SESA SAĞLIKLI BESLENME VE DİYET DANIŞMANLIĞI LİMİTED ŞİRKETİ / DYT. SEDA SAĞBAŞ
BİLGİ GÜVENLİĞİ POLİTİKASI

1. GİRİŞ

1.1. Amaç

Sesa Sağlıklı Beslenme ve Diyet Danışmanlığı Limited Şirketi ile Dyt. Seda Sağbaş (Bundan böyle "**Sesa**" olarak adlandırılacaktır.), gerçekleştirmekte olduğu tüm faaliyetlerde, başta çalışanları, çalışan adayları, danışanları, potansiyel danışanları, ziyaretçileri, hukuki veya ticari ilişki ve/veya iş birliği içinde olduğu diğer kişi, kurum ve kuruluşlar ile bunların çalışanları, iş ortakları, hissedarları ve yetkilileri olmak üzere temas ettiği tüm kişisel veri sahiplerinin temel hak ve hürriyetlerine azami koruma sağlamayı, bu kapsamda tüm faaliyetlerini kişisel verilerin korunması mevzuatına uygun biçimde gerçekleştirmeyi, kişisel veri gizliliği ve güvenliğini her daim ön planda tutmayı amaç edinmiştir. Bu kapsamda, işbu Bilgi Güvenliği Politikasının ("**Politika**") hedefi, 6698 sayılı Kişisel Verilerin Korunması Kanunu ve ilgili mevzuat ("**KVKK**") ışığında Sesa bilgi sistemlerinin ve verilerin gizlilik, bütünlük ve erişilebilirliğinin sağlanmasını teminen alınacak önlemlere ilişkin genel çerçevenin çizilmesi ve gerekli önlemlerin alınmasının sağlanmasıdır.

1.2. Kapsam

Bu Politika, Sesa'nın tüm bilgi sistemleri, kaynakları ve varlıkları ile tüm departmanları ve çalışanlarını kapsayacak şekilde hazırlanmıştır. Tüm Sesa çalışanları Politika ile belirlenmiş olan kurallara uymak, kendilerine düşen sorumlulukları yerine getirmek ve Politikaya azami uyumun sağlanmasını sağlamakla yükümlüdür.

2. BİLGİ GÜVENLİĞİ POLİTİKASI

Bilgi Güvenliği Politikası çerçevesinde Sesa;

- Faaliyetleri kapsamında elde edilen kişisel/kurumsal kullanıcı verilerinin ve personel bilgilerinin korunmasına ve bunların gizliliğini sağlamaya yönelik olarak gerekli teknik ve idari önlemleri almayı,
- Bilgi sistemleri verilerinin bütünlüğünü, gizliliğini ve erişilebilirliğini sağlamaya yönelik gerekli önlemleri almayı ve kontrolleri tesis etmeyi,
- Bilgi sistemlerine ilişkin iş süreçleri ile diğer iş süreçlerinde görevler ayrılığı ilkesine uygun olarak yetkilendirme yapmayı,
- Bilgi sistemlerine ilişkin yetkilendirmelerde minimum yetkilendirme prensibini uygulamayı ve yetkileri düzenli olarak kontrol etmeyi,
- Bilgi sistemlerine dışarıdan gelebilecek her türlü tehdide karşı yeterli/gerekli ağ güvenliğini tesis etmeyi,
- Katmanlı güvenlik mimarisinin tesis edilmesini ve bunun sürekli gözetiminin yapılmasını,
- Gizli verilerin ve kişisel bilgilerin iletilmesinde ve saklanmasında şifreleme, maskeleme vb. güvenlik önlemleri almayı,
- Bilgi güvenliği ihlaline ilişkin olayların tespit edilmesi, raporlanması ve tekerrür etmemesine ilişkin güvenlik ihlali olay yönetimi süreci tesis etmeyi,
- Bilgi güvenliği konusunda çalışanlara ve bütün müşterilere farkındalık programı uygulamayı ve bu programa tüm çalışanların katılımını sağlamayı,
- Çalışma ortamlarında gerekli fiziksel ve çevresel güvenlik önlemlerini almayı,
- Bilgi güvenliği ve gizliliğinin sağlanması konusunda kamu otoritesinden gelebilecek her türlü talimat, tavsiye veya kararı zamanında ve eksiksiz uygulamayı taahhüt etmektedir.

3. TEMEL İLKELER

- Genel kabul görmüş ilgili uluslararası standartlar ve en iyi uygulama örnekleri göz önünde bulundurularak, faaliyetlere ilişkin bilgi sistemlerinin gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlamak amacıyla kural, ilke ve politikaları içeren bilgi güvenliği yönetim çerçevesi oluşturulur.

- Bilgi güvenliği yönetim çerçevesine uygun bir bilgi güvenliği yönetim sistemi oluşturulur.
- Bilgi güvenliği yönetim sisteminin oluşturulmasına, yönetilmesine, belirli aralıklarla gözden geçirilmesine ve gerekli hallerde güncellenmesine ilişkin görev, yetki ve sorumluluklar açıkça belirlenir.
- Bilgi güvenliği yönetim sistemi kapsamında her kademedeki personelin bilgi güvenliğine ilişkin görev, yetki ve sorumlulukları açıkça belirlenir ve ilgili personelin bundan haberdar olması sağlanır.
- Bilgi güvenliği yönetim sistemi kapsamında bilgi güvenliği ihlallerine ilişkin olayların izlenmesi ve raporlanmasına ilişkin gerekli mekanizmalar oluşturulur.
- Bilgi varlıklarının güvenlik gereksinimleri doğrultusunda uygun kontroller tesis etmek için bir bilgi varlıkları sınıflandırma kılavuzu hazırlanır. Her bir sınıftaki bilgi varlıklarına ilişkin erişim hakları ile saklama, iletme ve imha etme prosedürleri açıkça belirlenir, sınıflandırma ve bununla ilgili yükümlülükler konusunda tüm personel bilgilendirilir.
- Sesa, bilgi varlıklarını önem seviyesini ve yasal yükümlülükleri de dikkate alarak bilgi varlıkları sınıflandırma kılavuzuna uygun olarak sınıflandırır.
- Bilgi varlığının sınıfı belirlenirken gizlilik derecesi, bütünlük gereksinimi, kullanılabilirlik gereksinimi, saklama süresi ve asgari yedekleme sıklığı ile veriler özelinde hassas müşteri verisi, kişisel veri ya da sır kapsamındaki veri olup olmadığı gibi kriterler göz önünde bulundurulur.
- Bilgi güvenliği yönetim sisteminde, personelin işe başlaması, görev ve pozisyon değiştirmesi ve işten ayrılması da dahil olmak üzere personele ilişkin tüm hususlar bilgi güvenliğini etkileyen yönleriyle değerlendirilir ve gerekli tedbirler alınır.
- Bilgi güvenliği yönetim sistemi kapsamındaki faaliyetler ile ilgili Sesa nezdindeki her türlü donanım ile altyapının ve bunlarla ilgili fiziksel çevrenin güvenliği sağlanır.
- Faaliyetleri ile ilgili Sesa nezdinde bulunmayan (dış hizmete konu edilen) donanım ile altyapının ve bunlarla ilgili fiziksel çevrenin güvenliğinin sağlanması için gerekli özen gösterilir.
- İç ve dış ağlar arasında sistem ile ilgili gerçekleşen her türlü iletişim sürecinin ve ana faaliyetlere ilişkin operasyonel işlemlerin, güvenlik kontrolleri ve araçları kullanılarak gerçekleşmesi sağlanır.
- Güvenlik kontrolleri ve araçların tesis edilmesinde, bir güvenlik katmanının aşılması halinde diğer güvenlik katmanının devreye girdiği katmanlı güvenlik mimarisi esas alınır ve güncel teknolojiye uygun çözümler kullanılır.
- Bilgi sistemleri ile ilgili yapılacak her türlü değişiklikte bilgi güvenliğinin sağlanması konusunda gereken özenin gösterilmesi zorunludur.
- Bilgi güvenliği yönetim sistemi kapsamında kendilerine görev, yetki ve sorumluluk verilmiş olan personel, bilgi güvenliği yönetim sisteminin bilgi güvenliği konusundaki mevzuata, standartlara ve Sesa politikalarına uyum durumunu sürekli olarak izler, uyumun sağlanması için gerekli tedbirleri alır ve uyum durumunu Müdürler Kurulu'na düzenli olarak raporlar.
- Sesa hizmetlerinden faydalanan kullanıcıların bilgi güvenliği hususlarında farkındalığını arttıracak, ilgili mevzuat hakkında bilgi sahibi olmalarını sağlayacak gerekli faaliyetleri yürütülür ve bu çalışmalar belgelenir.
- Güvenlik açıklarını giderecek gerekli yamalar ve güncellemeler zamanında yapılır.
- Personelin Sesa iç ağındaki uygulama ve sistemlerine Sesa dışından uzaktan erişim gerçekleştirmesine, ilgili kontrol mekanizmalarından geçerek işin ve günün şartlarının gerekleri doğrultusunda onaylanmadığı sürece izin verilmez.
- Uzaktan erişime izin verildiği durumlarda güçlü kimlik doğrulamaya dayanan güvenli bağlantı yöntemleri uygulanır.
- Personelin Sesa iç ağındaki uygulama ve sistemlere uzaktan erişimlerine ilişkin iz kayıtları tutulur, bağlantının süresi ve bağlantının yapılabileceği cihazlar kısıtlanır ve personel belli aralıklarla kimliğini tekrar doğrulamaya zorlanır.
- Gerçekleştirilen faaliyetler ile ilgili olarak görevler ayrılığı ve görevin gerektirdiği kapsam kadar yetki prensipleri ile tutarlı etkin bir kimlik doğrulama ve erişim yönetimi yapısı oluşturulur.
- Bilgi güvenliği yönetim sisteminin etkinliği yılda en az bir defa test edilir.
- Sesa yönetimi, kullanılmakta olan veya ihtiyaç duyabileceği uygulamalar için bir beyaz liste oluşturur ve

bilgi sistemleri unsurlarında sadece ihtiyaç duyulan uygulamaların yüklü olmasını sağlar. Bu unsurlara beyaz liste dışındaki uygulamaların yüklenmesini ve bu uygulamaların çalıştırılmasını engelleyecek önlemleri alır.

- Bilgi sistemleri unsurları üzerinde beyaz listede yer almayan herhangi bir uygulamanın yüklü olup olmadığına yönelik düzenli olarak tarama gerçekleştirilir.
- Bilgi sistemleri unsurları gerekli sıklıkta ve düzenli bir şekilde kontrol edilerek zararlı yazılımlar ve güvenlik açıklarının tespit edilmesini sağlayacak altyapı oluşturulur.
- Sesa'nın e-posta sunucusuna gelen ve giden e-postalar taranarak zararlı yazılım barındıran ya da Sesa'nın iş ihtiyaçları doğrultusunda gereksiz olan eklentiler içeren e-postaları engelleyecek çözümler kullanılır.
- Personelin, zorunlu iş gereksinimi olmadıkça yerel yönetici yetkisine sahip olmasına izin verilmez.
- Yerel yönetici yetkisine yönelik bir ihtiyaç olması durumunda iş birimi ve KVK Görevlisinin onayını müteakip söz konusu yetkinin tanımlı ve kayıtlı prosedürler çerçevesinde ve iş bitiminde tekrar geri alınacak şekilde verilmesi sağlanır.

4. TEMEL BAŞLIKLAR

4.1. Bilgi Güvenliği Organizasyonu

KVK Komitesi Sesa bünyesinde bilgi güvenliği organizasyonu oluşturur ve bilgi güvenliği politikalarının bütünsel bir yaklaşımla oluşturulması, sürdürülmesi ve yönetilmesine ilişkin çalışmalar Bilgi Güvenliği Politikası kapsamında yürütülür.

4.2. Bilgi Güvenliği Rol ve Sorumlulukları

- Bilgi Güvenliğinin planlanması, uygulanması ve kontrol edilmesi faaliyetlerini gerçekleştirmek üzere, KVK Komitesi, KVK Görevlisi ve çalışanlar aktif rol alır.
- Bilgi Güvenliği Politikası KVK Komitesi tarafından yılda en az bir defa gözden geçirilir ve Müdürler Kurulu/Dyt. Seda Sağbaş tarafından onaylanır.
- Bilgi Güvenliği Politikası oluşturulurken Sesa'nın güvenlik stratejisi, güvenlik gereksinimleri, yasal ve düzenleyici zorunluluklar göz önünde bulundurulur.

4.3. Bilgi Varlıklarının Yönetimi

Basılı ve dijital ortamda oluşturulan, iletilen, saklanan veya sözlü olarak paylaşılan tüm veriler bilgi varlıkları kapsamındadır. Verinin iletilmesinde, işlenmesinde, erişilmesinde, saklanmasında, imhasında kullanılan uygulama, yazılım ve donanımlar da bilgi varlıkları kapsamına girer. Bilgi varlıklarının ve bu veriyle ilgili tüm varlıkların gizliliği, bütünlüğü, erişilebilirliği sağlanarak bu varlıkların hasar görmesi, değişmesi, ifşa olması veya kaybolması önlenir. Bilgi varlıkları sınıflandırılır. Bilgilerin bu sınıflandırmaya uygun olarak kullanılması sağlanır. Her varlığa bir sahip atanır ve varlıklarla ilgili sorumluluklar bu sahipler üzerine verilir.

4.4. Risklerin Yönetimi

Sesa'nın bilgi güvenliğine ilişkin risk değerlendirme yaklaşımı Veri Sınıflandırma Kataloğu ile belirlenir. Bilgi varlıklarıyla ilgili oluşabilecek risklerin tanımlanması, derecelendirilmesi, işlenmesi ve gözden geçirilmesi çalışmaları belirlenen risk değerlendirme yaklaşımına uygun olarak gerçekleştirilir.

4.5. Bilgi Güvenliğine İlişkin Farkındalık Yaratılması

KVK Komitesi bütün personeli için farkındalık eğitim gerekliliklerini belirler ve personele buna uygun bir şekilde eğitim sağlar. İşe yeni alınan her çalışana bilgi güvenliği konusunda gerekli eğitim sağlanır. Sesa, çalışanlarından eğitim aldıklarına ve bu kapsamda bilgi güvenliği hususunda üstlerine düşeni yerine getireceklerine ilişkin yazılı taahhütname alınır.

4.6. Fiziksel ve Çevresel Güvenlik

- Faaliyetlerin gerçekleştirildiği binalara, ofislere yetkisiz/izinsiz girişleri engellemek için gerekli fiziksel güvenlik önlemleri alınır.
- Faaliyetlerde kullanılan bilgi teknolojileri ekipmanına yönelik gerekli güvenlik kontrolleri uygulanarak, bilgi varlıklarının kaybı, hasarı, çalınması, tehlikeye girmesi durumunda faaliyetlerin kesintiye uğraması engellenir.
-

4.7. Haberleşme ve İletişim Yönetimi

- Bünyemizde operasyonel süreçlere yönelik sorumluluklar tanımlanırken bir işi yapan rol ile yapılan işi denetleyen rol aynı kişiye verilmez.
- Yazılım ve bilginin bütünlüğünü korumak amacıyla kötü niyetli kodlara ve uygulamalara karşı güvenlik kontrolleri gerçekleştirilir.
- Bilginin ve bilgi varlıklarının bütünlüğünü ve kullanılabilirliğini sağlamak için yedekleme faaliyetleri gerçekleştirilir.
- Ağdaki bilginin ve destekleyici altyapının korunması sağlanır.
- İnternet sitesi hizmetlerinin güvenlik gereklilikleri sağlanır.
- Yetkisiz bilgi işleme faaliyetlerini algılamak amacıyla bilgi sistemleri uygulamalarına yönelik denetim izleri oluşturulur.
- Gerekli aralıklarla sızma testleri yapılır.
-

4.8. Erişim Kontrolü

- Bilgi sistemlerine ve varlıklarına erişimi kontrol etmek için kullanıcı erişimleri güvenlik gereksinimlerini temel alacak şekilde yönetilir ve yetkisiz erişimler önlenir.
- Erişim yetkileri görevler ayrılığı ilkesine ve gerekli olan minimum yetkilendirme prensibine uygun olarak sağlanır. Yetkiler düzenli olarak gözden geçirilir.
- Ağ erişimlerine yönelik güvenlik kontrolleri ile ağ bağlantılı hizmetlere yetkisiz erişimler engellenir.
- İşletim sistemlerine ve uygulamalara yönelik erişim kontrolleri hayata geçirilir. Mobil bilgi işleme ve uzaktan çalışma hizmetlerini kullananlar için bilgi güvenliği gereksinimleri karşılanır.

4.9. Ağ Güvenliği

- Ağ trafiğinde güvenliği sağlamak amacıyla, ağ kontrol güvenlik sistemleri bulunur.
- Ağ güvenliğinde dış güvenlik duvarı, IPS, iç güvenlik duvarı, SSM gibi katmanlı güvenlik mimarisi (bir güvenlik katmanının aşılması durumunda diğer güvenlik katmanının devreye girdiği) kullanılır.
- Ağ güvenliğinde kullanılan sistemler, sürekli gözetim altında tutulur. Dış ağ ile kurulan bağlantılarda VPN ve SSL kullanılır.

4.10. Bilgi Sistemlerinin Geliştirilmesi ve Bakımı

- Bilgi sistemlerine yönelik geliştirme ve bakım operasyonlarında güvenlik gereksinimleri uygulanır.
- Sistem dosyalarının ve sistem verilerinin güvenliğini sağlamak amacıyla güvenlik kontrolleri uygulanır.
- Uygulamalar ve sistemler üzerinde yapılacak değişiklikler kontrollü olarak gerçekleştirilir ve güvenlik riskleri azaltılır.
- Dışarıdan sağlanan yazılım geliştirmelerinin bilgi güvenliği gereksinimlerini sağlaması temin edilir.

4.11. Bilgi Güvenliği Olay Yönetimi

- Bilgi sistemleri ile ilişkili bilgi güvenliği olayları derhal gecikmeksizin raporlanır.
- Raporlama güvenlik olayına ilişkin düzeltici önlemlerin zamanında alınabilmesini sağlayacak şekilde gerçekleştirilir.
- Tüm çalışanların, tedarikçilerin ve üçüncü taraf kullanıcıların bilgi güvenliği olaylarının raporlanmasına katılımı sağlanır.
- Olayların sonucunda iyileştirici faaliyetler hayata geçirilir tekrar eden olayların önüne geçilir.

4.12. Bilgi Sistemleri Sürekliliği

İş faaliyetlerindeki kesilmeleri önlemek, önemli iş süreçlerini bilgi sistemleri aksaklıklarından korumak için bilgi sürekliliği faaliyetleri gerçekleştirilir.

5. POLİTİKAYA UYUM

Bu politikayı ihlal edenler, işten çıkarılmaya kadar varabilen uygun disiplin işlemlerine, bunun yanı sıra hem hukuki hem de cezai yaptırımlara tabi tutulabilir.

6. POLİTİKANIN YÜRÜRLÜĞÜ, YAYIMLANMASI VE MUHAFAZASI

6.1. Yürürlük

İşbu Politika 01.01.2023 tarihinde yürürlüğe girmiştir. Yürürlükte bulunan mevzuat ve Politika arasında uyumsuzluk bulunması halinde yürürlükteki mevzuat uygulanır. Herhangi bir nedenle söz konusu uyumsuzluğa ilişkin olarak Politikanın güncellenmesinin gecikmesi, özellikle hukuki ve teknolojik gelişmelere istinaden gerekli önlemlerin alınmasına engel değildir.

6.2. Yayım

İşbu Politika, Sesa iç ağında ve internet sitesinde herkesin erişimine açık bir biçimde bulundurulur.

6.3. Muhafaza

İşbu Politika ıslak imzalı basılı kâğıt ve elektronik kayıt olmak üzere iki ortamda muhafaza edilir. Islak imzalı basılı kâğıt nüshası KVK Komitesi dosyasında; elektronik kaydı ise Sesa iç ağında saklanır.

7. HUKUKİ DAYANAKLAR

Politikanın başlıca hukuki dayanakları aşağıdaki gibidir:

- 6698 sayılı Kişisel Verilerin Korunması Kanunu
- Veri Sorumluları Sicili Hakkında Yönetmelik
- Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik

Sesa Sağlıklı Beslenme ve Diyet Danışmanlığı Limited Şirketi / Dyt. Seda Sağbaş