde veya kategori düzeyinde verilebilir.

Kazan Soda; bu gerekliliği uygulamak ve şirket verilerini, sistemlerini ve çıkarlarını korumak için yapay zekâ kullanımını izleyebilir, kısıtlayabilir, engelleyebilir veya soruşturabilir.

5.2 Hesap Verebilirlik ve Sahiplik

İş amaçlı kullanılan her yapay zekâ sistemi, yapay zekâ destekli hizmet, yapay zekâ entegrasyonu, onaylı yapay zekâ aracı ve yapay zekâ kullanım senaryosunun açıkça atanmış sahipliğe sahip olması gerekir.

İş Sahibi; yapay zekâ kullanım senaryosunun iş amacından, kullanımının meşruiyetinden, sonuçlarından, risklerinden ve uyumundan sorumludur. İş Sahibi; kullanımın gerekçelendirildiğinden, kullanım senaryosunun onaylanmış sınırlar içinde kaldığından, kullanıcıların uygun şekilde eğitildiğinden ve çıktılarının uygun şekilde kullanıldığından emin olmalıdır.

Teknik Sahip; teknik uygulamadan, yapılandırmadan, entegrasyondan, operasyondan, bakımdan, teknik yaşam döngüsü yönetiminden ve geçerli güvenlik ve teknoloji kontrollerinin koordinasyonundan sorumludur. Teknik Sahip; çözümün onaylanmış mimariye, erişim, izleme, değişiklik ve destek gerekliliklerine uygun olarak devreye alındığından ve işletildiğinden emin olmalıdır.

Yöneticiler; ekiplerindeki yapay zekâ kullanımının bu politikaya uygun olmasını ve inceleme ya da onay gerektiren kullanımın uygun şekilde üst makamlara iletilmesini sağlamaktan sorumludur. Bireysel kullanıcılar; yapay zekâyı ne girdikleri, çıktıları nasıl doğruladıkları ve onaylanmış kullanım koşulları içinde hareket edip etmedikleri konusunda sorumlu olmaya devam eder.

Hiçbir yapay zekâ yeteneği, açık sahiplik olmadan iş bağlamında kullanılamaz. Sahiplik belgelenmeli ve kullanım senaryosunun yaşam döngüsü boyunca güncel tutulmalıdır.

5.3 Veri Koruma ve Kullanım Kısıtlamaları

Yapay zekâ ile kullanılan tüm veriler; Kazan Soda'nın veri sınıflandırması ve işleme gerekliliklerine uygun olarak sınıflandırılmalı ve işlenmelidir. Yapay zekâyı kullanmadan önce kullanıcılar; bilginin Kamuya Açık, Dahili, Gizli, Kısıtlı veya başka şekilde mahremiyet, sözleşme, hukuki, emniyet, güvenlik, ihracat kontrolü ya da düzenleyici kısıtlamalara tabi olup olmadığını belirlemelidir.

Kullanıcılar; aşağıdakileri onaylanmamış veya yetkili olmayan herhangi bir yapay zekâ sistemine girmemeli, yüklememeli, eklememeli, yapıştırmamalı, iletmemeli veya başka şekilde ifşa etmemelidir: gizli iş bilgileri, ticari sırlar, fikri mülkiyet, süreç veya mühendislik bilgileri, formüller, tasarımlar, operasyonel bilgiler, kişisel veriler,

YAPAY ZEKA POLİTİKASI

tedarikçi veya müşteri bilgileri, finansal bilgiler, hukuki veya sözleşmesel bilgiler, güvenlik bilgileri, kimlik bilgileri, sistem yapılandırma verileri, emniyet açısından kritik bilgiler, düzenlemeye tabi bilgiler veya ifşası, kötüye kullanımı, kaybı ya da değiştirilmesi Kazan Soda'ya veya başkalarına zarar verebilecek herhangi bir veri.

Bu tür bilgilerin kullanımına yalnızca yapay zekâ sistemi o veri sınıfı için açıkça onaylandığında ve uygun sözleşmesel, teknik ve organizasyonel güvenceler mevcut olduğunda izin verilir. Şüphe durumunda bilgi kullanılmamalıdır.

5.4 Güvenlik ve Teknoloji Kontrolleri

Tüm yapay zekâ sistemleri, hizmetleri, ajanları, entegrasyonları ve yapay zekâ destekli özellikleri; kullanımdan önce ve yaşam döngüleri boyunca geçerli siber güvenlik ve teknoloji yönetişimi gerekliliklerine uymalıdır.

Bu; uygun olduğu şekilde güvenli kimlik doğrulama ve yetkilendirme, en az ayrıcalıklı erişim, onaylanmış teknik mimari, güvenli yapılandırma, günlüklenme ve izleme, zafiyet ve yama yönetimi, kimlik bilgilerinin, jetonların ve gizli anahtarların korunması, iç sistemler ve API'lerle güvenli entegrasyon, değişiklik yönetimi, sürüm kontrolü, olay tespiti ve müdahalesi, güvenli geliştirme uygulamaları ve harici sağlayıcıların söz konusu olduğu durumlarda üçüncü taraf güvenlik incelemesini içerir.

Yapay zekâ; onaylanmış teknoloji kontrollerini atlayan, yönetilmeyen bağlantılar oluşturan, izin verilmeyen otomasyonu mümkün kılan, güvenlik izlemesini zayıflatan veya şirket sistemlerine uygun inceleme, test ve onay olmaksızın kod, yapılandırma ya da mantık katan bir şekilde uygulanmamalıdır.

Yapay zekânın geliştirme ortamlarına, iş birliği platformlarına, kurumsal uygulamalara, veri depolarına veya altyapıya bağlandığı durumlarda, bu ortamlara ilişkin geçerli güvenlik ve teknoloji gereklilikleri tam olarak uygulanmaya devam eder.

5.5 İnsan Gözetimi

Bir hata, eksiklik, halüsinasyon, yanlışlık, güvenlik zayıflığı veya yanlış anlama; emniyete, uyuma, mahremiyete, hukuki konuma, finansal çıkarlara, çalışanlara, müşterilere, tedarikçilere, operasyonlara veya itibara zarar dâhil olmak üzere önemli zarara yol açabileceği durumlarda, yapay zekâ kararlar veya eylemler için tek dayanak olarak kullanılmamalıdır.

İnsan gözetimi anlamlı ve riskle orantılı olmalıdır. Sorumlu kişi; kullanımın bağlamını ve amacını anlamalı, yapay zekâ çıktısının makul olup olmadığını değerlendirebilmeli, gerektiğinde çıktılara güvenmeden önce bunları gözden geçirebilmeli ve gerektiğinde yapay zekâ destekli faaliyete itiraz edebilmeli, onu reddedebilmeli, geçersiz kılabilmesi veya durdurabilmesidir.

İnsan gözetimi her zaman yapay zekâ çıktı döngüsünün bir parçası olmalıdır; teknoloji olgunlaştıkça ve uygulanan kullanım senaryosu ilerledikçe, gözetim düzeyi veya döngüleri risk seviyelerine bağlı olarak azaltılabilir.

İnsan incelemesi yüzeysel bir onay adımı olarak değerlendirilmemelidir. Konunun daha yüksek riskli, teknik olarak karmaşık veya operasyonel açıdan hassas olduğu durumlarda, inceleme uygun şekilde nitelikli personel tarafından gerçekleştirilmelidir.

5.6 Emniyet ve Kritik Operasyonlar

Yapay zekâ; emniyeti, süreç bütünlüğünü, mühendislik güvencesini, kritik kontrolleri, çevre korumasını veya ticari ve endüstriyel süreçlerin güvenilir işleyişini tehlikeye atacak şekilde kullanılmamalıdır.

YAPAY ZEKA POLİTİKASI

Yapay zekâ; emniyet açısından kritik işlevleri otonom olarak kontrol etmemeli, emniyet prosedürlerini veya tehlike kontrollerini onay olmaksızın değiştirmemeli, mühendislik incelemesini ya da değişiklik yönetimini atlamamalı veya emniyeti, tehlikeli operasyonları, düzenlemeye tabi süreçleri ya da acil durum müdahalesini etkileyen konularda doğrulama olmaksızın güvenilmemelidir.

Yapay zekânın OT/ICS ortamlarında, süreç kontrol sistemlerinde veya diğer üretim kontrol ortamlarında kullanılması, Kazan Soda resmi olarak onaylamadıkça bu politika sürümü kapsamında izinli değildir.

Yapay zekânın operasyonel, endüstriyel, madencilik, lojistik, mühendislik, kalite, laboratuvar veya emniyetle ilgili bağlamlarda kullanılması önerildiğinde, kullanım; uygun teknik, emniyet, siber güvenlik, operasyonel ve uyum paydaşlarının katılımı dâhil olmak üzere kapsamlı inceleme ve kontrole tabi olmalıdır.

5.7 Üçüncü Taraf ve Tedarik Kontrolleri

Herhangi bir üçüncü taraf yapay zekâ ürünü, tedarikçi yapay zekâ özelliği, barındırılan yapay zekâ hizmeti, dış kaynaklı yapay zekâ destekli çözüm veya harici yapay zekâ sağlayıcısı; onay veya kullanımdan önce uygun durum tespitine tabi olmalıdır.

Durum tespiti; uygun olduğu şekilde veri işleme ve saklama uygulamalarını, şirket verilerinin model eğitiminde kullanılıp kullanılmadığını, barındırma ve veri konumunu, gizlilik ve fikri mülkiyet korumasını, güvenlik kontrollerini ve sertifikalarını, sözleşmesel korumaları ve kısıtlamaları, olay bildirim yükümlülüklerini, destek ve dayanıklılığı, önemli değişikliklerin şeffaflığını, entegrasyon risklerini ve erişim gerekliliklerini ele almalıdır.

Hiçbir üçüncü taraf yapay zekâ çözümü; ilgili iş, BT, siber güvenlik, mahremiyet, hukuk, satın alma ve diğer gerekli paydaşların uygun incelemesi olmaksızın benimsenemez.

5.8 Uyum ve Yasalara Uygun Kullanım

Yapay zekâ; geçerli yasalara, düzenlemelere, sözleşmesel yükümlülüklere, iç politikalara ve mesleki yükümlülüklere uygun olarak kullanılmalıdır. Bu; veri koruma, mahremiyet, gizlilik, fikri mülkiyet, kayıt yönetimi, güvenlik, iş sağlığı ve güvenliği, sektöre özgü düzenlemeler ile adil ve sorumlu davranışa ilişkin gereklilikleri içerir.

Kullanıcılar; yasa dışı, yanıltıcı, aldatıcı, ayrımcı, taciz edici, manipülatif veya Kazan Soda politikası ya da yükümlülükleriyle tutarsız içerikleri, eylemleri ya da kararları oluşturmak veya desteklemek için yapay zekâyı kullanmamalıdır. Yasa veya düzenlemenin belirli bir insan incelemesi, izlenebilirlik, belgeleme ya da yetkilendirme gerektirdiği durumlarda, yapay zekâ kullanımı bu gereklilikler karşılanmaya devam edecek şekilde tasarlanmalı ve işletilmelidir.

5.9 Çıktı Doğrulama ve Sorumlu Kullanım

Tüm yapay zekâ tarafından üretilen veya yapay zekâ destekli çıktılar; güvenilmeden, dışarıyla paylaşılmadan, kayıtlara dâhil edilmeden, analizde kullanılmadan veya eylemleri ya da kararları desteklemek için kullanılmadan önce gözden geçirilmeli ve doğrulanmalıdır.

Doğrulamanın derinliği riski ve bağlamı yansıtmalıdır. Kullanıcılar; çıktının doğru, eksiksiz, güncel, uygun şekilde kaynaklandırılmış, amaç için yeterince tarafsız ve kullanıma uygun olup olmadığını değerlendirmelidir. Yapay zekâ çıktıları; iyi yazılmış, teknik olarak ifade edilmiş veya kendinden emin bir şekilde sunulmuş olmaları nedeniyle doğru varsayılmamalıdır.

Yapay zekâ tarafından üretilen veya yapay zekâ destekli içerik; insan tarafından oluşturulan içerik için gereken aynı düzeyde inceleme, onay ve kayıt kontrolü olmaksızın resmi bir kayıt, düzenleyici sunum, hukuki iletişim,

YAPAY ZEKA POLİTİKASI

müşteri taahhüdü, emniyet talimatı, mühendislik talimatı, kalite kararı veya dışarıya yayımlanan bir beyan olarak yayımlanmamalıdır.

Kullanıcılar; nihai iş ürününden, karardan, iletişimden veya eylemden sorumlu olmaya devam eder. Yapay zekâ desteği; doğrulama, eleştirel düşünme ve muhakeme uygulama yükümlülüğünü ortadan kaldırmaz.

5.10 Yasaklı Kullanım

Kazan Soda; onaylanmış yönetim sınırlarının dışında kalan veya emniyete, güvenliğe, mahremiyete, fikri mülkiyete, yasal uyuma ya da operasyonel bütünlüğe kabul edilemez risk oluşturan yapay zekâ kullanımını yasaklar. Ayrıntılı yasaklı kullanım kategorileri ve kontrol sınırları, Yapay Zekâ Kullanım ve Yönetişim Politikası ile ilgili standartlarda tanımlanmıştır.

En azından, yasaklı kullanım; yetkisiz yapay zekâ araçlarını veya hizmetlerini, korunan verilerin ya da fikri mülkiyetin yetkisiz ifşasını, yetkisiz otonom eylemi ya da sistem değişikliğini, onaylanmış kontrolleri atlayan kullanımı ve emniyet açısından kritik veya OT/ICS bağlamlarında herhangi bir yasaklı yapay zekâ kullanımını içerir.

5.11 Üretken Yapay Zekâ ve Büyük Dil Modellerinin (BDM) Kullanımı

Kazan Soda; üretken yapay zekânın ve büyük dil modellerinin verimlilik ve analitik fayda sağlayabileceğini, ancak aynı zamanda gizlilik, veri sızıntısı, fikri mülkiyet, doğruluk, yanlılık ve kontrolsüz içerik üretimine ilişkin artan riskler de oluşturduğunu kabul eder.

Kazan Soda; gerekçelendirildiği durumlarda iş amaçlı kullanım için onaylı güvenli yapay zekâ platformları sağlayacak veya belirleyecektir. Şirket işleri için yalnızca onaylı büyük dil modelleri kullanılabilir. Kamuya açık veya onaylanmamış büyük dil modelleri; tanımlı koşullar altında açıkça yetkilendirilmedikçe Kazan Soda işleri için kullanılmamalıdır.

Kullanıcılar; büyük dil modeli Kazan Soda tarafından onaylanmadıkça, amaçlanan kullanım yetkilendirilmedikçe, ilgili veri sınıfına izin verilmedikçe ve sözleşmesel, güvenlik, mahremiyet ve gizlilik güvenceleri mevcut olmadıkça, bir büyük dil modeline bilgi girmemeli, yüklememeli, eklememeli, yapıştırmamalı veya başka şekilde ifşa etmemelidir.

Kazan Soda'nın fikri mülkiyeti; formüller, mühendislik spesifikasyonları, tasarımlar, teknik dokümantasyon, süreç bilgisi, optimizasyon parametreleri, operasyonel yöntemler, araştırma bilgileri ve diğer tescilli bilgiler dâhil olmak üzere, onaylanmamış herhangi bir büyük dil modeline veya harici yapay zekâ hizmetine ifşa edilmemelidir. Bilginin fikri mülkiyet veya gizli bilgi oluşturup oluşturmadığı konusunda belirsizlik olduğunda, Gizli olarak değerlendirilmeli ve kullanılmamalıdır.

Kazan Soda; büyük dil modeli kullanımını izleyebilir, erişimi kısıtlayabilir, yetkisiz kullanımı tespit edebilir ve şirket bilgilerinin veri sızıntısını, kötüye kullanımını veya ifşasını önlemek için teknik kontroller uygulayabilir.

5.12 Yapay Zekâ Ajanları, Otonom Sistemler ve Yapay Zekâ Destekli Geliştirme

Yapay zekâ ajanları, otonom asistanlar, araç kullanan yardımcı pilotlar (copilot), iş akışı ajanları ve yapay zekâ destekli geliştirme yetenekleri; yükselen güvenlik, operasyonel ve yönetim riski oluşturur ve bu nedenle belirli onay, sahiplik ve kontrol gerekliliklerine tabidir.

Bu tür yetenekler yalnızca onaylanmış BT ve yönetim süreçleri aracılığıyla devreye alınabilir ve tanımlı sahiplik, onaylanmış mimari, güvenli geliştirme ve değişiklik kontrolü, günlüklenme, erişim kontrolü, test ve insan gözetimi altında çalışmalıdır.

YAPAY ZEKÂ POLİTİKASI

Yapay zekâ ajanları, otonom sistemler ve yapay zekâ destekli geliştirmeye ilişkin ayrıntılı kısıtlamalar, onay koşulları ve teknik kontrol gereklilikleri, Yapay Zekâ Kullanım ve Yönetişim Politikası ile destekleyici standartlarda tanımlanmıştır.

BT veya diğer yetkili teknik ekipler tarafından kullanılsa bile, yapay zekâ destekli geliştirme; güvenli geliştirme, akran incelemesi, test, güvenlik değerlendirmesi, değişiklik kontrolü ve onay gerekliliklerine tabi olmaya devam etmelidir.

6. ROLLER VE SORUMLULUKLAR

Kazan Soda; yönetim, iş, teknik ve kontrol işlevleri aracılığıyla yapay zekâ yönetişimi için açık hesap verebilirlik atar. Ayrıntılı sorumluluklar, Yapay Zekâ Kullanım ve Yönetişim Politikası ile destekleyici standartlarda tanımlanmıştır.

Yürütme Komitesi ve Politika Sahibi; genel politika çerçevesinden, yönetim yönünden ve Kazan Soda genelinde yapay zekâ kullanımının periyodik gözden geçirilmesinden sorumludur.

İş Sahipleri ve Teknik Sahipler; iş amacı, uygun kullanım, operasyon ve geçerli yönetim gerekliliklerine uyum dâhil olmak üzere kendi sorumluluk alanlarındaki onaylı yapay zekâ kullanımından sorumludur.

Siber Güvenlik, Mahremiyet, Hukuk, Uyum, Satın Alma, Yöneticiler ve Kullanıcılar; Kazan Soda'nın yapay zekâ yönetim çerçevesi kapsamında kendilerine atanan kontrol, gözetim, üst makamlara iletme ve sorumlu kullanım faaliyetlerini gerçekleştirmekten sorumlu olmaya devam eder.

Mahremiyet ve Veri Koruma; kişisel verilerin ve düzenlemeye tabi bilgilerin kullanımının geçerli veri koruma yükümlülüklerine ve iç veri yönetişimi gerekliliklerine uygun olmasını sağlamaktan sorumludur.

Hukuk ve Uyum; yapay zekâ kullanımıyla ilgili hukuki, düzenleyici, sözleşmesel, kayıt ve etik yükümlülükler konusunda danışmanlık yapmaktan ve dış taahhütler ile düzenlemeye tabi faaliyetler üzerindeki kontrolü desteklemekten sorumludur.

Satın Alma ve Üçüncü Taraf Yönetimi; durum tespitini, sözleşme incelemesini, tedarikçi güvencesini ve üçüncü taraf yapay zekâ çözümlerinin kontrollü edinimini desteklemekten sorumludur.

Yöneticiler; ekiplerindeki personelin bu politikayı anlamasını ve uygulamasını, gerekli eğitimleri tamamlamasını ve onay gerektiren yapay zekâ kullanımını üst makamlara iletmesini sağlamaktan sorumludur.

Çalışanlar ve Kullanıcılar; yalnızca onaylı yapay zekâyı kullanmaktan, verileri korumaktan, çıktıları doğrulamaktan, eğitimleri takip etmekten, belirsizliği üst makamlara iletmekten ve olayları, kötüye kullanımları ya da endişeleri raporlamaktan sorumludur.

HSSE (İSG ve Çevre); ilgili tesis, maden ve OT/ICS ile ilgili kullanım senaryoları dâhil olmak üzere sağlığı, emniyeti, güvenliği, çevreyi, operasyonel riski, kritik kontrolleri veya olay yönetimini etkileyebilecek yapay zekâ kullanımları için gözetim ve konu uzmanlığı sağlar.

YAPAY ZEKA POLİTİKASI

7. YÖNETİŞİM VE GÖZETİM

Kazan Soda; görünürlük, hesap verebilirlik, orantılı kontrol ve işlevler arası inceleme sağlayan bir yapay zekâ yönetim çerçevesi sürdürecektir.

Yapay zekâ yönetimi riske dayalı olacaktır. Hassas veri, düzenlemeye tabi faaliyetler, dışarıya yönelik çıktılar, resmi kayıtlar, sistem entegrasyonları, yapay zekâ destekli geliştirme, yapay zekâ ajanları, operasyonel etki veya emniyet açısından önem içeren kullanımlar, kapsamlı inceleme ve kontrole tabi olacaktır. Destekleyici yönetim dokümanları, uygun olduğunda önceden yetkilendirilmiş düşük riskli kullanımı ve hızlandırılmış onayları tanımlayabilir.

Yönetişim; uygun olduğu durumlarda iş, BT, siber güvenlik, mahremiyet, hukuk, uyum, satın alma, HSSE ve operasyonel paydaşlar dâhil olmak üzere ilgili işlevleri kapsayacaktır.

Kazan Soda; kontrolü, izlemeyi, incelemeyi, güvenceyi ve denetlenebilirliği desteklemek için onaylı yapay zekâ araçları, onaylı yapay zekâ kullanım senaryoları, yapay zekâ destekli çözümler ve uygun olduğunda sahiplik, amaç ve risk durumu üzerinde görünürlük sürdürecektir.

Yapay zekâ kullanımının yaşam döngüsü boyunca; değerlendirme, onay, uygulama, operasyon, izleme, değişiklik, periyodik gözden geçirme ve devreden çıkarma dâhil olmak üzere uygun yönetim uygulanacaktır.

8. UYUM, İSTİSNALAR VE YAPTIRIM

Bu politikaya uyum zorunludur. Kazan Soda adına hareket eden tüm personel ve üçüncü taraflar, gerekliliklerine uymalıdır.

İstisnalar; resmi olarak talep edilmeli, risk değerlendirmesine tabi tutulmalı, belgelenmeli, uygun otorite tarafından onaylanmalı ve süreyle sınırlı olmalıdır. Yasa dışı faaliyet, kabul edilemez emniyet riski veya güvenlik, mahremiyet, fikri mülkiyet ya da düzenleyici yükümlülüklerin önemli ölçüde ihlali yaratacak hiçbir istisna verilemez.

Kazan Soda; bu politikaya uyumu doğrulamak ve yetkisiz, güvenli olmayan ya da uyumsuz yapay zekâ kullanımını tespit etmek için izleme, inceleme, denetim ve güvence faaliyetleri gerçekleştirebilir.

Yapay zekâ ile ilgili olaylar gecikmeksizin raporlanmalıdır. Olaylar; yapay zekâ araçları aracılığıyla veri sızıntısını, yetkisiz yapay zekâ kullanımını, güvenli olmayan veya hatalı yapay zekâ çıktıları, yapay zekâ içeren güvenlik ihlalini, yapay zekâ kullanılarak oluşturulan yetkisiz kod ya da otomasyonu, yetkisiz yapay zekâ ajanı faaliyetini veya yapay zekânın hukuki, operasyonel, emniyet, mahremiyet, fikri mülkiyet ya da güvenlik riskine katkıda bulunduğu herhangi bir olayı içerir ancak bunlarla sınırlı değildir.

Uyumsuzluk; erişimin kaldırılması, zorunlu yeniden eğitim, disiplin işlemi, sözleşmesel işlem, hukuki süreç veya ihlalin riski ve ciddiyetiyle orantılı diğer önlemlerle sonuçlanabilir.

Kazan Soda; iyi niyetli endişe bildirimlerini destekleyecek ve yapay zekâ ile ilgili endişeleri sorumlu bir şekilde dile getiren bireylere karşı misillemeye müsamaha göstermeyecektir.

9. İLGİLİ DOKÜMANLAR VE ÇERÇEVE UYUMU

Bu politika; bilgi güvenliği, kabul edilebilir kullanım, veri sınıflandırması ve işleme, mahremiyet, kayıt yönetimi, risk yönetimi, güvenli geliştirme, üçüncü taraf riski, iş sağlığı ve güvenliği, olay yönetimi ve değişiklik yönetimine

YAPAY ZEKA POLİTİKASI

ilişkin politikalar, standartlar ve prosedürler dâhil olmak üzere Kazan Soda'nın daha geniş yönetim çerçevesiyle birlikte okunmalıdır.

Bu politika; operasyonel yönetim modelini, ayrıntılı teknik gereklilikleri, onay beklentilerini ve yapay zekâ kullanımına ilişkin kanıt gerekliliklerini tanımlayan Yapay Zekâ Kullanım ve Yönetişim Politikası, Yapay Zekâ Standardı ile diğer ilgili prosedürler, kılavuzlar ve işletme kontrolleri tarafından desteklenir.

Gerekliliklerin çakıştığı durumlarda, daha katı kontrol uygulanır.

10. TANIMLAR

Yapay Zekâ (YZ); üretken yapay zekâ, makine öğrenimi, öngörücü veya optimizasyon modelleri, gömülü yapay zekâ özellikleri, büyük dil modelleri, yapay zekâ asistanları ve yapay zekâ ajanları dâhil olmak üzere yapay zekâ yeteneklerini ifade eder.

Yapay Zekâ Ajansı; eylem gerçekleştirebilen, araç kullanabilen, sistemlerle etkileşime girebilen, API'leri çağırabilen, iş akışlarını yürütebilen veya basit içerik üretiminin ötesinde belirli bir özerklik düzeyiyle hareket edebilen yapay zekâ destekli bir yeteneği ifade eder.

Onaylı Yapay Zekâ Aracı; Kazan Soda tarafından tanımlı iş amaçlı kullanım için resmi olarak değerlendirilmiş ve yetkilendirilmiş bir yapay zekâ platformunu, aracını, hizmetini, modelini veya özelliğini ifade eder.

İş Sahibi; bir yapay zekâ kullanım senaryosunun amacından, kullanımından, sonuçlarından ve riskinden sorumlu, hesap verebilir iş rolünü ifade eder.

Teknik Sahip; bir yapay zekâ sisteminin veya hizmetinin uygulanmasından, yapılandırılmasından, entegrasyonundan, operasyonundan ve teknik kontrolünden sorumlu, hesap verebilir teknik rolü ifade eder.

Üretken Yapay Zekâ veya BDM; istemlere ya da veri girdilerine dayalı olarak metin, kod, görsel, özet, öneri veya diğer çıktıları üretebilen yapay zekâ sistemlerini ifade eder.

Gömülü Yapay Zekâ Özelliği; başka bir yazılım ürünü, platformu veya tedarikçi hizmeti içinde yer alan yapay zekâ yeteneğini ifade eder.

İnsan Gözetimi; yapay zekâ destekli faaliyeti gerektiğinde anlayabilen, değerlendirebilen, ona itiraz edebilen, onu geçersiz kılabilen veya durdurabilen yetkili bir kişi tarafından gerçekleştirilen anlamlı inceleme ve kontrolü ifade eder.

Yapay Zekâ Destekli Geliştirme; yapay zekâ tarafından üretilen çıktıları kullanarak kod, betik, otomasyon veya uygulamaların oluşturulmasını, değiştirilmesini ya da devreye alınmasını ifade eder ve güvenli geliştirme, inceleme, test ve değişiklik kontrolü gerekliliklerine tabi olmaya devam eder.

Gizli Veri; fikri mülkiyet, ticari sırlar, ticari bilgiler, teknik bilgiler ve diğer korunan iş bilgileri dâhil olmak üzere, ifşa edilmesi, değiştirilmesi, kötüye kullanılması veya kaybedilmesi durumunda Kazan Soda'ya ya da başkalarına zarar verebilecek kamuya açık olmayan bilgileri ifade eder.

Kısıtlı Veri; mahremiyet, emniyet, güvenlik, hukuki, düzenleyici veya operasyonel hassasiyet nedeniyle daha yüksek koruma gerekliliklerine tabi verileri ifade eder.

YAPAY ZEKA POLİTİKASI

11. EĞİTİM, GÖZDEN GEÇİRME VE BAKIM

Personel; Kazan Soda tarafından gerekli görüldüğü durumlarda iş amaçlı onaylı yapay zekâyı kullanmadan önce gerekli yapay zekâ ile ilgili eğitimi tamamlamalı ve geçerli yönetim gerekliliklerinde belirtildiği şekilde tazeleme veya role dayalı eğitimleri tamamlamalıdır.

Kazan Soda; bu politikayı en az yılda bir kez ve düzenleme, iş operasyonları, teknoloji, tehdit ortamı, olay deneyimi veya organizasyonel yönetimde önemli değişiklikler olduğunda gözden geçirecektir.

Kazan Soda; politikanın etkili, güncel ve denetlenebilir kalmasını sağlamak için onaylı yapay zekâ araçları, onaylı kullanım senaryoları, sahiplik ve politika güncellemeleri üzerinde uygun görünürlüğü sürdürecektir.

GENEL MÜDÜR