1. BİLGİ GÜVENLİĞİ TANIMI

Bilgi güvenliği, bilginin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda, istenmeyen kişiler tarafından elde edilmesini önlenmesi anlamına gelmektedir.

Gelişen teknoloji ile beraber bilginin korunması gereken tehditlerin çokluğu ve bunlara karşı güvenlik çözümleri oluşturma gerekliliği firmaları yeni arayışlara itmiş ve bilgi güvenliği sürecinin işletilmesi için kendi bünyesinde ya da dış kaynaklı yetkin personel yardımı ile bilgi güvenliği yazılı ve sözlü olarak şirket personeline iletilmesi ve bilinçlendirilmesi sürecini başlatmıştır.

Bu süreç sonucunda dünya genelinde diğer güvenlik sistemlerinde olduğu bilgi güvenliğinin de bir standarda oturtulması istenmiş ve bugünkü adı ile ISO 27001 ortaya çıkmıştır.

Bilgi güvenliği politikamızda bu standarda uygun olarak aşağıdakilerin korunması amaçlanmıştır.

Gizlilik: Bilginin sadece erişim yetkisi verilmiş kişilere erişilebilir olduğunu garanti etmek;

Bütünlük: Bilginin ve işleme yöntemlerinin doğruluğunu ve yetkisiz değiştirilememesini temin etmek;

Erişilebilirlik: Yetkili kullanıcıların, gerek duyulduğunda bilgiye ve ilişkili kaynaklara en hızlı şekilde erişebileceklerini garanti etmek.

2. BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ OLUŞTURULMA AMACI

Kuruluş, kurumun güvenilirliğini ve kurumsal imajını korumak, kurumun bilgi varlıklarına ilişkin risk değerlendirme ve risk işleme faaliyetleriyle bilgi güvenliğine ilişkin var olan ya da oluşabilecek olan riskleri azaltmak, yasal zorunluluklara ve mevzuatlara uymak, çalışanlarının bilgi güvenliğine ilişkin farkındalığını arttırmak ve bilgi seviyesini yükseltmek amacı ile kendi bünyesinde BGYS kurulmasına ve uygulanmasına karar vermiştir.

3. BİLGİ GÜVENLİĞİ POLİTİKASI DOKÜMANININ GÜNCELLENMESİ VE GÖZDEN GEÇİRİLMESİ

Politika dokümanının sürekliliğinin sağlanmasından ve gözden geçirilmesinden BGYS Yöneticisi sorumludur.

Bilgi Güvenliği Politikası Dokümanı, yılda bir kez periyodik olarak ya da sistem yapısını veya risk değerlendirmesini etkileyecek organizasyona ait değişiklikler, iş şartları, değişen yasal zorunluluklar, kurumsal teknik altyapıda köklü değişiklikler gibi herhangi bir değişiklikten sonra da periyodik süreç beklenmeksizin gözden geçirilmeli ve herhangi bir değişiklik gerekiyorsa versiyon değişimi olarak kayıt altına alınmalı ve her versiyon üst yönetime onaylatılmalıdır. Bilgi Güvenliği Yönetim Sistemi sürecini etkileyecek yapısal bir değişiklik olduğunda gözden geçirilmelidir.

Sistem üzerindeki herhangi bir yapıyı ve ya risk değerlendirmesini etkileyecek önemli bir değişiklikten sonra değişiklik kayıt altına alınmalı ve her değişim BGYS Sorumlusu ve Üst Yönetimine onaylatılmalıdır.

Her kayıt altına alınan değişiklik tüm kullanıcılara portal üzerinden yayınlanmalıdır. Ayrıca kullanıcılar, e-posta ile bilgilendirilmelidir.

4. BİLGİ GÜVENLİĞİ ALT YAPISI

BGYS yöneticisi şirket içinde bilgi güvenliği ile ilgili bilgilerin sağlanması, düzenlenmesi, diğer personele aktarılması ve kontrol edilmesinden sorumlu şirket personeldir. BGYS yöneticisine sürekli bilgi akışı olmalı ve en az senede bir kez bilgi güvenliği gündemi ile aşağıdaki maddeleri değerlendirmelidir.

Bu gündem maddelerini aşağıdaki kısaca özetlenmiştir.

- Bilgi güvenliği politikalarının ve sorumlulukların gözden geçirilmelidir.
- Bilgi güvenliği olaylarının ve hatalarının gözden geçirilmelidir.
- Bilgi güvenliği sisteminde oluşan değişimlerin ve sistem üzerinde oluşan ya da oluşabilecek tehditlerin gözden geçirilmelidir.
- Bilgi güvenliği için önceliklerin gözden geçirilmelidir.

BGYS yöneticisi toplantıların yılda kaç kere olacağına, hangi tarihlerde düzenleneceğine ve toplantı tarihi değiştirme yetkisine sahiptirler. Oluşan şartlara göre BGYS yöneticisi, yukarıda belirtilen gündeme yeni madde ekleyebilir ya da herhangi bir maddeyi gündemden çıkarabilir.

5. RİSK ANALİZİ VE YÖNETİMİ STRATEJİSİ

Risk analizi için aşağıdaki metot uygulanmaktadır. Bu faaliyetle ilgili kayıtlar risk değerlendirme raporunda tutulmaktadır;

Kapsam dâhilindeki ve bilgi ile ilişkisi olan her varlığın tespiti için varlık keşif çalışması yapılır. Varlık bildirim formları ile her kullanıcının sahip olduğu (kullandığı ve yönettiği) varlıklar tespit edilir ve varlıkların sorumluları atanır.

Varlık değerlendirmesi Varlık Değeri Kriterlerine göre yapılır.

Her varlık için zayıflıklar ve tehditler tanımlanır. Varlıkların her biri için İş Etkisi Kriterlerinden uygun olan değer atanır. Risk hesaplama formülü kullanılarak her bir varlık için var olan risk değeri hesaplanır. Risk takip tablosunda tanımlanan her bir risk için aylık risk durum değerlendirmeleri yapılarak son durum hesaplanır. Risk değerleri için Risk Değerlerine Göre İşleme Seçeneklerinden uygun olanı seçilir.

5.1. **Risk Değerlendirme Metodolojisi**

İş etkisi değerlendirilirken varlığın iş üzerindeki kesinti etkisi, yerine koyma maliyeti, bilginin gizliliği, imaja olan etkisi, yasal ve hukuki yükümlülükler bakımından yaratacağı zarar (müşteriye ait bilgi gibi) konuları ele alınmalıdır.

Olasılık aralığı tespit edilirken zayıflıkların çokluğu ve var olan kontrollerin bu zayıflıkları ne kadar kapatabildiği, saldırgan motivasyonu, tehdit biçiminin uygulanma kolaylığı, bilginin rakipler için cazibesi, personelin psikolojisi, uygulamanın hassas ve kontrol edilemeyen (politikaya uymama-kuralın etrafından dolaşma) çalışan davranışı gibi unsurlar değerlendirilmelidir.

Bulunan iş etki değeri ile risk puanı yüksek orta ve düşük seviyelerde yukarıda verilen aralıkta puanlanır. Bu iki değerin çarpımı risk puanını verir. Bulunan risk puanı için yukarıda verilen aralıklarda düşük orta veya yüksek seviyelerden hangisine denk düştüğü tespit edilir. 1-10 puan arası düşük, 11-20 puan arası orta, 21-25 puan arası yüksek risk seviyesini ifade eder. Amaç risk seviyesini tüm varlıklar için kabul edilebilir risk seviyesi olan "düşük" seviyeye çekmektir.

5.2. Risk İşleme Metodolojisi

Risk değerlendirme sonucunda tüm varlıklarla ilgili risk değerleri tespit edilir. Bu değerlendirme sürekli olarak yapısal, kurumsal ve uygulama değişiklikleri çerçevesinde izlenir ve değişken risk sürekli yeniden hesaplanır. Risk işleme seçenekleri şunlardır:

Risk kabul, riskten kaçınma, riski azaltma ve kontrol etme, riskin transferi.

Kabul edilebilir risk seviyesi yönetim tarafından **0-10** puan arası riskler olarak tanımlanmıştır. Tüm varlıklar için hedefimiz riskleri bu seviyeye çekmektir.

Aksi belirtilmedikçe bütün risklerin azaltılması ve kontrol edilmesi birincil aksiyondur.

Risk işlemede birincil aksiyon kontrollerin seçilmesidir. Kontroller; uygulayıcısının ve bu uygulamayı izleyip ölçecek ilgili amirin görüşlerinin alınması, konuyla ilgili teknik iç-dış uzmanların ve danışmanların görüşlerinin alınması ile seçilir. Burada kontrol amaçları ve kontrollerin ifadesi yer alır. Bu kontrollerin teknik düzeyde nasıl uygulanacağı konu uzmanları ve kontrolü uygulayacak kişilerin seçimiyle oluşturulur. Seçilen en uygun kontrolün maliyeti tespit edilir ve riski azaltılacak varlıkla ilgili yapılan varlık değerlemesi ve iş etkisinden dolayı potansiyel mali zararla kıyaslaması yapılır. Maliyet fayda analizi sonucu seçilen kontrolün uygulanabilir olup olmadığına karar verilir. Uygulanabilir kontroller hayata geçirilir. Uygulanabilir olmayan kontroller için tekrar gözden geçirme yapılarak maliyet fayda dengesi sağlanana kadar araştırma süreci devam eder.

Uygulanan kontrol ile ilgili kayıtlar risk işleme planında belirtilir. Maliyetler ve alınan sonuçlar BGYS forumlarında görüşülür ve riskin yeni durumda ölçüm sonucu risk işleme planındaki ilgili yere yazılır.

Risk puanı kabul edilebilir seviyeye çekilene kadar gerekiyorsa yeni kontroller uygulanır ve ölçümlere devam edilir.

Riskin son durumu yönetime onaylatılır ve yönetim tarafından kabul edilen riskler için risk işleme faaliyeti tamamlanmış olur.

Risk işleme sonrası hangi periyotta riskin takip edileceği belirlenir. Bir risk hiç bir zaman tamamen ortadan kalkmaz. Varlık üzerindeki tehditler devamlı değişir ve varlığın iş etkisi de zamanla değişebilir. Bu nedenle periyodik yeniden gözden geçirmeler yapılarak riskin son durumu sürekli ölçümlenir.

5.3. SoA – Uygulanabilirlik İfadesi

Seçilen kontrollerin her birinin seçilme amacı, kontrolün içeriği, kontrolün uygulanma biçimi ve uygulanmıyorsa nedeni kısa adı SoA (Statement of Applicability) olan dokümanda belirtilmektedir. SOA Gizli bilgi sınıfındadır ve yalnızca BGYS takımının erişimine açıktır.

Bilgi güvenliği amaçları ve uygulamaları SoA'da detaylandırılmıştır. Uygulanan ve uygulanacak tüm kontroller SoA'da kaydedilir. Bu doküman Risk işleme planı ile çapraz kontrol sağlayarak herhangi bir kontrolün atlanmamasını saplamaktadır.

6. BİLGİ HASSASİYETİ VE RİSKLER

6.1. Bilgi Varlıkları

Dizüstü bilgisayarlar, ekranlar, CD ve DVD ortamındaki veriler, evraklar, klasör ve evrak dolapları, sunucular gibi elektronik veya yazılı-baskılı ortamda bulunan veya iletim ortamında (internet, e-posta, telefon vb.) yer alan tüm veriler kurumumuz için bilgi varlığı olarak tanımlanmıştır.

7. BİLGİ GÜVENLİĞİ POLİTİKA, PROSEDÜR VE PLANLARI

BGYS Politikası kurumumuzca yayınlanan bir çok farklı politika, prosedür, talimat ve rehberi kontrol ve risk yönetimi amaçları çerçevesinde adresler.

7.1. Bilgi Güvenliği Politikası

Bilgi sistemleri tarafından yayınlanan bu dokümanda genel bilgi güvenliği kuralları tanımlanmıştır.Her çalışan bu dokümanda belirtilen kurallara uymakla sorumludur.

7.2. Bilgi Güvenliği Prosedürleri ve Planları

Bilgi yedekleme, ihlal olayı müdahale, iç denetim, doküman ve kayıtların kontrolü, kullanıcı tanımlama, iş sürekliliği planı, acil durum eylem planı, risk işleme planı gibi prosedür ve planlarda sistemin işleyişi anlatılmaktadır. İlgili çalışanlar yönetimce tanımlanan ve yayınlanan bu prosedür ve planlara uygun hareket etmelidirler.

7.3. Bilgi Güvenliği Kitapçığı

Kurum bünyesinde tüm çalışanların genel olarak uyması gereken kurallar kitapçık olarak hazırlanıp tüm personele dağıtılmıştır. Çalışanlar bu kitapçıkta önerilen uygulamaları takip etmeli ve zayıflık ve tehditlere karşı uyanık olmalıdırlar. Bu kitapçıkta tanımlanan bilgi güvenliği ihlallerini yapmamalı ve bu ihlalleri gözlemlediğinde mutlaka BGYS takımına bildirmelidirler.

7.4. Bilgi güvenliği Sözleşmeleri

Kullanıcılar kurumumuzca tanımlanmış ve yayınlanmış gizlilik sözleşmelerini imzalayarak kurum politikalarına uyacaklarını taahhüt ederler. Taahhütname ve kurallar farklı dokümanlardır. Personel Bilgi Güvenliği Sözleşmesi (Taahhütnamesi) işe alınan her çalışanın (PC kullansın kullanmasın, kadrolu veya sözleşmeli tüm personel) imzaladığı bir belgedir. Dış taraflarla da ayrıca gizlilik sözleşmesi yapılmaktadır.

8. Bilgi Güvenliği Eğitimleri

Tüm kurum çalışanlarına bilgi güvenliği bilinçlendirme eğitimleri düzenlenmiştir. Yönetim çalışanların tamamına bilgi güvenliği yönetim sistemimin gerekliliklerini, amaçlarını, kurallarını ve yaptırımlarını öğretmiş ve bilinçliliği sağlamıştır. İşe yeni giren tüm çalışanlara adaptasyon eğitimleri kapsamında bilgi güvenliği eğitimleri verilmesi sağlanmıştır.

BGYS takımı üyelerine bilgi güvenliği yönetim sistemi kurulumu ve risk yönetimi eğitimi verilmiştir.

Yönetim, BGYS takımı ve çalışanların bilgi güvenliği konusunda bilinçliliği ve eğitimi için gerekli kaynakları tahsis etmektedir.

9. BİLGİ GÜVENLİĞİ İÇ DENETİMLERİ

Kurulan bilgi güvenliği yönetim sisteminin standarda ve tanımlanan politika ve prosedürlere uygunluğunun tespiti için düzenli olarak gerçekleştirilecek iç tetkikler planlanmıştır. İç tetkiklerin nasıl gerçekleştirileceği İç Tetkik Prosedüründe tanımlanmıştır ve bu prosedüre uygun olarak düzenli iç tetkikler yapılarak sistemdeki uygunsuzluklar tespit edilmektedir.

10. SÜREKLİ İYİLEŞTİRME VE DÜZELTİCİ – İYİLEŞTİRİCİ FAALİYETLER

10.1. Sürekli iyileştirme

İşletmemizdeki BGYS'nin, sürekli iyileştirilmesi için temel araçlarımız; BGYS politika ve hedefleri, gözden geçirme toplantıları, iç denetimler, doğrulama kontrolleri(risk değerlendirmeler), üçüncü taraf denetimleri, yasal denetimler, veri analizi, uygunsuzluklar ile düzeltici ve önleyici faaliyetlerdir. Bu süreçler sonunda iyileştirme alanları belirlenerek, uygulamalar yapılır ve etkinlik izlenir ve bu faaliyetler BGYS'nin gözden geçirme girdisi olarak da değerlendirilerek ihtiyaç duyulan değişiklikler yapılır.,

10.2. Düzeltici faaliyetler

İşletmemizdeki BGYS'de tespit edilen her türlü karşılaşılan problemin köküne (ana kaynağına) inebilmek için kayıt edilerek analiz yapılır. Bu şekilde, problemin çözülmesi ve bir daha oluşmaması için önlem alınır. Ayrıca, potansiyel problemleri önlemeye yardımcı olarak da bu bilgiler kullanılacaktır (önleyici işlem). Tüm yapılanlar, alınan önlemler etkinlik açısından daha sonra iç denetim veya benzer yöntemlerle(risk değerlendirme planlarınca) gözden geçirilecektir. Düzeltici faaliyetler ISO 27001 BGYS'nin gözden geçirilmesinde girdi olarak ele alınır. Düzeltici faaliyetlerin önceliği, risk değerlendirme sonuçlarına bağlı olarak belirlenir.

10.3. İyileştirici faaliyetler

Potansiyel uygunsuzlukların nedenlerini ortadan kaldırmak ve meydana gelmelerini önlemek için iç denetimler, periyodik kontroller(risk değerlendirme planlarına göre) , sürekli geliştirme faaliyetleri (politika ve hedefler dahil) BGYS'ni gözden geçirme toplantıları ve haftalık tespitler kullanılmaktadır. Yapılacak Önleyici çalışmalar potansiyel problemlerin etkisine uygun olacaktır. Esas olan, varsa değişen risklerin tanımlanması ve önemli ölçüde değişen riskler üzerinde yoğunlaşarak önleyici faaliyet gerçekleştirmektir. Önleyici faaliyetlerin önceliği, risk değerlendirme sonuçlarına bağlı olarak belirlenir.

11. YÖNETİMİN ONAYI

Kurum yönetimi olarak, "Güvenlik Politikası" nın uygulanmasının ve kontrolünün yapılmasının, güvenlik ihlallerinde de gerekli yaptırımın icra edilmesinin yönetim tarafından desteklenmektedir.

Belirlenen ilke ve politikaların sürdürülebilirliği ve geliştirilmesine yönelik çalışmalar yine Üst Yönetim tarafından desteklenir.

HAZIRLAYAN	ONAYLAYAN

12. **BİLGİ GÜVENLİĞİ İLKE ve POLİTİKALARININ OLUŞTURULMASI**

Vimsa Otomotiv bünyesinde mevcut ve oluşturulacak tüm faaliyetlere ilişkin bilgilerin güvenliğini sağlayacak, yetki seviyelerine göre bilgileri koruyacak ve bütün çalışanlar ile paydaşların yetkilerine göre ulaşabilecekleri Bilgi Güvenliği Yönetim İlke ve Politikaları Üst Yönetim tarafından belirlenir.

Vimsa Otomotiv'in tüm birim ve çalışanları **TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı**'na uygun hareket eder ve sürekli gelişimine katkı sağlarlar.

Bilgi Güvenliği Yönetim Sistemi çerçevesindeki yenilikler, değişimler ve gelişmeler tüm çalışanların ve paydaşların farkındalıklarını sağlayacak ve artıracak şekilde duyurulur.