ENTEGRE YÖNETİM SİSTEMİ POLİTİKASI

DOCUART olarak; faaliyetlerimizi müşteri memnuniyeti, kalite, bilgi güvenliği, **kişisel verilerin ve mahremiyetin korunması**, iş sürekliliği, çevrenin korunması ve çalışanlarımızın sağlık ve güvenliğinin gözetilmesi anlayışıyla yürütmeyi temel ilke edinmiş bulunmaktayız.

Bu doğrultuda; **ISO 9001 Kalite Yönetim Sistemi, ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi, ISO/IEC 27701 Gizlilik Bilgi Yönetim Sistemi, ISO 22301 İş Sürekliliği Yönetim Sistemi, ISO 14001 Çevre Yönetim Sistemi ve ISO 45001 İş Sağlığı ve Güvenliği Yönetim Sistemi** standartlarının gerekliliklerini esas alan Entegre Yönetim Sistemimizi oluşturmayı, uygulamayı, sürdürmeyi ve sürekli olarak iyileştirmeyi taahhüt ederiz.

Bu kapsamda;

- Müşterilerimizin ihtiyaç, beklenti ve uygulanabilir şartlarını karşılayan **kaliteli, güvenilir, gizliliğe duyarlı ve sürdürülebilir hizmetler** sunmayı ve müşteri memnuniyetini sürekli geliştirmeyi,
- Kuruluşumuzun amaç ve yönü ile uyumlu **kalite, bilgi güvenliği, gizlilik, kişisel veri koruma, iş sürekliliği, çevre ve iş sağlığı ve güvenliği hedefleri** belirlemeyi ve bu hedeflerin gerçekleştirilmesini desteklemeyi,
- Tüm bilgi varlıklarımızın **gizlilik, bütünlük ve erişilebilirlik** ilkeleri doğrultusunda korunmasını sağlamayı; bilgi güvenliği risklerini sistematik şekilde değerlendirmeyi, ele almayı ve yönetmeyi,
- **Kişisel verilerin ve diğer kişisel olarak tanımlanabilir bilgilerin (PII) hukuka uygun, adil, şeffaf, amaçla sınırlı ve gerekli olduğu ölçüde işlenmesini** sağlamayı,
- Kişisel verilerin işlenmesi, saklanması, aktarılması, erişilmesi ve imha edilmesine ilişkin **gizlilik risklerini belirlemeyi, değerlendirmeyi ve uygun kontrollerle yönetmeyi**,
- Kişisel veri sahiplerinin ve ilgili tarafların uygulanabilir mevzuat ve sözleşmeler kapsamında sahip olduğu **bilgi edinme, erişim, düzeltme, silme, itiraz ve diğer haklarının** desteklenmesini sağlamayı,
- Kişisel verilerin yetkisiz veya hukuka aykırı işlenmesini, erişilmesini, değiştirilmesini, kaybolmasını, ifşa edilmesini veya amaç dışı kullanılmasını önlemek amacıyla **uygun teknik ve idari kontrolleri** uygulamayı,
- Kişisel verilerin işlenmesi faaliyetlerinde **veri minimizasyonu, amaçla sınırlılık, saklama süresinin sınırlandırılması ve doğruluk** ilkelerini gözetmeyi,
- Kişisel verilerin üçüncü taraflara aktarılması, hizmet alınan taraflarla paylaşılması veya sınır ötesi aktarılması gereken durumlarda **uygulanabilir yasal, düzenleyici ve sözleşmesel şartları** dikkate almayı,
- Kişisel veri işleme faaliyetlerini, ilgili tarafları, amaçları ve gerekli olduğu ölçüde veri kategorilerini belirlemeyi ve bunlara ilişkin **gizlilik bilgi yönetimi süreçlerini** oluşturmayı ve sürdürmeyi,
- Kişisel verilerin korunmasına ilişkin yükümlülükleri yerine getirmek amacıyla gerekli durumlarda **gizlilik etki değerlendirmeleri ve benzeri risk değerlendirme çalışmalarını** gerçekleştirmeyi,

- Kişisel veri ihlalleri ve gizlilik olaylarının belirlenmesi, değerlendirilmesi, bildirilmesi, müdahale edilmesi ve gerekli düzeltici faaliyetlerin gerçekleştirilmesine yönelik **olay yönetimi süreçlerini** işletmeyi,
- Faaliyetlerimizin sürekliliğini etkileyebilecek tehdit ve riskleri belirleyerek **iş sürekliliğini sağlamak**, kritik faaliyetlerin kabul edilebilir sürelerde sürdürülebilmesini ve kesintiler sonrasında uygun şekilde yeniden başlatılmasını desteklemek,
- Faaliyetlerimizden kaynaklanan çevresel etkileri belirlemeyi ve yönetmeyi; **çevrenin korunmasını, kirliliğin önlenmesini ve olumsuz çevresel etkilerin azaltılmasını** sağlamak,
- Faaliyetlerimizin çevresel performansını geliştirmek amacıyla **kaynakların verimli kullanılmasını, enerji ve doğal kaynak tüketiminin azaltılmasını, atıkların azaltılmasını ve uygun şekilde yönetilmesini** desteklemek,
- İklim değişikliği ve kuruluşumuzun faaliyetleriyle ilişkili diğer çevresel konuları, uygulanabilir olduğu ölçüde yönetim sistemimizin amaç ve faaliyetlerinde dikkate almak,
- Çalışanlarımızın ve faaliyetlerimizden etkilenebilecek diğer kişilerin **iş sağlığı ve güvenliğini korumayı**, iş kazaları, yaralanmalar ve işle ilgili sağlık bozulmalarının önlenmesini sağlamayı,
- Faaliyetlerimizde ortaya çıkabilecek **İSG tehlikelerini ortadan kaldırmayı ve İSG risklerini azaltmayı**, güvenli ve sağlıklı çalışma koşullarının oluşturulmasını ve sürdürülmesini sağlamayı,
- Çalışanların iş sağlığı ve güvenliği konularında **danışma ve katılımını** desteklemeyi, görüş ve önerilerinin yönetim sistemi içerisinde değerlendirilmesini sağlamayı,
- Faaliyetlerimizle ilgili **uygulanabilir yasal şartlara, düzenleyici şartlara, sözleşmesel yükümlülüklere ve kuruluşumuzun uymayı taahhüt ettiği diğer şartlara** uygun hareket etmeyi,
- Kalite, bilgi güvenliği, **gizlilik ve kişisel veri koruma**, iş sürekliliği, çevre ve İSG ile ilgili **risk ve fırsatları belirlemeyi, değerlendirmeyi ve uygun kontrollerle yönetmeyi**,
- Yönetim sistemlerinin etkinliğini desteklemek amacıyla süreçlerimizin performansını, hedeflerimizi ve ilgili göstergelerimizi **izlemeyi, ölçmeyi, değerlendirmeyi ve gerektiğinde iyileştirmeyi**,
- Yönetim sisteminin gerektirdiği **yetkinlik, farkındalık, eğitim ve iletişim** faaliyetlerini gerçekleştirmeyi; çalışanlarımızın Entegre Yönetim Sistemi içerisindeki sorumluluklarının ve katkılarının farkında olmasını sağlamayı,
- İç ve dış iletişim ihtiyaçlarını belirleyerek yönetim sistemleriyle ilgili bilgilerin **doğru, zamanında ve uygun şekilde paylaşılmasını** sağlamayı,
- Acil durumlar, iş sürekliliğini tehdit eden olaylar, çevresel acil durumlar, İSG riskleri ve **bilgi güvenliği ile gizlilik olayları** karşısında hazırlıklı olmayı, müdahale kapasitemizi geliştirmeyi ve gerekli durumlarda müdahale süreçlerini test ederek gözden geçirmeyi,
- Yönetim sistemlerinin uygunluğunu, yeterliliğini ve etkinliğini **düzenli olarak gözden geçirmeyi** ve elde edilen sonuçlar doğrultusunda gerekli iyileştirmeleri gerçekleştirmeyi,
- Uygunsuzlukların ve bilgi güvenliği/gizlilik olaylarının nedenlerini ele almayı, gerekli düzeltici faaliyetleri gerçekleştirmeyi ve benzer uygunsuzlukların tekrarını önlemeyi,

- Entegre Yönetim Sisteminin **kalite, bilgi güvenliği, gizlilik, kişisel veri koruma, iş sürekliliği, çevre ve İSG performansını sürekli iyileştirmeyi**

taahhüt ederiz.

Bilgi Gizliliği, Kişisel Verilerin ve Mahremiyetin Korunması

Müşterilerimizin, çalışanlarımızın, tedarikçilerimizin ve web sitesi ziyaretçilerimizin DOCUART ile paylaştığı **kişisel veriler, kişisel olarak tanımlanabilir bilgiler ve diğer gizli bilgilerin gizliliğinin korunması** esastır.

Kişisel veriler ve diğer gizli bilgiler; yalnızca **belirlenmiş ve meşru amaçlar doğrultusunda, gerekli olduğu ölçüde ve uygulanabilir yasal, düzenleyici ve sözleşmesel şartlara uygun olarak** işlenir.

Bu bilgiler; uygulanabilir yasal ve sözleşmesel yükümlülükler, yetkilendirme veya ilgili tarafın açık izni gibi geçerli bir dayanak bulunmadığı sürece yetkisiz gerçek veya tüzel kişilerle paylaşılmaz.

Bilgiye ve kişisel verilere erişim, yalnızca **görev, yetki ve iş gereksinimi** doğrultusunda gerçekleştirilir. Bilgi varlıklarının ve kişisel verilerin yetkisiz erişim, kullanım, değişiklik, kayıp veya ifşaya karşı korunması için gerekli bilgi güvenliği ve gizlilik kontrolleri uygulanır.

Kişisel verilerin toplanması, kullanılması, saklanması, aktarılması ve imha edilmesi süreçlerinde **gizlilik ve veri koruma ilkeleri** gözetilir. Kişisel verilerin yalnızca gerekli süre boyunca muhafaza edilmesi ve saklama süresinin sonunda uygulanabilir şartlara uygun şekilde imha edilmesi veya anonim hale getirilmesi sağlanır.

Kişisel veri sahiplerinin uygulanabilir mevzuat kapsamında sahip olduğu hakların kullanılabilmesi için gerekli süreçler oluşturulur ve bu talepler ilgili prosedürler doğrultusunda değerlendirilir.

Kişisel veri ihlalleri ve gizlilik olaylarının tespit edilmesi, değerlendirilmesi, kayıt altına alınması, müdahale edilmesi ve uygulanabilir durumlarda ilgili taraflara ve yetkili otoritelere bildirilmesi sağlanır.

Elektronik iletişim ve bilgilendirme faaliyetleri, ilgili mevzuat ve alınmış izinler doğrultusunda yürütülür. İlgili kişiler, mevzuatın izin verdiği ölçüde elektronik iletişim tercihlerini değiştirme veya iletişim listesinden çıkarılma taleplerini DOCUART'a iletebilir.

Yönetim Sisteminin Uygulanması

Bu politika; DOCUART'ın faaliyetleri, süreçleri ve ilgili taraflarının ihtiyaçları dikkate alınarak oluşturulmuş olup **ISO 9001, ISO/IEC 27001, ISO/IEC 27701, ISO 22301, ISO 14001 ve ISO 45001** kapsamında oluşturulan Entegre Yönetim Sisteminin uygulanması için bir çerçeve oluşturur.

Politika, kuruluşun stratejik yönü ile uyumlu olarak düzenli aralıklarla gözden geçirilir; kuruluşun faaliyetlerinde, yasal ve diğer şartlarda, ilgili tarafların ihtiyaç ve beklentilerinde, kişisel veri işleme faaliyetlerinde veya yönetim sistemi koşullarında meydana gelen değişiklikler doğrultusunda gerektiğinde güncellenir.

Politikanın kuruluş içerisinde **duyurulması, anlaşılması ve uygulanması**, ilgili taraflara uygun yöntemlerle iletilmesi ve ihtiyaç halinde erişilebilir olması sağlanır.

DOCUART yönetimi, Entegre Yönetim Sisteminin etkin bir şekilde uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için gerekli kaynakları sağlamayı; **bilgi güvenliği, kişisel verilerin korunması ve mahremiyetin sağlanması dahil olmak üzere tüm yönetim sistemi şartlarının yerine getirilmesini** ve bu politikanın tüm çalışanlar tarafından benimsenmesini desteklemeyi taahhüt eder.