İÇERİK

1. AMAÇ

Bilgi, diğer önemli ticari varlıklar gibi, bir işletme için değeri olan ve bu nedenle korunması gereken bir varlıktır. Bilgi güvenliği, bilgiyi ticari sürekliliği sağlamak, ticari kayıpları en aza indirmek ve ticari fırsatların ve yatırımların dönüşünü en üst seviyeye çıkarmak için geniş tehlike ve tehdit alanlarından korur.

Bilgi birçok biçimde bulunabilir. Kağıt üzerine yazılmış ve basılmış olabilir, elektronik olarak saklanmış olabilir, posta yoluyla veya elektronik imkanlar kullanılarak gönderilebilir ya da karşılıklı konuşma sırasında sözlü olarak ifade edilmiş olabilir. Bilgi hangi biçimi alırsa alsın, her zaman uygun şekilde korunmalıdır. Bilgi güvenliği aşağıdakilerin korunması olarak tanımlanır;

- Gizlilik

Bilginin sadece erişim yetkisi verilmiş kişilerce erişilebilir olduğunun garanti edilmesidir.

- Bütünlük

Bilginin orjinal halinin korunması, veri kaybının engellenmesidir. Bilginin ve işleme yöntemlerinin doğruluğunun ve bütünlüğünün temin edilmesidir.

- Erişebilirlik

Yetkilendirilmiş kullanıcıların gerek duyulduğunda bilgiye ve ilişkili kaynaklara erişime sahip olabileceklerinin garanti edilmesidir.

Yönetim Amacı;

Yönetim, Knauf Insulation iş süreçlerin bilhassa ihracat ve ithalat süreçlerinde kullanılan bilginin bütünlüğünün, erişilebilirliğinin ve gizliliğinin, kuruluşun devamlılığı açısından son derece önemli olduğunu görmüş ve bu amaçla bir bilgi güvenliği yönetim sistemi kurulmasına karar verilmiştir ve bunun için ve ISO 27001 Bilgi Güvenliği Standardı ve müşterilerimizle yaptığımız sözleşmeler ve yasal gereklilikler referans olarak alınmaktadır. Bilhassa gümrük süreçlerinde imtiyaz sağlamakta olan Yetkilendirilmiş Yükümlülük Statüsünün gereği olarak da ISO 27001 standardına uyum ihtiyacı oluşmuştur.

2. KAPSAM

Bilgi Güvenliği Yönetim Sistemi Kapsamı, Bilgi Güvenliği Yönetim Sistemi Kapsam dökümanında (BGY01) tanımlanmıştır.

3. SORUMLULUKLAR

Bilgi güvenliği, yönetim takımının tüm bireylerince paylaşılan bir iş sorumluluğudur. Bilgi Güvenliği Politikasına uyum konusunda ise her bir Knauf Insulation ferdi bireysel anlamda sorumludur.

Bilgi Güvenliği görev ve soumlulukları BGYS Roller Görevler ve Nitelikler Dokumanında tanımlanmıştır.

Herhangi bir çalışanın bilinçli olarak güvenlik kurallarını ihlal veya ihmal etmesi resmi bir disiplin sürecinin uygulanmasını gerektirir.

4. UYGULAMA

Knauf Insulation, kendisine ve paydaşlarına ait bütün bilgilerini ve bilgi varlıklarını gizlilik, bütünlük ve erişilebilirliğine yönelik iç veya dış, kasıtlı veya kasıtsız bütün tehditlere karşı koruması için gerekli bilgi güvenliği önlemlerinin alınmasını amaçlamaktadır.

Knauf Insulation'da uygulanmakta olan BGYS'nin amaçları aşağıdaki gibidir:

- Knauf Insulation'ın tabi olduğu her türlü ulusal ve uluslararası yasa, mevzuat ve düzenlemeler ile sözleşmelerden doğan yükümlülüklerinin yerine getirilmesi,
- Finans, Personel ya da Kurumsal Kaynak Planlaması sistemindeki bilgilerin gizliliği, bütünlüğü ve erişilebilirliğinin sağlanması,
- Gümrük Bakanlığı Yetkilendirilmiş Yükümlülük Statüsü mevzuatına uygunluğun sağlanması,
- Kamu kurumlarına yapılması zorunlu olan bildirimler için gerekli olan elektronik ve basılı belgelerin korunması,
- Knauf Insulation operasyonlarının ve süreçlerinin iş sürekliliğinin sağlanması,
- Knauf Insulation, Tedarikçileri, İş Ortakları ve Paydaşlarının Ticari Sırlarının ve İtibarının, kişisel bilgilerinin korunması
- Çalışanlarımızın varlığı, çalışanlarımızın şirkete bağlılığı, kişisel bilgilerinin korunması,
- Yetkilerin ve bilgilerin iş amacıyla ve yetkilendirilen hizmetler için kullanılması,
- Bilgi güvenliği bilincinin kurum kültürünün bir parçası haline getirilmesi.

Knauf Insulation Bilgi Güvenliği Politikası, **Knauf Insulation** veri/bilgi/yazılım/donanım varlıklarının oluşturulması, transferi, kullanımı, yedeklenmesi, saklanması, kontrolü ve imha edilmesi sırasında gizliliğinin, bütünlüğünün, ve erişilebilirliğinin sağlanmasıdır. Bunun için, başta yasal şartlar olmak üzere bilgi güvenliği ile ilgili gerekliliklerin sağlanması, risklerin belirlenmesi, değerlendirilmesi, güvenlik tedbirlerinin alınması, alınan tedbirlerin etkinliğinin değerlendirilmesi ve gözden geçirilmesi ve Bilgi Güvenliği Sisteminin etkinliğinin gelişen ihtiyaçlar ve teknoloji doğrultusunda sürekli iyileştirilmesi esastır.

Knauf Insulation Bilgi Güvenliği Stratejisi aşağıdaki esaslar üzerine kuruludur;

1. Knauf Insulation üzerinden sağlanan her türlü hizmet, işlem ve veri ile bunların sunumunda kullanılan sistemlerin güvenliğinin sağlanması,
2. Müşteri, çalışan ve tedarikçiler tarafından ulaşılan ve kullanılan kritik bilgi ve bilişim sistemlerinin güvenliğinin sağlanması,
3. Siber güvenlik olaylarının etkilerinin en düşük düzeyde kalmasına, olayların ardından sistemlerin en kısa sürede normal çalışmalarına dönmesine yönelik stratejik siber güvenlik eylemlerinin belirlenmesine ve oluşan suçun adli makam ve kollukça daha etkin araştırılmasının ve soruşturulmasının sağlanması

Risk Yönetimi

Risk analizi, potansiyel tehdit ve tehlikelerin bilgi varlıkları üzerinde oluşturabileceği etkileri değerlendirir. Risk yönetimi bu potansiyel tehdit ve tehlikelerin etkilerini kaldırmak, azaltmak, başka taraflara sıçramasını önlemek için gerekli güvenlik tedbirlerini önermek, kurmak ve izlemektir.

Risk Yönetimi Fonksiyonları;

1. Risk altındaki bilgi varlıklarının tanımlanması:

Bilgi varlıkları, bilgi, veri, yazılım, donanım, dokümantasyon, raporlar, resmi dokümanlar, evraklar, bilginin kullanıldığı, saklandığı, işlendiği, transfer edildiği, bulunduğu sistemler, süreçler ve bu system ve süreçlerin devamlılığı için gereken altyapı, personel ve tadarikçilerdir.

2. Bu varlıklara yönelik risklerin belirlenmesi,
3. Risklerin gerçekleşmesi durumunda kurum üzerinde yaratacağı etkinin büyüklüğü ve gerçekleşme ihtimalinin yüksekliği ışığında risklerin derecelendirilmesi
4. Tabi olunan sözleşme, düzenleme, yasal ve düzenleyici gereksinimler ile iş gereksinimleri ışığında kabul edilebilir risk seviyesinin belirlenmesi
5. Kabul edilebilir risk seviyesinin üzerindeki riskler için Risk İşleme Planlarının başlatılması

Risk Analizi yılda bir kez tekrar edilecek ve mevcut riskler gözden geçirilecektir. Güvenlik risklerinin gözden geçirilmesi aşağıdakiler için önemlidir:

a) iş gerekleri ve önceliklerindeki değişiklikleri dikkate almak.
b) yeni tehditler ve güvenlik boşlukları üzerine düşünmek.
c) denetimlerin etkili ve uygun sürdüğünü teyid etmek.

Bilgi Güvenliği Hedefleri

Risk analizinin her yıl tekrar edilmesinin ardından, üst yönetim tarafından, bilgi güvenliği gereksinimlerine ve risk analizi sonuçlarına göre bilgi güvenliği hedefleri belirlenir, ilgili süreç sahipleri ile bilgi güvenliği hedefleri konusunda mutabık kalınır. Üzerinde uzlaşılan hedefler ilgili taraflara duyurulur. Hedefler SMART kriterlerine uygun olarak takip edilmektedir. Her bir bilgi güvenliği hedefine ulaşılması için alınması gereken aksiyonlar, son tamamlanma tarihi, sonuçların nasıl değerlendirileceği ve aksiyon sahipleri Yillik Süreç Performans Ölçüm Planı' nda belirtilmektedir. Hedeflerin karşılanma durumu yılda bir gözden geçirilir,

Güncelleme

BGYS politikası, Bilgi Güvenliği Koordinatörü tarafından yılda bir gözden geçirilir gerekirse güncellenir. Bunun dışında, yeni bir mevzuat, yasal ya da sözleşme gerekliliği, yeni pazar, yeni iş ortakları veya yeni müşteriler gibi çalışma ortamının, şartların ya da süreçlerin değişmesi durumunda da BGYS politikası gözden geçirilir ve gerekiyorsa güncellenir.