SANİFOAM ENDÜSTRİ VE TÜKETİM ÜRÜNLERİ SANAYİ TİCARET ANONİM ŞİRKETİ

KURUMSAL BİLGİ GÜVENLİĞİ POLİTİKASI VE BİLGİ SİSTEMLERİ YÖNETİM ÇERÇEVESİ

Sanifoam Endüstri ve Tüketim Ürünleri Sanayi Ticaret Anonim Şirketi (Şirket), faaliyetlerini sürdürürken işlediği bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini kurumsal bir değer olarak kabul eder. Bu çerçevede hazırlanan Bilgi Güvenliği Politikası, Sermaye Piyasası Kurulu'nun (SPK) VII-128.9 sayılı Bilgi Sistemleri Yönetimi Tebliği ve 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) ile tam uyum içerisinde, ancak Şirketin yasal sorumluluklarını makul ve yönetilebilir bir düzeyde tutacak şekilde yapılandırılmıştır. KVKK Politikası şirketin web sitesinde ayrıca yer almaktadır. İşbu politika, Şirketin sahip olduğu tüm bilgi varlıklarını hedef alan tehditlerin yönetilmesini, risklerin minimize edilmesini ve operasyonel sürekliliğin teknolojik imkânlar dâhilinde en üst seviyede tutulmasını hedefler.

Bilgi Güvenliği Yönetişimi ve Organizasyonel Yapı

Şirketin bilgi güvenliği stratejisi, üst yönetimin tam desteği ve organizasyonel birimlerin eşgüdümlü çalışması üzerine inşa edilmiştir. Bilgi güvenliğinin sadece teknik bir departmanın sorumluluğu olmadığı, tüm kademelerde bir kurumsal kültür olarak benimsendiği bu yapı, SPK düzenlemelerinin öngördüğü yönetişim standartlarını karşılamaktadır.

Yönetim Kurulunun Sorumlulukları ve Gözetimi

Sanifoam Yönetim Kurulu, bilgi güvenliği politikalarının oluşturulması, onaylanması ve periyodik olarak gözden geçirilmesinden birinci derecede sorumludur. Yönetim Kurulu, bilgi sistemlerine yönelik risklerin yönetimi için gerekli olan bütçe, insan kaynağı ve teknolojik altyapıyı tahsis ederken, bu süreçlerin fiili olarak işlediğini gözetim mekanizmalarıyla takip etmeyi taahhüt eder. Kurumsal yönetişim ilkeleri uyarınca Yönetim Kurulu, bilgi sistemleri güvenliğini Şirketin genel risk yönetimi stratejisinin ayrılmaz bir parçası olarak değerlendirmektedir.

Görev Unvanı	Bilgi Güvenliği Kapsamındaki Sorumluluğu	İlgili Yetki Alanı
Yönetim Kurulu	Politikanın onayı, kaynak tahsisi ve stratejik gözetim.	En Üst Karar Mercii
Genel Müdür	Operasyonel uyum ve üst yönetime raporlama.	İcra Kurulu
Bilgi Sistemleri Güvenliği Sorumlusu	Teknik kontrollerin tesisi, risk analizi ve ihlal yönetimi.	Bağımsız Denetim ve Gözetim
KVKK Komitesi	Kişisel verilerin korunması ve yasal uyum süreçleri.	Veri Mahremiyeti

Bilgi Sistemleri Güvenliği Sorumlusunun (BSGS) Rolü

SPK tebliğ hükümleri gereğince, Şirket bünyesinde bilgi sistemleri yönetim faaliyetlerinden bağımsız, teknik yetkinliğe sahip bir Bilgi Sistemleri Güvenliği Sorumlusu 30.06.2026 tarihine kadar belirlenecektir. Bu sorumlu, bilgi güvenliği kontrollerinin işletilmesini takip etmekle, zafiyet taramalarını koordine etmekle ve yılda en az bir kez üst yönetime kapsamlı risk raporu sunmakla mükellef olacaktır. BSGS, bilgi sistemleri operasyonlarını yürüten ekiplerle çıkar çatışması oluşturmayacak şekilde konumlandırılmış olup, doğrudan üst yönetime raporlama yapacaktır.

KVKK Komitesi ve Veri Sorumlusu Temsilciliği

Sanifoam bünyesinde oluşturulan KVKK Komitesi, Komite başkanlığında faaliyetlerini sürdürmekte olup, bilgi güvenliği politikasının kişisel verilerin korunması ayağını yönetmektedir. Komite, verilerin işlenmesi, saklanması ve imha edilmesi süreçlerini kanuni ilkelere uygun hale getirirken, bilgi güvenliği ihlalleri durumunda İlgili Kişilerin ve Kurulun bilgilendirilmesi süreçlerini koordine eder.

Bilgi Varlıklarının Yönetimi ve Sınıflandırma

Şirketin sahip olduğu bilgilerin değeri, stratejik önemi ve yasal hassasiyeti her varlık için farklıdır. Bu nedenle, tüm bilgi varlıkları tanımlanmalı, envantere kaydedilmeli ve uygun bir sınıflandırma sistemine tabi tutulmalıdır.

Varlık Sahipliği ve Envanter

Her bilgi varlığı (donanım, yazılım, veri tabanı, fiziksel belge vb.) için bir "Varlık Sahibi" belirlenir. Varlık sahibi, ilgili varlığın sınıflandırılmasından ve erişim yetkilerinin düzenli olarak gözden geçirilmesinden sorumludur. Şirket, sahip olduğu bilgi varlıklarını içeren güncel bir envanteri muhafaza eder ve bu envanter üzerinden yıllık risk analizlerini gerçekleştirir.

Bilgi Sınıflandırma Metodolojisi

Bilgi, gizlilik derecesine göre dört ana grupta sınıflandırılır. Bu sınıflandırma, "bilmesi gereken" prensibi doğrultusunda erişim kontrollerinin temelini oluşturur.

Sınıflandırma Etiketi	Tanım ve Örnekler	Koruma Gereksinimi
Çok Gizli	İfşası halinde Şirkete geri dönülemez zarar verecek stratejik veriler, özel nitelikli kişisel veriler.	En yüksek düzeyde şifreleme, çok faktörlü doğrulama, fiziksel kilit.
Gizli	Rekabet avantajını etkileyebilecek ticari sırlar, müşteri listeleri, finansal tablolar.	Erişim kayıtlarının sıkı takibi, sadece yetkili personel erişimi.
Hizmete Özel	Sadece belirli birimler tarafından bilinmesi gereken operasyonel veriler, personel özlük bilgileri.	Şirket içi ağ sınırlaması, kullanıcı bazlı yetkilendirme.
Kamuya Açık	Faaliyet raporları, web sitesi içerikleri, basın bültenleri.	Standart sistem bütünlüğü kontrolleri.

Risk Yönetimi ve Güvenlik Kontrolleri

Risk yönetimi, Sanifoam'un bilgi güvenliği yaklaşımının temel taşıdır. Şirket, riskleri tamamen ortadan kaldırmanın mümkün olmadığını kabul ederek, "risk temelli yaklaşım" ile olası tehditlerin etkilerini kabul edilebilir seviyelere indirmeyi hedefler.

Risk Analiz Süreci

Yılda en az bir kez veya Şirket altyapısında önemli bir değişiklik meydana geldiğinde risk analizi tekrarlanır. Risk analizi kapsamında; bilgi varlıklarına yönelik tehditler, sistemlerin zafiyetleri ve bu risklerin gerçekleşme

ihtimali ile etkisi değerlendirilir. Analiz sonuçları doğrultusunda; riskin azaltılması, transfer edilmesi, kaçınılması veya makul seviyedeki risklerin kabul edilmesi stratejileri uygulanır.

Sızma Testleri ve Zafiyet Taramaları

SPK VII-128.9 Tebliği uyarınca, Şirket bilgi sistemleri üzerinde yılda en az bir kez bağımsız uzmanlar tarafından sızma testleri gerçekleştirilir. Bu testler, hem internet üzerinden gelen dış tehditleri hem de iç ağdan kaynaklanabilecek zafiyetleri kapsar. Test sonuçları BSGS tarafından raporlanarak üst yönetime sunulur ve tespit edilen açıklıkların giderilmesi için bir iyileştirme planı oluşturulur.

Erişim Kontrolü ve Kimlik Yönetimi

Bilgiye erişim, "en az yetki" (least privilege) ve "görevler ayrılığı" (segregation of duties) ilkelerine dayanır. Bu ilkeler, yetkisiz erişimlerin önlenmesi ve olası hataların veya kötü niyetli girişimlerin tespiti açısından kritiktir.

Kullanıcı Hesapları ve Yetkilendirme

Kullanıcı hesapları, personelin görev tanımına uygun olarak oluşturulur. Her kullanıcıya benzersiz bir kimlik atanır ve hesapların ortak kullanımı yasaktır. Personelin işe başlaması, görev değişikliği veya işten ayrılması durumunda erişim yetkileri derhal güncellenir veya iptal edilir. Yetki matrisleri yılda en az bir kez ilgili birim yöneticileri tarafından gözden geçirilerek gereksiz yetkilerin temizlenmesi sağlanır.

Parola Güvenliği ve Çok Faktörlü Doğrulama

Sistemlere erişimde kullanılan parolaların güvenliği için aşağıdaki standartlar uygulanır:

- Parolalar en az 8 karakter uzunluğunda olmalı ve büyük/küçük harf, rakam ve özel karakter içermelidir.
- Parolalar 90 günde bir değiştirilmeli ve eski parolalar tekrar kullanılmamalıdır.
- Kritik sistemlere ve uzaktan erişim noktalarına (VPN vb.) girişte çok faktörlü kimlik doğrulama (MFA) kullanımı zorunludur.

Operasyonel Güvenlik ve Ağ Yönetimi

Bilgi sistemlerinin güvenli bir şekilde işletilmesi, ağ altyapısının korunması ve kötü amaçlı yazılımlara karşı önlem alınması operasyonel güvenliğin temelini oluşturur.

Ağ Güvenliği ve Segmentasyonu

Şirket ağı, farklı güvenlik seviyelerine sahip bölümlere (VLAN) ayrılarak izole edilmiştir. Özellikle üretim hatlarını kontrol eden sistemler ile kurumsal ağ arasında sıkı bir denetim mekanizması bulunur. İnternet trafiği, güncel güvenlik duvarları (Firewall) ve saldırı engelleme sistemleri (IPS/IDS) üzerinden filtrelenerek zararlı içeriklerin girişi engellenir.

Kötü Amaçlı Yazılımlardan Korunma

Tüm sunucu ve kullanıcı bilgisayarlarında merkezi olarak yönetilen güncel antivirüs ve uç nokta güvenliği (EDR) yazılımları kullanılır. Kullanıcıların sistemlere onaylanmamış yazılımlar yüklemesi ve USB gibi harici depolama birimlerinin izinsiz kullanımı engellenir.

Fiziksel ve Çevresel Güvenlik

Bilgi işlem sistemlerinin ve hassas verilerin bulunduğu fiziksel alanlar, yetkisiz erişimlere ve çevresel tehditlere karşı koruma altına alınmıştır.

Güvenli Alanlar ve Giriş Kontrolü

Sistem odaları ve arşiv alanları gibi kritik bölgelere girişler, yetkilendirilmiş personel ile sınırlandırılmıştır. Bu alanlara giriş-çıkışlar kartlı sistemler veya biyometrik yöntemlerle takip edilir ve kayıt altına alınır. Ziyaretçilerin bu alanlara girişi sadece refakatçi eşliğinde ve kayıt altında mümkündür.

Çevresel Tehditlere Karşı Korunma

Bilgi işlem altyapısının sürekliliği için yangın algılama ve söndürme sistemleri, iklimlendirme üniteleri ve kesintisiz güç kaynakları (UPS/Jeneratör) tesis edilmiştir. Bu sistemlerin periyodik bakımları yapılarak her an çalışır durumda olmaları sağlanır.

Bilgi Güvenliği İhlal Olayı Yönetimi

Güvenlik ihlallerinin hızlı bir şekilde tespit edilmesi, raporlanması ve müdahale edilmesi, olası zararların minimize edilmesi açısından hayati öneme sahiptir.

İhlal Raporlama ve Müdahale

Herhangi bir güvenlik ihlali veya zayıflığı tespit eden çalışanlar, durumu derhal BSGS'ye veya KVKK Komitesi'ne bildirmekle yükümlüdür. İhlal olaylarına müdahale için önceden tanımlanmış bir "Olay Müdahale Planı" izlenir. Bu plan; olayın analizi, etkisiz hale getirilmesi, verilerin kurtarılması ve kök neden analizini kapsar.

Denetim İzleri (Logging)

Sistemler üzerinde gerçekleştirilen tüm kritik işlemlerin denetim izleri (log kayıtları) otomatik olarak tutulur. Bu kayıtlar; kullanıcı kimliği, işlem zamanı, erişilen kaynak ve işlem sonucunu içerir. Denetim izleri, bütünlüğü korunacak şekilde güvenli bir ortamda saklanır ve geriye dönük incelemeler için asgari 5 yıl boyunca muhafaza edilir.

İş Sürekliliği ve Felaket Kurtarma

Olağanüstü durumlarda Şirketin kritik iş süreçlerinin aksamaması ve verilerin kaybolmaması için gerekli stratejiler belirlenmiştir.

Yedekleme Politikası

Veriler, kritiklik seviyelerine göre belirlenen periyotlarla (günlük, haftalık vb.) yedeklenir. Yedeklerin bir kopyası, asıl verinin bulunduğu lokasyondan farklı bir fiziksel veya bulut ortamında, şifreli bir şekilde saklanır. Yedeklerden geri dönme testleri yılda en az bir kez yapılarak yedekleme sisteminin güvenilirliği doğrulanır.

İş Süreklilik Planları

Kritik iş fonksiyonlarını destekleyen bilgi sistemleri için "İş Sürekliliği ve Felaket Kurtarma Planları" hazırlanmıştır. Bu planlar, bir felaket anında hangi sistemlerin öncelikle devreye alınacağını ve kurtarma hedeflerini (RTO/RPO) belirler. Planların etkinliği periyodik tatbikatlarla ölçülür ve gerekli iyileştirmeler yapılır.

Eğitim ve Farkındalık

Bilgi güvenliğinin en önemli bileşeni insan farkındalığıdır. Şirket, çalışanlarının güvenlik bilincini artırmak için sürekli eğitim faaliyetleri yürütür.

Eğitim Türü	Hedef Kitle	Kapsam	Periyot
Temel Bilgi Güvenliği	Tüm Personel	Şifre kullanımı, sosyal mühendislik, temiz masa.	Yılda 1 kez
KVKK Farkındalık	Tüm Personel	Kişisel verilerin işlenmesi ve haklar.	Yılda 1 kez
Teknik Güvenlik	BT Personeli	Sistem sıkılaştırma, güvenli yazılım geliştirme.	Sürekli

Yönetim Bilgilendirme	Üst Yönetim	Risk durumu ve siber tehdit trendleri.	Yılda 2 kez

Yasal Uyumluluk ve Sorumluluğun Sınırlandırılması

Sanifoam, bilgi güvenliğini sağlarken ilgili tüm yasal mevzuata uyumu taahhüt eder. Ancak, dijital dünyadaki risklerin tamamen ortadan kaldırılamayacağı gerçeğiyle, yasal sorumluluklarını makul bir zeminde tanımlar. İş bu politika şirketin daha öncede yayınlanmış “Kişisel Verilerin Korunması ve İşlenmesi Politikası” ile birlikte değerlendirilir ve işlenir.

En İyi Çaba ve Makul Güvenlik

Şirket, bilgi varlıklarını korumak için teknolojik imkânlar ve maliyet-fayda dengesi gözetilerek "en iyi çabayı" gösterir. Alınan önlemler, güncel tehdit ortamına ve endüstri standartlarına uygun olarak tesis edilmiştir. Şirket, kendi kusuru olmaksızın gerçekleşen üçüncü taraf siber saldırıları, donanım arızaları veya mücbir sebeplerden kaynaklanan veri kayıpları ve kesintiler nedeniyle oluşabilecek dolaylı zararlardan, mevzuatın izin verdiği ölçüde sorumlu tutulamaz.

Kullanıcı Sorumlulukları ve Disiplin Süreci

Her çalışan, kendisine tahsis edilen erişim bilgilerinin ve cihazların güvenliğinden bizzat sorumludur. Şirket politikalarına, prosedürlerine ve güvenlik kurallarına aykırı hareket eden, kasıtlı veya ağır ihmali bulunan personel hakkında Şirket içi disiplin yönetmeliği ve yasal mevzuat çerçevesinde gerekli işlemler başlatılır.

Politikanın Gözden Geçirilmesi ve Yürürlük

İşbu Bilgi Güvenliği Politikası, Sanifoam Yönetim Kurulu’nun onayı ile yürürlüğe girmiştir. Politika, Şirketin iş ihtiyaçlarındaki değişiklikler, yeni siber tehditler veya yasal düzenlemeler doğrultusunda yılda en az bir kez gözden geçirilir ve gerekli görülmesi halinde güncellenir. Politika metni ve ilgili alt prosedürler tüm çalışanların erişimine açık olan kurumsal platformlarda yayınlanır.

Bu politika belgesi, Sanifoam Endüstri ve Tüketim Ürünleri Sanayi Ticaret Anonim Şirketi’nin kurumsal itibarını korurken, bilgi sistemlerini modern bir güvenlik çerçevesine oturtmayı ve paydaşlarına güven vermeyi amaçlayan bir üst doküman niteliğindedir. Uygulama detayları, bu politikaya bağlı olarak hazırlanan teknik prosedürler ve çalışma talimatları ile belirlenir.

İşbu Bilgi Güvenliği Politikası, 26/12/2025 tarih ve 2025/406 sayılı Yönetim Kurulu kararı ile yürürlüğe girmiş olup, ayrıca Şirket kurumsal internet sitesi üzerinden kamuya açıklanır. Bu Politikada yapılacak değişiklikler de aynı usule tabidir.