1. AMAÇ

Kişisel verilerin gizliliğinin, güvenliğinin sağlanması ve ilgili hukuki düzenlemelere uyum, **İLMOR ve LİOR Kimya Teks. San. ve Tic. Ltd. Şti.'nin** (Şirket) en önemli öncelikleri arasında yer almakta olup, bu konuda azami özen gösterilmektedir.

Bu Politikanın hazırlanmasında; Türkiye Cumhuriyeti Anayasası ve 6698 Sayılı Kişisel Verilerin Korunması Kanunu'nda (KVKK) yer alan düzenlemeler başta olmak üzere kişisel verilerin korunmasına ilişkin ilgili hukuki normlarda ve Kişisel Verileri Koruma Kurulu kararlarında yer alan hükümler dikkate alınmıştır.

Bu Politikanın temel amacı, **Şirket** tarafından hukuka uygun bir şekilde yürütülen kişisel veri işleme faaliyeti ve kişisel verilerin korunmasına yönelik teknik ve idari tedbirler alınmasını sağlamak için bilgi güvenliği ilkelerini belirlemektir.

Buna ilaveten, hazırlanan Politika ve bu Politika kapsamında hazırlanan diğer Politika ve Prosedürler, KVKK ve kişisel veri güvenliğine ilişkin diğer ilgili yasal düzenlemelere uyum ilkelerini sürdürülebilir kılmayı amaç edinmektedir.

2. KAPSAM

Bu politikanın kapsamı, **Şirket** tarafından otomatik olan veya herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla gerçekleştirilen, kişisel verileri işlenen gerçek kişilere yönelik olarak hazırlanmıştır.

3. SORUMLULUK

Bu Politika dokümanının yürütmesinden ve ilgililerine duyurulmasından Şirket yönetimi ve KVKK Komitesi; uygulanmasından tüm Şirket çalışanları sorumludur.

4. POLİTİKA

4.1. Kişisel Veri Güvenliğine Yönelik Teknik Tedbirler

Kişisel Verilerin Korunması Kanunu kapsamında Şirkete ait donanım ve yazılım varlıklarında yer alan kişisel verilerin korunmasına yönelik, Şirket tarafından aşağıda belirtilen teknik tedbirler alınmalıdır.

1) Bilgi varlıkları envanteri oluşturulmalı ve varlık envanterine erişim, sadece yetkili personelin erişebileceği şekilde sınırlandırılmalıdır.

2) Donanım ve yazılım varlıklarında ortaya çıkan değişiklikler ilgili varlık envanterine kaydedilmelidir.

3) Elektronik ve fiziksel varlıklara ve bu ortamlarda bulunan kişisel verilere erişim kullanıcılara ya da rollere göre belirlenmelidir.

4) Hangi kullanıcıların hangi kişisel verilere hangi yetki düzeyinde eriştiğini gösteren Erişim Yetki Matrisi oluşturulmalıdır.

5) Kimlik doğrulama ve yetkilendirme süreçleri tanımlanmalı, merkezi kimlik doğrulama ve yetkilendirme yazılımları kullanılmalıdır.

6) Kullanıcı hesap yönetimi yapılmalıdır.

7) Ayrıcalıklı hesaplar yönetilmelidir.

8) İşten ayrılma ya da görev değişikliği gibi süreçler için kullanıcı yetkilerinin kaldırılması ya da güncellenmesi süreçleri yönetilmelidir.

9) Kurumsal uygulamalar ve yazılımlarda yer alan kişisel veriler kullanıcı yetkilerine göre gerektiğinde maskelenmelidir.

10) Ağ yönetimi ve güvenliği sağlanmalıdır.

11) Sunucu, istemci, misafir, güvenlik kameraları vb. kullanım amaçlarına göre ağ ayrıştırması yapılmalıdır.

12) Uzaktan erişim yapılması gereken durumlar için gerekli güvenlik tedbirleri alınmalı ve erişim kayıtları tutulmalıdır.

13) E-posta sistemlerinin güvenliği sağlanmalıdır.

14) Spam ve oltalama (phishing) amaçlı e-postalar ve zararlı e-posta eklerine yönelik kontroller için Antivirüs ve Antispam sistemleri kullanılmalıdır.

15) Güvenli internet erişimi ve erişim kayıtlarının tutulmasına yönelik güvenlik önlemleri alınmıştır.

16) İz kayıtları (log); fiziksel ortam (kartlı ya da biyometrik geçiş gibi), sunucu, uygulama, internet ve ağ hareketleri için ayrı ayrı tutulmalı ve yönetilmelidir.

17) Karmaşık parola kullanılması ve değişim süreleri tanımlanmalıdır.

18) Kriptografik kontroller ve anahtar yönetimine ilişkin süreçler tanımlanmalıdır.

19) Bilgi güvenliği ve kişisel veri güvenliğine yönelik olarak personele farkındalık eğitimleri verilmelidir.

20) Risk analizi yapılmalı ve risk içeren elektronik ve fiziksel faktörler belirlenerek, risklerin ölçülmesi ve en alt düzeye indirilmesi için faaliyetler yapılmalıdır.

21) Zararlı yazılımlardan korunmaya yönelik Antivirüs yazılımları kullanılmalıdır.

22) Sızma testleri yapılarak olası zafiyet ve tehditlere yönelik çalışma yapılmalı ve kapatılan açıklar hakkında doğrulama testleri yapılmalıdır.

23) Saldırı tespit ve önleme sistemleri kullanılmalıdır.

24) Sistem odası ve veri merkezinin fiziksel güvenliği sağlanmalı ve bu ortamlara yönelik izleme (duman detektörü, sıcaklık takibi, nem ölçümü, kamera kaydı, alarm üretilmesi gibi) yapılmalıdır.

25) Sistem odası ve veri merkezinde otomatik gazlı yangın söndürme sistemi kullanılmalıdır.

26) İşletim sistemleri, kurumsal uygulamalar, üçüncü taraf yazılım ve yamaların güncellikleri periyodik olarak kontrol edilmelidir.

27) Kullanılan bulut hizmetlerinin güvenliği sağlanmalıdır.

28) Mobil cihazların güveliği sağlanmalı, kaybolma ve çalınma durumlarına karşı bu cihazlar uzaktan yönetilebilmelidir.

29) Veri kaybını ve sızıntısını önleme amaçlı tedbirler alınmalıdır.

30) Sanal sistemlerin güvenliği sağlanmalıdır.

31) Kişisel ve hassas veri içeren taşınabilir cihazlar şifrelenmelidir.

32) Özel nitelikli kişisel verilerin korunmasına yönelik harici güvenlik önlemleri (şifreleme, çok faktörlü kimlik doğrulama vb.) alınmalıdır.

33) Otomatik günlük yedeklemeler yapılmalı, belirli aralıklarla yedekten dönme testi yapılarak olası felaket durumlarına karşı iş sürekliliği sağlanmalıdır.

34) Bilgi güvenliği izleme ve denetleme yöntemleri belirlenmelidir.

35) İhlal olayı bildirim süreçleri oluşturulmalıdır.

36) Kişisel veri içeren donanımlar elektronik atık olarak kullanılmadan önce, içeriğinde eyer alan tüm veriler güvenli olarak yok edilmelidir.

37) Kişisel verilerin silinmesi, yok edilmesi ve anonimleştirilmesine yönelik sistem üzerinden otomatik yöntemler tanımlanmalıdır.

4.2. Kişisel Veri Güvenliğine Yönelik Hazırlanan Teknik Dokümanlar

6698 sayılı Kişisel Verilerin Korunması Kanunu ve ikincil düzenlemeler doğrultusunda Şirket tarafından bu Politika dokümanının "**Kişisel Veri Güvenliğine Yönelik Teknik Tedbirler**" başlıklı 4.1 bölümünde sayılan teknik tedbirlerin uygulanmasına rehberlik etmesi amacıyla aşağıda yer alan dokümanlar hazırlanmıştır.

Dokümanlar içerisinde yer alan "**Çalışanlar İçin Bilgi Güvenliği Talimatı**" İnsan Kaynakları tarafından, yeni işe başlayan personelin okuyup imzalamasını sağlanır. Hali hazırda çalışan personelden Talimat'ı okumayan ve imzalamayanlar için İnsan Kaynakları aynı süreci işletir. İşe yeni başlayan personel Bilgi İşlem Müdürlüğüne bildirilir.

4.2.1. Politikalar

1) Kişisel Verilerin Korunmasına Yönelik Bilgi Güvenliği Politikası
2) Çerez Politikası

4.2.2. Prosedürler

1) Erişim Kontrol Prosedürü
2) Kullanıcı Hesap Tanımlama ve Yetkilendirme Prosedürü
3) Ağ ve Sistem Güvenliği Prosedürü
4) Yedekleme Prosedürü
5) Risk Yönetim Prosedürü
6) Kriptografik Kontroller ve Anahtar Yönetim Prosedürü
7) İhlal Olayı Yönetim Prosedürü
8) İzleme, Ölçme ve Denetim Prosedürü
9) Düzeltici Faaliyet ve Sürekli İyileştirme Prosedürü
10) Yönetimin Gözden Geçirmesi Prosedürü
11) Doküman Kayıt Kontrolü Prosedürü

4.2.3. Formlar

1) Erişim Yetki Matrisi
2) Risk Analizi Tablosu
3) İhlal Olayı Bildirim Formu
4) YGG Toplantı Tutanağı
5) Geçerli Doküman Listesi

4.2.4. Talimatlar

1) Çalışanlar İçin Bilgi Güvenliği Talimatı

5. DAĞITIM

Şirket çalışanları ve ilgili taraflar ile paylaşılmaktadır.

GENEL MÜDÜR